DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix H

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	)	No. 1:15-cv-00662-TSE

OBJECTIONS AND RESPONSES BY DEFENDANTS NATIONAL SECURITY AGENCY AND ADM. MICHAEL S. ROGERS, DIRECTOR, TO PLAINTIFF'S FIRST AND SECOND SETS OF REQUESTS FOR ADMISSION

Pursuant to Rule 36 of the Federal Rules of Civil Procedure and District of Maryland Local Rule 104, Defendants National Security Agency ("NSA") and Adm. Michael S. Rogers, Director of the NSA, in his official capacity (together, the "NSA Defendants"), by their undersigned attorneys, object and respond as follows to Plaintiff Wikimedia Foundation's first and second sets of Requests for Admission, dated November 7 and 29, 2017, respectively.

GENERAL OBJECTIONS AND OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS

1. The NSA Defendants object to Plaintiff's Requests for Admission to the extent, as set forth in response to specific requests below, that they are improper attempts to use requests for admission as discovery devices, specifically, as interrogatories.

2. The NSA Defendants object to Plaintiff's Requests for Admission to the extent, as set forth in response to specific requests below, that they seek information regarding the intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

3. The NSA Defendants object to Plaintiff's Requests for Admission to the extent, as set forth in response to specific requests below, they seek information that is irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

4. As set forth in response to specific requests below, the NSA Defendants object to the definition of the term "Circuit" as vague and ambiguous insofar as it is meant, by its reference to the use of that term in the Privacy and Civil Liberties Oversight Board's "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (the "PCLOB Section 702 Report") to assign the term "Circuit" a meaning other than its ordinary meaning in the telecommunications industry. The PCLOB is an independent agency within the Executive Branch, and the NSA Defendants do not have information regarding what, if anything, that entity intended by the term "Circuit" beyond the ordinary meaning of that term within the telecommunications industry as understood by the NSA Defendants.

5. As set forth in response to specific requests below, the NSA Defendants object to the definition of the term "Internet Transaction" as vague and ambiguous insofar as it is meant, by its reference to the use of that term in the PCLOB Section 702 Report, to assign the term "Internet Transaction" a meaning other than that understood by the NSA Defendants. The PCLOB is an independent agency within the Executive Branch, and the NSA Defendants do not have information regarding what, if anything, that entity intended by the term "Internet Transaction" beyond the meaning of that term as understood by the NSA Defendants.

6. As set forth in response to specific requests below, the NSA Defendants object to the definition of "Review" as compound, unduly burdensome and oppressive, and so vague and ambiguous as to render specific requests in which it is used incapable of reasoned response.

7. As set forth in response to specific requests below, the NSA Defendants object to the definition of "Interacted With" as compound, and, insofar as it incorporates the definition of "Review," also as unduly burdensome and oppressive, and so vague and ambiguous as to render specific requests in which it is used incapable of reasoned response.

8. As set forth in response to specific requests below, the NSA Defendants object to Plaintiff's Requests for Admission to the extent that they seek information that is protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

9. The following objections and responses are based upon information currently known to the NSA Defendants, and they reserve the right to supplement or amend their objections and responses should additional or different information become available.

10. Nothing contained in the following objections and responses shall be construed as a waiver of any applicable objection or privilege as to any request or as a waiver of any objection or privilege generally. Inadvertent disclosure or unauthorized disclosure of information subject to a claim of privilege shall not be deemed a waiver of such privilege.

OBJECTIONS AND RESPONSES TO FIRST SET OF REQUESTS FOR ADMISSION

REQUEST FOR ADMISSION NO. 1: Admit that there are between 45 and 55 international submarine cables that carry INTERNET COMMUNICATIONS directly into or directly out of the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Admission No. 1 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 1 as unduly burdensome and oppressive insofar as it requests that the NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that it is difficult to determine the exact number of international submarine telecommunications cables that carry Internet communications directly into or out of the United States, because it is not publicly known whether particular cables carry Internet communications as opposed to telephonic or private-network communications. The Federal Communications Commission, which issues licenses to own and operate submarine cables and associated cable landing stations located in the United States, most recently reported that approximately 45 privately owned trans-ocean fiber optic cables (also referred to in the report as cable systems) landing in the United States or its territories were in service as of December 31, 2015. *See* Federal Communications Commission, International Bureau Report, 2015 U.S. International Circuit Capacity Data (August 2017), at 4 & Tables 4(A) & 4(B) at T-5 to T-8, available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-346376A2.pdf. Telecommunications market research and consulting firm Telegeography publishes an online Submarine Cable Landing Directory, https://www.telegeography.com/telecom-resources/submarine-cable-landing-directory, which lists 45-50 privately owned international undersea cable systems landing in the United States or its territories, many of which, however, contain multiple cables or legs. Telegeography also publishes online a map purporting to depict the international submarine cables connecting the United States with other nations as of December 11, 2017, available at https://www.submarinecablemap.com.

The NSA Defendants respond further that, according to data available from Telegeography, international submarine cables typically contain 2-8 pairs of fiber-optic cables. Each fiber-optic pair is typically capable of carrying between approximately 15 and 120 individual communications circuits on different light wavelengths, depending on age and technology used. As a result, an individual submarine cable may carry between approximately

30 and 960 communications circuits. (Individual circuits may be subdivided further to create multiple "virtual circuits" through application of various technologies.) Each wavelength carried on a fiber-optic pair is typically capable of transporting between 10 and 100 gigabits of data per second (10-100 Gbps), meaning that a typical submarine cable can carry between approximately 300 and 96,000 Gbps of data.

REQUEST FOR ADMISSION NO. 2: Admit that the international submarine cables that carry INTERNET COMMUNICATIONS directly into or directly out of the UNITED STATES make landfall at approximately 40 to 45 different landing points within the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Admission No. 2 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 2 as unduly burdensome and oppressive insofar as it requests that NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that, as noted in response to Request for Admission No. 1, above, it is not publicly known whether particular international submarine telecommunications cables carry Internet communications as opposed to telephonic or private-network communications, and it is therefore difficult as well to determine the exact number of points at which the cables carrying Internet communications make landfall within the United States. Telegeography's online Submarine Cable Landing Directory, https://www.telegeography.com/telecom-resources/submarine-cable-landing-directory, indicates that international undersea cable systems currently in service make landfall within the territory of the United States at approximately 75-80 locations.

REQUEST FOR ADMISSION NO. 3: Admit that the INTERNET BACKBONE includes international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Admission No. 3 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 3 as unduly burdensome and oppressive insofar as it requests that NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that yes, the Internet backbone includes but is not limited to international submarine telecommunications cables that carry Internet communications.

REQUEST FOR ADMISSION NO. 4: Admit that the INTERNET BACKBONE includes high-capacity terrestrial cables that carry traffic within the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Admission No. 4 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 4 as unduly burdensome and oppressive insofar as it requests that NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that yes, the Internet backbone includes but is not limited to high-capacity terrestrial telecommunications cables that carry Internet communications within the United States.

REQUEST FOR ADMISSION NO. 5: Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS that are in transit on the INTERNET BACKBONE, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

OBJECTION: The NSA Defendants object to Request for Admission No. 5 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 5 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 6: Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are in transit on the INTERNET BACKBONE, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

OBJECTION: The NSA Defendants object to Request for Admission No. 6 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 6 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants also object to Request for Admission No. 6 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that in the course of the Upstream Internet collection process, certain

Internet transactions transiting the Internet backbone networks of certain electronic communication service providers are filtered for the purpose of excluding wholly domestic communications; are then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures; and must pass through both the filter and the screen before they can be ingested into Government databases.

REQUEST FOR ADMISSION NO. 7: Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.

OBJECTION: The NSA Defendants object to Request for Admission No. 7 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 7 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 8: Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.

OBJECTION: The NSA Defendants object to Request for Admission No. 8 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 8 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants also object to Request for Admission No. 8 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that in the course of the Upstream Internet collection process, certain Internet transactions transiting the Internet backbone networks of certain electronic communication service providers are filtered for the purpose of excluding wholly domestic communications; are then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures; and must pass through both the filter and the screen before they can be ingested into Government databases.

REQUEST FOR ADMISSION NO. 9: Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

OBJECTION: The NSA Defendants object to Request for Admission No. 9 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 9 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. §3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 10: Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

OBJECTION: The NSA Defendants object to Request for Admission No. 10 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 10 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants also object to Request for Admission No. 10 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that in the course of the Upstream Internet collection process, certain Internet transactions transiting the Internet backbone networks of certain electronic communication service providers are filtered for the purpose of excluding wholly domestic communications; are then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures; and must pass through both the filter and the screen before they can be ingested into Government databases.

REQUEST FOR ADMISSION NO. 11: Admit that the NSA does not consider an INTERNET COMMUNICATION "collected," within the meaning of the 2014 NSA Minimization Procedures, until after it has REVIEWED the contents of the communication and has selected it for RETENTION.

OBJECTION: The NSA Defendants object to Request for Admission No. 11 as an improper attempt to use a request for admission as a discovery device, specifically, as an

interrogatory. The NSA Defendants also object to Request for Admission No. 11 because what the NSA "consider[s]" the collection of an Internet communication to be, within the meaning of the 2014 NSA Section 702 Minimization Procedures or otherwise, is irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

The NSA Defendants also object to Request for Admission No. 11 to the extent that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1). Finally, the NSA Defendants object to Request for Admission No. 11 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that the NSA considers the term "collection" as it applies to the Upstream Internet collection process, whether in the 2014 NSA Section 702 Minimization Procedures or otherwise, to be the ingestion of Internet transactions into Government databases after they have been filtered for the purpose of excluding wholly domestic communications, and then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures.

REQUEST FOR ADMISSION NO. 12: Admit that, in the course of Upstream surveillance, the NSA RETAINS WHOLLY DOMESTIC COMMUNICATIONS.

OBJECTION: The NSA Defendants object to Request for Admission No. 12 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 12 because it

seeks information that is irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants admit that, as found by the Privacy and Civil Liberties Oversight Board, technical measures taken to prevent acquisition of wholly domestic communications in the Upstream Internet collection process do not operate perfectly. However, the current NSA Section 702 Minimization Procedures require that wholly domestic communications "be promptly destroyed upon recognition," subject to limited exceptions described in Section 5 therein.

REQUEST FOR ADMISSION NO. 13: Admit that the NSA conducts Upstream surveillance on multiple INTERNET BACKBONE CIRCUITS.

OBJECTION: The NSA Defendants object to Request for Admission No. 13 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 13 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 14: Admit that the NSA conducts Upstream surveillance on multiple "international Internet link[s]," as that term is used by the government in its submission to the Foreign Intelligence Surveillance Court, titled "Government's Response to the Court's Briefing Order of May 9, 2011," and filed on June 1, 2011, *see* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011).

OBJECTION: The NSA Defendants object to Request for Admission No. 14 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants also object to Request for Admission No. 14 on the ground

that it attributes the phrase "international Internet link" to a Government document when in fact the phrase is taken from an opinion of the Foreign Intelligence Surveillance Court that does not purport to quote directly from the referenced Government document. *See* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). Whether the phrase "international Internet link" is contained within the referenced Government document is information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. §3605(a).

The NSA Defendants further object to Request for Admission No. 14 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 15: Admit that the NSA conducts Upstream surveillance at multiple INTERNET BACKBONE "chokepoints" or "choke points" (as that term is used by YOU).

OBJECTION: The NSA Defendants object to Request for Admission No. 15 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants also object to Request for Admission No. 15 as vague and ambiguous insofar as it does not specify where or in what context the NSA Defendants allegedly use the term "chokepoints" or "choke points." To the extent that Plaintiff's reference to that term alludes to what is described in the Amended Complaint as an "NSA slide," *see* Am. Compl. ¶ 68, the NSA Defendants object to this request as implicitly seeking information (which can be neither confirmed nor denied) regarding the authenticity of the purported slide, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants further object to Request for Admission No. 15 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 16: Admit that the document attached hereto as Exhibit A, titled "Why are we interested in HTTP?," is a true and correct excerpted copy of a genuine document.

OBJECTION: The NSA Defendants object to Request for Admission No. 16 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit A "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit A as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 16 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 17: Admit that the statements within the document attached hereto as Exhibit A were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: The NSA Defendants object to Request for Admission No. 17 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit A as evidence of intelligence activities allegedly conducted by the NSA, on the grounds that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 18: Admit that statements within the document attached hereto as Exhibit A were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: The NSA Defendants object to Request for Admission No. 18 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit A as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 19: Admit that the document attached hereto as Exhibit B, titled "Fingerprints and Appids," and "Fingerprints and Appids (more)," is a true and correct excerpted copy of a genuine document.

OBJECTION: The NSA Defendants object to Request for Admission No. 19 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit B "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit B as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 19 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 20: Admit that the statements within the document attached hereto as Exhibit B were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: The NSA Defendants object to Request for Admission No. 20 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit B as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected

from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 21: Admit that statements within the document attached hereto as Exhibit B were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: The NSA Defendants object to Request for Admission No. 21 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit B as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 22: Admit that the document attached hereto as Exhibit C, "Seven Access Sites—International 'Choke Points'," is a true and correct excerpted copy of a genuine document.

OBJECTION: The NSA Defendants object to Request for Admission No. 22 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit C "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit C as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 22 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 23: Admit that the statements within the document attached hereto as Exhibit C were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: The NSA Defendants object to Request for Admission No. 23 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in

Exhibit C as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 24: Admit that statements within the document attached hereto as Exhibit C were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: The NSA Defendants object to Request for Admission No. 24 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit C as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 25: Admit that the document attached hereto as Exhibit D, titled "SSO's Support to the FBI for Implementation of their Cyber FISA Orders," is a true and correct copy of a genuine document.

OBJECTION: The NSA Defendants object to Request for Admission No. 25 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit D "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit D as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 25 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 26: Admit that the statements within the document attached hereto as Exhibit D were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: The NSA Defendants object to Request for Admission No. 26 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit D as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 27: Admit that statements within the document attached hereto as Exhibit D were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: The NSA Defendants object to Request for Admission No. 27 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit D as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 28: Admit that the document attached hereto as Exhibit E, titled "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" and dated July 28, 2009 (the "NSA Targeting Procedures") is a true and correct copy of a genuine document.

OBJECTION: To the extent that Plaintiff seeks to establish the authenticity of Exhibit E as evidence of targeting procedures allegedly used by the NSA in 2009, the NSA Defendants object to Request for Admission No. 28 (i) as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case, *see*

October 3, 2017, Order, ECF No. 117 at 1, (ii) as irrelevant, in particular, to Plaintiff's standing to seek prospective relief, and (iii) on the ground that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 29: Admit that the statements within the document attached hereto as Exhibit E were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: To the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit E as evidence of intelligence activities allegedly conducted by the NSA in 2009, the NSA Defendants object to Request for Admission No. 29 as irrelevant and on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 30: Admit that statements within the document attached hereto as Exhibit E were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: To the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit E as evidence of intelligence activities allegedly conducted by the NSA in 2009, the NSA Defendants object to Request for Admission No. 30 as irrelevant and on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 31: Admit that the document attached hereto as Exhibit F, titled "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," dated July 2014, and available at https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf, is a true and correct copy of a genuine document.

OBJECTION: The NSA Defendants object to Request for Admission No. 31 as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

RESPONSE: Subject to the objection stated above, and without waiving it, the NSA Defendants admit that Exhibit 1 hereto is a true and correct (public) copy of the "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," dated July 2014, and available at https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf.

REQUEST FOR ADMISSION NO. 32: Admit that the statements within the document attached hereto as Exhibit F were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: The NSA Defendants object to Request for Admission No. 32 as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

RESPONSE: Denied. The 2014 NSA Section 702 Minimization Procedures, Exhibit 1 hereto, were adopted by the Attorney General of the United States, in consultation with the Director of National Intelligence, as attested by the Attorney General's signature thereto.

REQUEST FOR ADMISSION NO. 33: Admit that statements within the document attached hereto as Exhibit F were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: The NSA Defendants object to Request for Admission No. 33 as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

RESPONSE: Denied. The 2014 NSA Section 702 Minimization Procedures, Exhibit 1 hereto, were adopted by the Attorney General of the United States, in consultation with the Director of National Intelligence, as attested by the Attorney General's signature thereto.

OBJECTIONS AND RESPONSES TO SECOND SET OF REQUESTS FOR ADMISSION

REQUEST FOR ADMISSION NO. 34: Admit that, in conducting Upstream surveillance, the NSA has COPIED at least one WIKIMEDIA INTERNET COMMUNICATION.

OBJECTION: The NSA Defendants object to Request for Admission No. 34 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1). The NSA Defendants further object to Request for Admission No. 34 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 35: Admit that, in conducting Upstream surveillance, the NSA has REVIEWED the content of at least one WIKIMEDIA INTERNET COMMUNICATION.

OBJECTION: The NSA Defendants object to Request for Admission No. 35 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1). The NSA Defendants further object to Request for Admission No. 35 on the

grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

The NSA Defendants also object to Request for Admission No. 35 insofar as the definition of "Review[ed]," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

REQUEST FOR ADMISSION NO. 36: Admit that, in conducting Upstream surveillance, the NSA has RETAINED at least one WIKIMEDIA INTERNET COMMUNICATION.

OBJECTION: The NSA Defendants object to Request for Admission No. 36 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1). The NSA Defendants further object to Request for Admission No. 36 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

Dated: January 8, 2018

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
Trial Attorneys

U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Counsel for the NSA Defendants

EXHIBIT 1

EXHIBIT B

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

(U) Section 1 - Applicability and Scope

(U) These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of information, including non-publicly available information concerning unconsenting United States persons, that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act").

(U) If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity.

~~(S//NF)~~ Nothing in these procedures shall restrict NSA's performance of lawful oversight functions of its personnel or systems, or lawful oversight functions of the Department of Justice's National Security Division, Office of the Director of National Intelligence, or the applicable Offices of the Inspectors General. Additionally, nothing in these procedures shall restrict NSA's ability to conduct vulnerability or network assessments using information acquired pursuant to section 702 of the Act in order to ensure that NSA systems are not or have not been compromised. Notwithstanding any other section in these procedures, information used by NSA to conduct vulnerability or network assessments may be retained for one year solely for that limited purpose. Any information retained for this purpose may be disseminated only in accordance with the applicable provisions of these procedures.

(U) For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA).

(U) Section 2 - Definitions

(U) In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

(a) (U) Acquisition means the collection by NSA or the Federal Bureau of Investigation (FBI) through electronic means of a non-public communication to which it is not an intended party.

(b) (U) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person.

(c) (U) Communications of a United States person include all communications to which a United States person is a party.

(d) (U) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement.

(e) (U) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications.

(f) (U) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person.

(g) ~~(TS//SI//NF)~~ Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication [redacted] or multiple discrete communications [redacted]

(h) (U) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection.

(i) (U) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation.

(j) (U) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes.

(k) (U) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person:

(1) (U) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person.

(2) (U) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

(3) (U) A person who at any time has been known to have been an alien admitted for lawful permanent residence is treated as a United States person. Any determination that a person who at one time was a United States person (including an alien admitted for lawful permanent residence) is no longer a United States person must be made in consultation with the NSA Office of General Counsel.

(4) (U) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence.

(U) Section 3 - Acquisition and Handling - General

(a) (U) Acquisition

(U) The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition.

(b) (U) Monitoring, Recording, and Handling

(1) (U) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be

disseminated under these procedures. Except as provided for in subsection 3(c) below, such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event.

(2) (U) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 3, 4, 5, 6, and 8 of these procedures.

(3) (U//~~FOUO~~) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime for purposes of assessing how the communication should be handled in accordance with these procedures.

(4) (U) Handling of Internet Transactions Acquired Through NSA Upstream Collection Techniques

a. (~~TS//SI//NF~~) NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown.

1. (~~TS//SI//NF~~) Notwithstanding subsection 3(b)(4)a. above, NSA may process Internet transactions acquired through NSA upstream collection techniques in order to render such transactions intelligible to analysts.

2. (~~TS//SI//NF~~) Internet transactions that are identified and segregated pursuant to subsection 3(b)(4)a. will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States.

(a) (~~TS//SI//NF~~) Any information contained in a segregated Internet transaction (including metadata) may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. Any Internet transaction that is identified and segregated pursuant to subsection

3(b)(4)a. and is subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States will be handled in accordance with Section 5 below.

(b) (U//~~FOUO~~) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be handled in accordance with subsection 3(b)(4)b. below and the other applicable provisions of these procedures.

(c) (U//~~FOUO~~) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be marked, tagged, or otherwise identified as having been previously segregated pursuant to subsection 3(b)(4)a.

3. ~~(TS//SI//NF)~~ Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a. will be handled in accordance with subsection 3(b)(4)b. below and the other applicable provisions of these procedures.

b. (U) NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

1. ~~(TS//SI//NF)~~ If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will first perform checks to determine the locations of the sender and intended recipients of that discrete communication to the extent reasonably necessary to determine whether the sender and all intended recipients of that communication are located in the United States. If an analyst determines that the sender and all intended recipients of a discrete communication within an Internet transaction are located in the United States, the Internet transaction will be handled in accordance with Section 5 below.

2. (U) If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will assess whether the discrete communication is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

(a) (U) If the discrete communication is to, from, or about a tasked selector, any U.S. person information in that communication will be handled in accordance with the applicable provisions of these procedures.

(b) (U) If the discrete communication is not to, from, or about a tasked selector but otherwise contains foreign intelligence information, and the discrete communication is not to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, that communication (including any U.S. person information therein) will be handled in accordance with the applicable provisions of these procedures.

(c) (U) If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable U.S. person, or a person reasonably believed to be located in the United States, the NSA analyst will document that determination in the relevant analytic repository or tool if technically possible or reasonably feasible. Such discrete communication cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such use.

3. ~~(TS//SI//NF)~~ An NSA analyst seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications in a FISA application, intelligence report, or section 702 targeting must appropriately document the verifications required by subsections 3(b)(4)b.1. and 2. above.

4. ~~(TS//SI//NF)~~ Notwithstanding subsection 3(b)(4)b. above, NSA may use metadata extracted from Internet transactions acquired on or after October 31, 2011, that are not identified and segregated pursuant to subsection 3(b)(4)a. without first assessing whether the metadata was extracted from: a) a discrete communication as to which the sender and all intended recipients are located in the United States; or b) a discrete communication to, from, or about a tasked selector. Any metadata extracted from Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a. above will be handled in accordance with the applicable provisions of these procedures. Any metadata extracted from an Internet transaction subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located inside the United States shall be destroyed upon recognition.

(5) (U) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream

collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph.

(6) (U) Further handling, retention, and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further handling, storage, and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below.

(c) (U) Destruction of Raw Data

(1) ~~(S//SI~~ [redacted] Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers that do not meet the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers may not be retained longer than five years from the expiration date of the certification authorizing the collection unless NSA specifically determines that each such communication meets the retention standards in these procedures.

(2) ~~(TS//SI//NF)~~ Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. An Internet transaction may not be retained longer than two years from the expiration date of the certification authorizing the collection unless NSA specifically determines that at least one discrete communication within the Internet transaction meets the retention standards in these procedures and that each discrete communication within the transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications. Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and handled only in accordance with the standards set forth above in subsection 3(b)(4) of these procedures.

(3) ~~(TS//SI//NF)~~ Any Internet transactions acquired through NSA's upstream collection techniques prior to October 31, 2011, will be destroyed upon recognition.

(4) ~~(S/NF)~~ NSA may temporarily retain specific section 702-acquired information that would otherwise have to be destroyed, pursuant to section 3(a)-(c) above, if the Department of Justice advises NSA in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. The specific information to be retained (including, but not limited to, the target(s) or selector(s) whose unminimized information must be preserved and the relevant time period at issue in the litigation), and the particular litigation for which the information will be retained, shall be identified in writing by the Department of Justice. Personnel not working on the particular litigation matter shall not access the unminimized section 702-acquired information preserved pursuant to a written preservation notice from the Department of Justice that would otherwise have been destroyed pursuant to these procedures. Other personnel shall only access the information being retained for litigation-related reasons on a case-by-case basis after consultation with the Department of Justice. The Department of Justice shall notify NSA in writing once the section 702-acquired information is no longer required to be preserved for such litigation matters, and then NSA shall promptly destroy the section 702-acquired information as otherwise required by these procedures. Circumstances could arise requiring that section 702-acquired information subject to other destruction/age off requirements in these procedures (e.g., Section 5) be retained because it is subject to a preservation requirement. In such cases the Government will notify the Foreign Intelligence Surveillance Court and seek permission to retain the material as appropriate consistent with law. Depending on the nature, scope and complexity of a particular preservation obligation, in certain circumstances it may be technically infeasible to retain certain section 702-acquired information. Should such circumstances arise, they will be brought to the attention of the court with jurisdiction over the underlying litigation matter for resolution.

(d) (U) Change in Target's Location or Status

(1) (U//~~FOUO~~) In the event that NSA reasonably believes that a target is located outside the United States and subsequently learns that the person is inside the United States, or if NSA concludes that a target who at the time of targeting was believed to be a non-United States person is in fact a United States person at the time of acquisition, the acquisition from that person will be terminated without delay.

(2) (U) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person at the time such communications were acquired, will be treated as domestic communications under these procedures.

(e) ~~(S//NF)~~ In the event that NSA seeks to use any information acquired pursuant to section 702 during a time period when there is uncertainty about the location of the target of the acquisition because the [redacted] post-tasking checks described in NSA's section 702

targeting procedures were not functioning properly, NSA will follow its internal procedures for determining whether such information may be used (including, but not limited to, in FISA applications, section 702 targeting, and disseminations). Except as necessary to assess location under this provision, NSA may not use or disclose any information acquired pursuant to section 702 during such time period unless NSA determines, based on the totality of the circumstances, that the target is reasonably believed to have been located outside the United States at the time the information was acquired. If NSA determines that the target is reasonably believed to have been located inside the United States at the time the information was acquired, such information will not be used and will be promptly destroyed.

(U) Section 4 - Acquisition and Handling - Attorney-Client Communications

(U) As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed dissemination of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination.

(U) Section 5 - Domestic Communications

~~(TS//SI//NF)~~ A communication identified as a domestic communication (and, if applicable, the Internet transaction in which it is contained) will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing and on a communication-by-communication basis, that the sender or intended recipient of the domestic communication had been properly targeted under section 702 of the Act, and the domestic communication satisfies one or more of the following conditions:

(1) ~~(TS//SI//NF)~~ such domestic communication is reasonably believed to contain significant foreign intelligence information. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained, handled, and disseminated in accordance with these procedures;

(2) ~~(TS//SI//NF)~~ such domestic communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such domestic communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures

set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communication is required for law enforcement purposes;

(3) ~~(TS//SI//NF)~~ such domestic communication is reasonably believed to contain technical data base information, as defined in Section 2(j), or information necessary to understand or assess a communications security vulnerability. Such domestic communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that is, or is reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. (U//~~FOUO~~) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. ~~(S//SI~~ [redacted] In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signal Intelligence Director, NSA, determines in writing that retention of a specific communication for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or

(4) (U//~~FOUO~~) such domestic communication contains information pertaining to an imminent threat of serious harm to life or property. Such information may be retained and disseminated to the extent reasonably necessary to counter such threat.

~~(S//NF)~~ Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may promptly notify the FBI of that fact, as well as any information concerning the target's location that is contained in the communication. NSA may also use information derived from domestic communications for collection avoidance purposes, and may provide such information to the FBI and CIA for collection avoidance purposes. NSA may retain the communication from which such information is

derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL).

(U) Section 6 - Foreign Communications of or Concerning United States Persons

(a) (U) Retention

(U) Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

(1) (U) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. (U) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. ~~(TS//SI//NF)~~ In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signals Intelligence Director, NSA, determines in writing that retention of a specific category of communications for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) (U) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) (U) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities.

~~(TS//SI//NF)~~ Foreign communications of or concerning United States persons that may be retained under subsections 6(a)(2) and (3) above include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(b) (U) Dissemination

(U) A dissemination based on communications of or concerning a United States person may be made in accordance with Section 7 or 8 below if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) (U) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) (U) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) (U) the communication or information indicates that the United States person may be:

a. an agent of a foreign power;

b. a foreign power as defined in section 101(a) of the Act;

c. residing outside the United States and holding an official position in the government or military forces of a foreign power;

d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;

(4) (U) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) (U) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications or network security vulnerability, but only after the agency that originated the information certifies that it is properly classified;

(6) (U) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) (U//~~FOUO~~) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or

(8) (U) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document.

(c) (U) Provision of Unminimized Communications to CIA and FBI

(1) (U) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will handle any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(2) (U) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will handle any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(U) Section 7 - Other Foreign Communications

(U) Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.

(~~TS//SI//NF~~) Foreign communications of or concerning a non-United States person that may be retained under this subsection include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(U//~~FOUO~~) Additionally, foreign communications of or concerning a non-United States person may be retained for the same purposes and in the same manner as detailed in Section 6(a)(1), above.

(U) Section 8 - Collaboration with Foreign Governments

(a) (U) Procedures for the dissemination of evaluated and minimized information. Pursuant to section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided below in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with sections 6(b) and 7 of these NSA minimization procedures.

(b) (U) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated:

(1) (U) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA.

(2) (U) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data.

(3) (U) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA.

(4) (U) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA.

(5) (U) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures.

7/24/14
Date

Eric H. Holder, Jr.
Attorney General of the United States

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix I

What do parrots and BGP routers have in common?

David Hauweele*, Bruno Quoitin
University of Mons (UMONS)
{first.last}@umons.ac.be

Cristel Pelsser†
University of Strasbourg
pelsser@unistra.fr

Randy Bush
Internet Initiative Japan (IIJ)
randy@psg.com

ABSTRACT

The Border Gateway Protocol propagates routing information accross the Internet in an incremental manner. It only advertises to its peers changes in routing. However, as early as 1998, observations have been made of BGP announcing the same route multiple times, causing router CPU load, memory usage and convergence time higher than expected.

In this paper, by performing controlled experiments, we pinpoint multiple causes of duplicates, ranging from the lack of full RIB-Outs to the discrete processing of update messages. To mitigate these duplicates, we insert a cache at the output of the routers. We test it on public BGP traces and discuss the relation of the cache performance with the existence of bursts of updates in the trace.

1. INTRODUCTION

The Border Gateway Protocol [1] (BGP) is the de facto standard used to exchange inter-AS routing information on the Internet. Its correct and scalable behavior is critical to the operation of the Internet. One of the keys to BGP scalability is the use of *incremental routing updates*: only changes in destination prefix reachability are advertised. These changes include the reachability of a new prefix, the unreachability of an existing destination (withdrawal), or a modification of the path attributes associated with a destination. Path attributes are involved in routing decisions and also ensure proper protocol behavior such as avoiding routing loops. According to the protocol specification, a BGP speaker should not issue an update containing the same BGP information as was most recently advertised for the prefix.

Anomalous BGP behavior has been observed as early as 1998 [2]. Based on a 9 months trace of the BGP traffic exchanged between backbone networks, Labovitz et al. showed lack of aggregation and high routing instability with up to 99% of exchanged routing information not being related to topological changes. In particular, they observed the occurrence of redundant BGP update messages that they called *duplicate updates*. At that time, most of the duplicates where due to bogus stateless BGP implementations. The authors noted that the observed high level of instability was detrimental to the operations of the Internet, causing high router CPU load, making routers unresponsive and in the worst cases leading to packet or routing information losses. In addition, they may sometimes trigger unreachability when interacting with route flap damping [3].

Several studies later revisited BGP dynamics [4–8] and its impact on router CPU load [9], some focused on BGP duplicates. Although the number of pathological updates declined over time, duplicates still constitute a significant part of the BGP traffic with up to 15% of the updates observed at RIPE monitors in 2006 [5]. It was later shown that the duplicate problem is even worse for routers in the core of the Internet with the portion of duplicates varying from 7% to 60% in 2008 [7]. More recently, in 2009, Park et al. [6] studied over 90 RouteViews/RIPE monitors and showed that the duplicates make up 13.5% of the aggregated BGP traffic. Routers can receive up to 86.4% of duplicates during their busiest time. These previous works show that duplicates are a continuing problem. We confirm this observation by looking at all sessions from EQUINIX, ISC, LINX and WIDE RouteViews collectors from 2009 to 2014. 48.5% of the traces we observed had more than 10% of duplicates. The traces also display a high variability with an average of $(18.84 \pm 22.31)\%$ duplicates. Finally, [6] hinted that a change in attributes attached to iBGP routes may trigger eBGP duplicates. To the best of our knowledge, so far, no thorough study has explained their origin or tried to mitigate the problem.

In this paper, we make the following contributions:

- We discuss in Section 2 the causes of today's duplicates. Although the majority of duplicates in 1998 were bogus route withdrawals, this is not the case today (less than 0.5% on almost all traces). To understand what causes duplicates, we inject carefully crafted BGP updates into a router and we correlate the input and output BGP traffic. Based on this, we identify different causes for duplicates. Most duplicates today are due to implementions trading off between memory footprint and statefulness.

- In Section 3, we devise a caching mechanism that mitigates duplicates. The benefit of using a cache is that the amount of memory used can be controlled. We evaluate the efficiency of our caching mechanism on several real world BGP traces, using several replacement strategies. We show that our cache significantly reduces duplicates for prefixes in the default free zone even with a small cache size.

2. THE ORIGIN OF DUPLICATES

To investigate the origin of BGP duplicates, we follow two different approaches. First we look at a router that receives live BGP feeds. We capture all the BGP traffic and we man-

*David started this work during his internship at IIJ.

†The credits go to IIJ for supporting Cristel's work.

ually correlate duplicates observed in the outbound traffic with messages in the inbound traffic. This is an approach similar to that used by Park et al. in [6] that gives us some initial insight on potential causes for duplicates.

Second, we perform a fully controlled experiment where we inject crafted sequences of messages into a test router. We then look for duplicates in the output messages. Our experiment allows to confirm the hypotheses of Park et al. on the origin of duplicates. We also go much further as we establish three additional causes for duplicates.

This section explains our methodology and subsequent observations.

2.1 Definitions

We define a duplicate as a *redundant* prefix advertisement with the *same attributes* as the most recent update for this prefix on the same session and not interleaved with a withdrawal or a session reset. This definition is stricter than the one in [2] where an update is considered a duplicate (AADup) if its AS-Path and Next-Hop do not change. When we count duplicates, we include the initial duplicated route advertisement.

We also define the *ratio of duplicates* as the number of duplicates (including the original messages) over the total number of messages. With this definition, a trace where every advertisement is duplicated will have a ratio of 100%.

2.2 Real BGP feed experiment

The objective of this experiment is to manually investigate some occurrences of duplicates by correlating the duplicates observed at the output of a router with the messages it receives. Our setup is shown in Fig. 1. Devices $r0$, $r1$ (Cisco) and $r2$ (Juniper) are real routers while *mon*0 is a dedicated host running a software BGP router (Quagga).

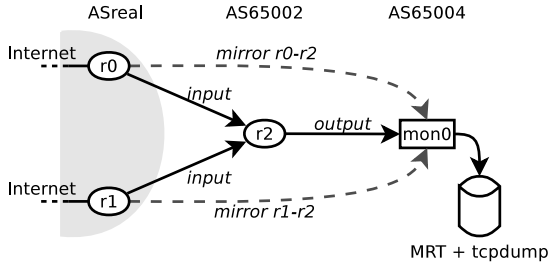


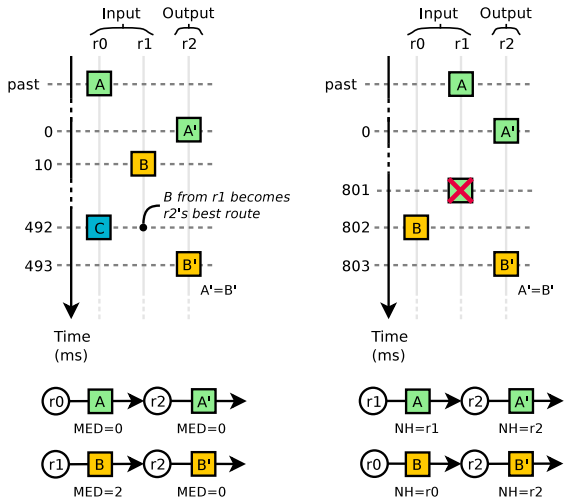
Figure 1: Setup for the I/O correlation.

The router under test is $r2$. It receives BGP messages from $r0$ and $r1$ through *input* eBGP sessions. After selecting its best routes, $r2$ sends BGP messages over a single *output* eBGP session to *mon*0. The routes learned by $r0$ and $r1$ are from real BGP feeds received in September 2013 for a duration of 23 days.

The *mon*0 host captures all the BGP messages received on the *mirror* and *output* sessions. The *mirror* sessions (dashed lines on Fig. 1) allow to capture the *input* routes advertised by the upstream routers $r0$ and $r1$. To reduce timing differences between the *input* and *mirror* sessions, both sessions are placed in the same update group on $r0$ and $r1$. The *Minimum Route Advertisement Interval* (MRAI) is also set to zero on these routers.

The messages are stored in MRT format. MRT records route advertisements, route changes and route withdrawals. Each record contains a timestamp and the path attributes. TCP-level traces of all the BGP messages received are also captured. This allows us to validate the MRT capture and dwelve deeper in the BGP message packet details e.g. to check the ordering of attributes.

We describe in the following paragraphs two common cases we observed. The first case involves the Multi-Exit-Discriminator (MED) attribute while the second case involves a rewritten Next-Hop. We do not know the exact frequency of these cases, as we have to manually extract the data.



(a) MED case (b) Next-Hop case

Figure 2: Common causes of duplicates. Timeline of the updates seen at the output of each router.

In the MED case, illustrated in Fig. 2a, we believe the duplicate is caused by a MED attribute stripped at the output of $r2$. Three different *input* routes are involved, all for the same IPv4 prefix. The first route, A, has an AS-Path of length 5 and a MED value of 0. The second route, B, has the same AS Path as A but a MED value of 2. The third route, C, has an AS Path of length 6 and a MED value of 0. At time 0ms, $r2$ announces route A learned from $r0$. Before announcing A, $r2$ updates the AS-Path and strips the MED, which produces route A'. At time 10ms, $r1$ announces route B to $r2$. The decision process of $r2$ ranks route A better than route B, causing no change in $r2$'s best route. At time 492ms, $r0$ announces to $r2$ route C which has a longer AS-Path. Route C implicitly withdraws route A. As a consequence, $r2$ now selects route B as best. Before announcing B, $r2$ strips the MED value, producing B'. *Output* routes A' and B' are equal, hence B' is a duplicate of A'.

In the case illustrated in Fig. 2b, we believe the duplicate is caused by the next-hop attribute. This case involves two routes. Route A announced first by router $r1$, is selected as best by $r2$ and announced on the *output* session at time 0ms. Before announcing route A, $r2$ rewrites the next-hop and emits route A'. At time 801ms, router $r1$ explicitly withdraws route A. At time 802ms, router $r0$ announces route B although it does not trigger any change in $r2$ yet. Finally, at time 803ms, router $r2$ selects route B as best. Before announcing route B, $r2$ rewrites the next-hop value with its own IP address, leading to route B'. Routes A and B only differ by their next-hop (resp. $r1$ and $r0$), hence routes A' and B' are identical.

2.3 Controlled experiment

To confirm the hypotheses of the previous section, we perform the same input/output matching in a fully controlled experiment. We systematically test a large set of situations that may not have appeared in the setting with a real, live BGP feed. We are able to find additional causes of duplicates and pinpoint more precisely the reasons behind these duplicates.

The setup depicted in Fig. 3 is similar to the previous experiment except we use a machine *inj*0, running Linux, to inject crafted updates to the router under test, $r0$, and another to capture its *output*. Router $r0$ is a Cisco 7200 running IOS v15.3. On *inj*0, we use ExaBGP [10] to inject synthetic updates. The monitoring host *mon*0 collects the routes observed on the *output* and *mirror* sessions with a Quagga BGP daemon and with tcpdump. The *mirror* session is used to validate *inj*0's program. We check the ability of this program to send BGP messages accurately. We measure that the minimum interval between two consecutive updates sent by ExaBGP is 1ms.

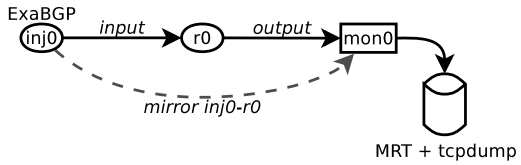


Figure 3: Setup for the injection.

Table 1 summarizes the results of the injection experiment. Due to space limitations, only results for a small number of test cases are presented. For each experiment, the first column shows the average delay between messages observed on the *input* and its standard deviation. Second column shows the same information for the *output*. The last column shows the ratio of duplicates. That is, the number of duplicates including the initial update over the number of updates (see Section 2.1).

Test case	Input (ms)	Output (ms)	Dup.
`NotVisible`	–	–	100%
`RFlap` (1 ms)	1.23 ± 0.50	3.47 ± 3.46	69.0%
`RFlap` (2 ms)	2.07 ± 0.39	2.84 ± 0.99	25.9%
`RFlap` (3 ms)	3.07 ± 0.44	3.06 ± 0.48	0.1%
`AFlap` (1 ms)	1.22 ± 0.69	3.74 ± 17.25	95.1%
`AFlap` (2 ms)	2.07 ± 0.36	2.07 ± 0.10	4.7%
`AFlap` (3 ms)	3.07 ± 0.44	3.06 ± 0.09	0.1%

Table 1: Results of selected injection test cases.

2.3.1 Internal / non-transitive / filtered attributes

This first set of experiments (`NotVisible`) considers the case of attributes whose changes should not be visible from the outside of an AS as they are either internal, non-transitive or filtered/rewritten by output policies. The objective of these experiments is to test whether or not such attributes could cause duplicate routes to be sent by the router.

For this purpose, we repeatedly send a sequence of 2 route updates (A, B) for the same destination prefix. Route B differs from route A for only a specific internal / non-transitive / filtered attribute. The expected behavior is as follows. When route A is received, it is selected as best as there is no other choice. It is then propagated on the output session. When route B is received, it replaces route A (implicit withdraw). Route B should not be propagated to the *output* session as it differs from route A only by an attribute that is either internal, non-transitive, or removed by a filter. Hence, on the *output* session, routes A and B are identical.

We observe a duplicate ratio of 100% for experiments in this class, as shown in Table 1 for the `NotVisible` test case. The router was not able to detect that the second route was a duplicate of the previous. We explain this behavior on the statelessness of the BGP implementation.

These results held for the following attributes: MED, Local Pref, Cluster List, and Originator ID. We also observed a 100% duplicates ratio for non-transitive Community values, for Community values stripped by outgoing policies and for rewritten Next-Hop (as already observed in Section 2.2).

2.3.2 Fast flapping route

In a second set of experiments (`RFlap`) we investigate the impact of a flapping route on the generation of duplicates. The experiment relies on the repetition of a simple sequence of 2 BGP updates (A, W) for the same prefix. A announces a route while W withdraws it.

The objective of this experiment is to trigger duplicates by forcing a route to change multiple times before the router has the opportunity to propagate it. To understand this behavior, we need to refine our model of how a router generates updates. When a route towards a prefix changes, the main BGP process does not send an update immediately. Instead, this task is delegated to a separate thread that periodically reads the RIB and advertises the routes marked as changed.

The following scenario illustrates how the transmission of a duplicate update can be caused. When the first Announce is received, the route is marked as changed in the RIB. The RIB is then scanned and an update is sent. Then, the Withdraw is received and the route is again marked as changed. However, before the RIB is scanned, the third message (second Announce) is received and the route is again marked as changed. When the RIB is scanned, the second Announce, identical to the first one is sent. It is a duplicate as the router did not have time to send a Withdraw between the two Announces.

We repeat this experiment with increasing delay between updates: 1ms, 2ms and 3ms. The results are in Table 1 for test case `RFlap`. We observe that with a 1ms interval, almost 70% of output updates are duplicates. When the interval between input updates increases, the ratio of duplicates decreases. With a 2ms interval, the ratio is almost 26% and at 3ms, there are almost no duplicates.

We also tested the impact of the MRAI on the generation of duplicates. We conducted the same experiment with a larger interval of 2 seconds and a MRAI set to 6 seconds. With this experiment we still generated more than 30% of duplicates.

2.3.3 Flapping attribute

This third set of experiments (`AFlap`) looks at flapping attributes. The principle is identical to the *RFlap* experiment except that the second message is not a withdraw but an update with a transitive attribute that flaps from one value to another and back. As an example, we present the results for routes where the origin AS in the AS-Path has value x in the first and third updates and has value $y \neq x$ in the sec-

ond update. We see in Table 1 for the `AFlap` test cases that the ratio of duplicates decreases with an increasing interval between the *input* BGP messages.

The explanation for these results is analogous to the *RFlap* experiment. When the interval between messages is small, the router marks the route as changed after the second message, but the third message, reversing the second update, is received before the second message is propagated downstream.

3. MITIGATING DUPLICATES

In Section 2, we found several causes explaining the generation of duplicates. According to the BGP specification, such duplicates should not appear. When a router advertises a route for a given prefix, it should store this route in the RIB-Out associated with the peer. When it later advertises a route for the same prefix, it looks at the current entry in the RIB-Out. If the current entry is the same as the new advertisement, the router does not send it because it would be a duplicate update.

We found out that although most router implementations support a RIB-Out, the implementation might be partial or operators might disable it to spare memory, especially on older hardware. Some vendors [11] explicitly recommend to disable the RIB-Out when the router has a large number of peers.

For this reason, we need to devise a solution that is not a full RIB-out but that still significantly reduces the number of BGP duplicates. This new mechanism must come at a lower cost than a RIB-Out in terms of memory consumption.

To obtain a baseline on the possible load reduction, we count the legitimate updates after filtering all duplicates. We compare this count to the number of updates in the original trace. We use a BGP trace obtained from the Equinix RouteViews collector and focus on the session with peer AS5769 (EQUIX-1). Fig. 4 shows two 12 hours excerpts of this session starting on 2013-9-17 at 0:00 (left) and 2013-9-18 at 4:00 (right). The Figure shows the total amount of updates received during the last hour (dark gray) and the same information after all duplicates have been filtered (light gray). On the left the trace has a relatively low rate of duplicates. We observe an average of 5,188 duplicates per hour. By filtering all duplicates, the number of updates on this period is reduced by an average factor of 1.62. On the right the trace features two large spikes of updates. On the largest spike, we count $5.46 * 10^5$ duplicates. By filtering all duplicates, the number of updates in this spike is reduced by a factor of 5.08.

We observe that a significant reduction in BGP traffic can be achieved by filtering duplicate updates. If CPU usage is proportional to the number of updates, sizable improvement in performance can be expected by getting rid of duplicates especially on small routers with limited CPU.

3.1 Caching router

Instead of a RIB-Out, we propose a small cache at the output of the router which can significantly reduce the number of duplicates at a far less memory cost. The advantage of this solution is that it can easily be added to the output of a router with little modifications of the BGP implementation.

A cache at the output of the router works similarly to a RIB-Out but using less memory. When a cache reaches its maximum capacity, it must remove one of its entries to add

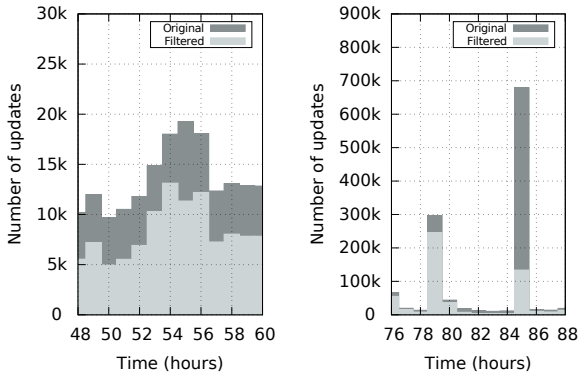


Figure 4: Two excerpts of the EQUIX-1 trace. Low rate of duplicates on the left. Spikes of duplicates on the right. We compare the original trace to the same trace with all duplicates filtered.

Name	Eviction strategy
`lru` / `mru`	Least/most recently queried entry.
`lrh` / `mrh`	Least/most recently hit entry.
`lfu` / `mfu`	Least/most frequently queried entry.
`lfh` / `mfh`	Least/most frequently hit entry.
`random`	Random entry.

Table 2: Eviction strategies

a new prefix. There are multiple ways to choose which prefix to remove when the cache is full. These selection methods are called *eviction strategies*. A cache is defined by its size and its eviction strategy.

In our case, the cache can be viewed as an Abstract Data Type (ADT) with the following operations: `query`, `remove` and `clear`. The `query` operation tells if an entry for a given key and value exists. If the given value is different from the entry in the cache, the entry is updated. If the cache does not contain an entry for this key, it adds this new entry to the cache. When the size reaches the cache limit, the cache eviction strategy comes into play. An entry is removed before the addition of the new entry to the cache. These two cases are considered *miss* queries. Instead, if the cache contains an entry for this key with the same value, the query is considered a *hit*.

The `remove` operation takes a key and if it exists, removes the associated entry from the cache. The `clear` operation removes all entries from the cache.

When the router advertises a given prefix and set of attributes, it queries the cache with the prefix as the key and the set of attributes as the value. In the case of a hit, the advertisement is a duplicate caught by the cache, and the router inhibits the advertisement. In the case of a miss, an advertisement is sent to the peer. When the router withdraws a given prefix, it removes the cache entry with the prefix as key and sends the withdraw to the peer. Finally when the router opens or reopens a session, the cache content is cleared and the router sends an open message to the peer.

3.2 Evaluation methodology

We assess the performance of the cache with the different eviction strategies listed in Table 2. The `random` cache

uses a pseudo random number generator to select an entry to remove. We use this strategy as a baseline to determine if other strategies are able to exploit characteristics of the input trace or if there is no specific pattern to exploit. Any such strategy should perform better in average than the random strategy.

In order to test the performance of the cache, we replay through the cache a previously captured trace. The cache then filters the duplicates. Since time does not matter for the eviction strategy, the cache can replay the trace without taking into account the elapsed time between each message. As a result it is possible to simulate the behavior of the cache on a captured trace much more rapidly than playing it directly on a router.

We use the Minimum Collection Time [12] (MCT) algorithm to accurately identify the start and duration of the routing table transfers in the BGP trace. We add an implicit OPEN message at the beginning of each detected table transfer so that updates within the table transfer do not count as duplicates.

3.3 Dataset

We measured the updates rate and duplicates ratio of several sessions at the RouteViews collectors from 2009 to 2014. We observed that the duplicate ratio was higher than 10% on 48.5% of the traces. The quantity of updates and duplicates also varies greatly from one session to another. The average rate of updates and duplicates per week across all traces observed in 2014 is of (3.6 ± 10.8) millions updates and (1.0 ± 3.7) millions duplicates respectively.

In order to take this variability into account, we apply the cache on three different sessions obtained from RouteViews collectors during one week period. We choose these three sessions as they contain a significant number of updates (> 1 million/week) but exhibit 3 extreme behaviours for what concerns the duplicates. Fig. 5 shows the hourly number of duplicates over time for these three traces.

	EQUIX-1	EQUIX-2	WIDE
Peer ASN	5769	2914	7500
Start	2013-09-15	2014-10-15	2013-09-15
End	2013-09-22	2014-10-22	2013-09-22
Updates	$4.5 * 10^6$	$1.55 * 10^7$	$1.2 * 10^6$
Duplicates	59.38%	98.36%	2.17%
Spikes	Large	No	Small

Table 3: Characteristics of three different traces.

Table 3 summarizes the characteristics of the traces. The number of updates and the ratio of duplicates observed vary greatly from one trace to another. The first trace, EQUIX-1, exhibits a large number of updates ($4.5{*}10^6$) and a high ratio of duplicates (59.38%), a large fraction of which (41%) visible as two large spikes of duplicates. In comparison EQUIX-2 has a higher number of updates ($1.55 * 10^7$) and a higher ratio of duplicates (98.36%) but displays no major spike. Finally the WIDE trace has a very low ratio of duplicates ($1.2 * 10^6$) and does not contain any large spike.

3.4 Results

We apply the cache on the WIDE and EQUIX-1 traces presented in Section 3.3. We also apply the cache on the third trace, EQUIX-2 with a fixed size of 65k entries and

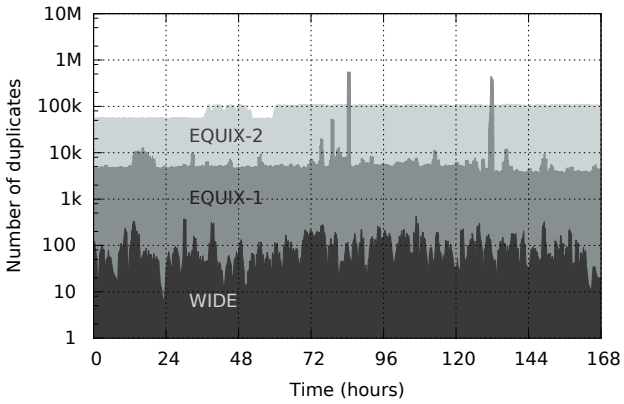


Figure 5: Three traces with different duplicates ratio. Each point shows the number of duplicates seen during the last hour.

	WIDE		EQUIX-1	
Cache	**32k**	**65k**	**32k**	**65k**
No cache	2.172%		59.38%	
`lfh`	1.351%	0.885%	49.14%	45.50%
`lfu`	1.324%	0.818%	49.09%	45.45%
`lrh`	0.040%	**0.009%**	42.91%	42.27%
`lru`	**0.039%**	0.016%	**42.90%**	42.25%
`mfh`	1.556%	1.121%	53.85%	50.30%
`mfu`	0.830%	0.173%	52.97%	48.17%
`mrh`	1.555%	1.078%	53.34%	49.68%
`mfu`	1.518%	1.014%	52.93%	49.04%
`random`	0.042%	0.020%	42.98%	**41.87%**

Table 4: Percentage of duplicates at the output of the EQUIX-1 and WIDE traces for different cache eviction strategies and sizes expressed in number of different routes.

the `lru` strategy. These traces were captured at different locations and time. They show different behaviours against which we test our solution.

Table 4 summarizes the percentage of duplicates found at the output of the WIDE and EQUIX-1 traces for two cache sizes, 32768 (32k) and 65536 (65k) different routes, and multiple strategies. The first line gives the duplicate ratio of the original trace (no cache applied). For the WIDE trace, the `lru` and `lrh` eviction strategies provide the best results. The best cache, `lrh`, reduces the original duplicate ratio by a factor 241. Further, the larger cache provides better results. In the case of the WIDE trace, the `lru` cache is 2.44 times as effective in filtering the duplicates with a cache that is twice as large.

On the EQUIX-1 trace, the cache performs poorly. With a 32k cache, the best results are achieved with the `lru` strategy. However, the output duplicate ratio remains high, at 42.9%. Doubling the cache size does not provide as much benefit as with the WIDE trace. Moreover, a striking result is that in the case of the large cache, the `random` eviction performs better than the other techniques. This indicates that the eviction strategies are not able to properly exploit the characteristics of the trace.

These results suggest that a higher duplicate ratio inhibits the performance of the cache. However, when we apply the `lru` cache of 65k on the EQUIX-2 trace, which exhibits a

higher duplicates ratio than EQUIX-1, the duplicate ratio drops from 98.36% to 5.83%. This reduces the number of updates for the trace by a factor of 50.

This shows that a cache is able to filter a session with a very high number of duplicates. I.e., the performance does not depend on the number of duplicates but rather on other characteristics of the trace. Actually, it depends on the number of distinct prefixes at the origin of those duplicates. During the EQUIX-2 trace this number stays at an average of 1000 prefixes per hour. During the EQUIX-1 trace this number stays at the same value most of the time. However when the largest spike of duplicates occurs more than $2*10^5$ distinct prefixes are involved during less than one hour. As a result the cache did not retain most of the route changes occurring during this period. Hence subsequent duplicates caused by these routes were not filtered by the cache.

3.5 Discussion

Although a cache is effective in filtering feeds with a high ratio of duplicates (e.g. EQUIX-2), we observed that spikes of updates involving a large number of distinct prefixes are detrimental to the performance of the cache. These spikes can have multiple origins. First, spikes of updates can be caused by large routing events beyond the router. Second, spikes can be caused by routing table transfers following a session reset or a change in outbound policies. It is indeed common for network operators to prompt a table transfer with a ROUTE REFRESH message in order to apply changes in their inbound policies. However spikes in this second category must have been filtered by the MCT algorithm applied beforehand.

While we can explain the origin of spikes, we do not know if these spikes represent a frequent feature of the BGP sessions. We now measure the maximum spike size in term of distinct prefixes for all RouteViews sessions we observed during the year 2014. We also apply a `lru` cache of 65k entries on all these traces to map the performance of the cache to the size of the spikes observed in the sessions. The sample size for all measured sessions is of 1339 traces.

We define attenuation as the ratio of the number of duplicates seen in the original trace over the number of duplicates seen after the cache. The average attenuation of duplicates for all observed traces is 300.47. If we distinguish the traces by the size of their maximum spikes, the average attenuation for traces with spikes larger and smaller than the size of the cache are 1.26 and 370.06 respectively.

The existence of updates spikes can negatively impact the possibility to mitigate the duplicates. We measured the presence of spikes among all observed sessions in 2014. For this purpose, we consider there is a spike in a trace when more than 65k distinct prefixes at the origin of future duplicates are transferred in less than one hour. According to this definition, 11.73% of the traces displayed large spikes of duplicates.

4. CONCLUSION

Redundant consecutive BGP announcements consume unnecessary bandwidth and CPU in routers. In addition, these messages delay the propagation of useful routing information. We observed that BGP sessions exhibit different behaviors. For some session the number of duplicates is low. But other sessions can exhibit a very high ratio of duplicates. We identified large spikes of duplicates in 11.73% of the sessions we observed in 2014. This may be a problem on chatty sessions.

We then identified three causes of duplicates: changes in attributes that are not propagated further, flapping of routes or attributes and, finally, incorrect implementations for sets in AS-Paths. We verified these causes by performing thorough controlled experiments.

To mitigate the problem we propose use of a cache to find the right trade-off between additional memory consumption and the reduction of duplicates. We show that the performance of a cache highly depends on the characteristics of the BGP trace, in addition to the eviction strategy. While a cache is suitable on some traces, it is not always the case. The current trend of pushing control functions outside the router, to devices that are not as limited memory-wise, opens the door to full Adj-RIB-Outs and thus enable to avoid using pretty hacks to get rid of BGP duplicates completely in the future.

5. REFERENCES

[1] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," RFC 4271, Jan. 2006.

[2] C. Labovitz, G. R. Malan, and F. Jahanian, "Internet routing instability," *IEEE/ACM Transactions on Networking*, vol. 6, no. 5, pp. 515–528, 1998.

[3] C. Pelsser, O. Maennel, P. Mohapatra, R. Bush, and K. Patel, "Route flap damping made usable," in *Passive and Active Measurement*, 2011, pp. 143–152.

[4] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed internet routing convergence," *ACM SIGCOMM CCR*, vol. 30, no. 4, pp. 175–187, 2000.

[5] J. Li, M. Guidero, Z. Wu, E. Purpus, and T. Ehrenkranz, "BGP routing dynamics revisited," *ACM SIGCOMM CCR*, vol. 37, no. 2, pp. 5–16, 2007.

[6] J. H. Park, D. Jen, M. Lad, S. Amante, D. McPherson, and L. Zhang, "Investigating occurrence of duplicate updates in BGP announcements," in *Passive and Active Measurement*, 2010, pp. 11–20.

[7] A. Elmokashfi, A. Kvalbein, and C. Dovrolis, "BGP churn evolution: a perspective from the core," *IEEE/ACM Transactions on Networking*, vol. 20, no. 2, pp. 571–584, 2012.

[8] A. Elmokashfi and A. Dhamdhere, "Revisiting bgp churn growth," *ACM SIGCOMM CCR*, vol. 44, no. 1, pp. 5–12, Dec. 2013.

[9] S. Agarwal, C. Chuah, S. Bhattacharyya, and C. Diot, "Impact of BGP dynamics on router CPU utilization," in *Passive and Active Network Measurement*, 2004, pp. 278–288.

[10] "ExaBGP," http://github.com/Exa-Networks/exabgp, 2014.

[11] "EXOS," http://documentation.extremenetworks.com/exos_commands/EXOS_All/EXOS_Commands_All/r_disable-bgp-adjribout.shtml, 2015.

[12] P.-C. Cheng, B. Zhang, D. Massey, and L. Zhang, "Identifying BGP routing table transfers," *Computer Networks*, vol. 55, no. 3, pp. 636–649, 2011.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix J

EXHIBIT A

Report on International Submarine Cables Landing in the US

Source: underlying data cloned from https://github.com/telegeography/www.submarinecablemap.com, most recent commit at 2018-01-02 14:09:33-05:00 (7d7cd9e8096d624717f2b4e56ebc72831e2ba7f6)

US Landing Points for International Submarine Cables

Landing 1 Bandon, Oregon, United States

Location: (124.4°W, 43.12°N)

1 International Cable:

- FASTER

  Owners:
  Google, KDDI, SingTel, China Telecom, China Mobile, Global Transit
  Other Countries:
  Japan, Taiwan

Landing 2 Bellport, New York, United States

Location: (72.94°W, 40.76°N)

1 International Cable:

- Yellow

  Owners:
  Level 3
  Other Country:
  United Kingdom

Landing 3

Boca Raton, FL, United States

Location: (80.09°W, 26.35°N)

6 International Cables:

- South America-1 (SAm-1)

  Owners:
  Telxius
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

- Bahamas Internet Cable System (BICS)

  Owners:
  Caribbean Crossings
  Other Country:
  Bahamas

- Monet

  Owners:
  Angola Cables, Google, Algar Telecom, Antel Uruguay
  Other Country:
  Brazil

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

- GlobeNet

  Owners:
  BTG Pactual
  Other Countries:
  Bermuda, Brazil, Colombia, Venezuela

- Colombia-Florida Subsea Fiber (CFX-1)

  Owners:
  C&W Networks
  Other Countries:
  Colombia, Jamaica

Landing 4

Brookhaven, New York, United States

Location: (72.91°W, 40.77°N)

1 International Cable:

- Atlantic Crossing-1 (AC-1)

  Owners:
  Level 3
  Other Countries:
  Germany, Netherlands, United Kingdom

Landing 5

Buffalo, New York, United States

Location: (78.88°W, 42.89°N)

1 International Cable:

- Crosslake Fibre

  Owners:
  Crosslake Fibre
  Other Country:
  Canada

Landing 6

Charlestown, Rhode Island, United States

Location: (71.65°W, 41.41°N)

1 International Cable:

- Challenger Bermuda-1 (CB-1)

  Owners:
  Cable Co.
  Other Country:
  Bermuda

Landing 7

El Segundo, California, United States

Location: (118.4°W, 33.92°N)

1 International Cable:

- Pacific Light Cable Network (PLCN)

  Owners:
  Pacific Light Data Communication Co. Ltd., Google, Facebook
  Other Countries:
  China, Philippines, Taiwan

Landing 8

Grover Beach, California, United States

Location: (120.6°W, 35.12°N)

2 International Cables:

- Pan-American Crossing (PAC)

  Owners:
  Level 3
  Other Countries:
  Costa Rica, Mexico, Panama

- Pacific Crossing-1 (PC-1)

  Owners:
  NTT
  Other Country:
  Japan

Landing 9

Harbour Pointe, Washington, United States

Location: (122.3°W, 47.89°N)

1 International Cable:

- Pacific Crossing-1 (PC-1)

  Owners:
  NTT
  Other Country:
  Japan

Landing 10

Hermosa Beach, California, United States

Location: (118.4°W, 33.86°N)

2 International Cables:

- JUPITER

  Owners:
  Amazon, Facebook, NTT, PLDT, PCCW, Softbank Telecom
  Other Countries:
  Japan, Philippines

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

Landing 11

Hillsboro, Oregon, United States

Location: (123°W, 45.52°N)

2 International Cables:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

Landing 12

Hollywood, Florida, United States

Location: (80.16°W, 26.01°N)

4 International Cables:

- Columbus-III

  Owners:
  Telecom Italia Sparkle, AT&T, Verizon, Telefonica, Portugal Telecom, Tata Communications, Ukrtelecom, Telkom South Africa, Telecom Argentina, Instituto Costarricense de Electricidad, Embratel, Cyta
  Other Countries:
  Italy, Portugal, Spain

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Maya-1

  Owners:
  Verizon, AT&T, Sprint, Hondutel, Telefonica, Orbitel, Telecom Italia Sparkle, C&W Networks, Entel Chile, Embratel, ETB, Axtel, Instituto Costarricense de Electricidad, Proximus, Prepa Networks, Orange, Tricom, RSL Telecom, América Móvil
  Other Countries:
  Cayman Islands, Colombia, Costa Rica, Honduras, Mexico, Panama

Landing 13

Island Park, New York, United States

Location: (73.66°W, 40.6°N)

1 International Cable:

- FLAG Atlantic-1 (FA-1)

  Owners:
  Global Cloud Xchange
  Other Countries:
  France, United Kingdom

Landing 14

Isla Verde, Puerto Rico, United States

Location: (66.02°W, 18.44°N)

3 International Cables:

- Saint Maarten Puerto Rico Network One (SMPR-1)

  Owners:
  TelEm Group, Dauphin Telecom
  Other Countries:
  Saint Martin, Sint Maarten

- ARCOS

  Owners:
  C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
  Other Countries:
  Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

- Antillas 1

  Owners:
  AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
  Other Country:
  Dominican Republic

Landing 15

Jacksonville, Florida, United States

Location: (81.66°W, 30.33°N)

3 International Cables:

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- South America Pacific Link (SAPL)

  Owners:
  Ocean Networks
  Other Countries:
  Chile, Panama

- Pacific Caribbean Cable System (PCCS)

  Owners:
  C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
  Other Countries:
  Aruba, Colombia, Curaçao, Ecuador, Panama

Landing 16

Kahe Point, Hawaii, United States

Location: (158.1°W, 21.35°N)

1 International Cable:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

Landing 17

Kapolei, HI, United States

Location: (158.1°W, 21.34°N)

1 International Cable:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

Landing 18

Kawaihae, Hawaii, United States

Location: (155.8°W, 20.04°N)

1 International Cable:

- Honotua

  Owners:
  OPT French Polynesia
  Other Country:
  French Polynesia

Landing 19 Keawaula, Hawaii, United States

Location: (158.2°W, 21.43°N)

2 International Cables:

- Telstra Endeavour

  Owners:
  Telstra
  Other Country:
  Australia

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

Landing 20 Los Angeles, California, United States

Location: (118.2°W, 34.05°N)

1 International Cable:

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

Landing 21

Lynn, Massachusetts, United States

Location: (70.95°W, 42.46°N)

1 International Cable:

- GTT Atlantic

  Owners:
  GTT
  Other Countries:
  Canada, Ireland, United Kingdom

Landing 22

Makaha, Hawaii, United States

Location: (158.2°W, 21.46°N)

3 International Cables:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

- South America Pacific Link (SAPL)

  Owners:
  Ocean Networks
  Other Countries:
  Chile, Panama

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

Landing 23

Manasquan, New Jersey, United States

Location: (74.05°W, 40.12°N)

3 International Cables:

- TAT-14

  Owners:
  BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
  Other Countries:
  Denmark, France, Germany, Netherlands, United Kingdom

- Gemini Bermuda

  Owners:
  C&W Networks
  Other Country:
  Bermuda

- Apollo

  Owners:
  Vodafone
  Other Countries:
  France, United Kingdom

Landing 24

Manchester, California, United States

Location: (123.7°W, 38.97°N)

1 International Cable:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

Landing 25

Miramar, Puerto Rico, United States

Location: (66.08°W, 18.45°N)

2 International Cables:

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Antillas 1

  Owners:
  AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
  Other Country:
  Dominican Republic

Landing 26

Morro Bay, California, United States

Location: (120.8°W, 35.37°N)

2 International Cables:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

Landing 27

Naples, FL, United States

Location: (81.8°W, 26.14°N)

1 International Cable:

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

Landing 28

Nedonna Beach, Oregon, United States

Location: (123.9°W, 45.64°N)

1 International Cable:

- Trans-Pacific Express (TPE) Cable System

  Owners:
  China Telecom, China Unicom, Chunghwa Telecom, KT, Verizon, NTT, AT&T
  Other Countries:
  China, Japan, Taiwan

Landing 29

North Miami Beach, Florida, United States

Location: (80.16°W, 25.93°N)

1 International Cable:

- ARCOS

  Owners:
  C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
  Other Countries:
  Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

Landing 30

Northport, New York, United States

Location: (73.34°W, 40.91°N)

1 International Cable:

- FLAG Atlantic-1 (FA-1)

  Owners:
  Global Cloud Xchange
  Other Countries:
  France, United Kingdom

Landing 31

Pacific City, OR, United States

Location: (124°W, 45.2°N)

2 International Cables:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

- New Cross Pacific (NCP) Cable System

  Owners:
  China Telecom, China Unicom, Chunghwa Telecom, KT, China Mobile, Microsoft, Softbank Telecom
  Other Countries:
  China, Japan, Taiwan

Landing 32

Pago Pago, American Samoa

Location: (170.7°W, -14.28°N)

2 International Cables:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

- Samoa-American Samoa (SAS)

  Owners:
  American Samoa Government, Elandia
  Other Country:
  Samoa

Landing 33 Piti, Guam

Location: (-144.7°W, 13.46°N)

5 International Cables:

- HANTRU1 Cable System

  Owners:
  Hannon Armstrong, Federated States of Micronesia Telecommunications Company, Marshall Islands Telecommunications Authority
  Other Country:
  Federated States of Micronesia

- PIPE Pacific Cable-1 (PPC-1)

  Owners:
  TPG
  Other Countries:
  Australia, Papua New Guinea

- Hong Kong-Guam (HK-G)

  Owners:
  RTI Connectivity
  Other Country:
  China

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

Landing 34

Redondo Beach, California, United States

Location: (118.4°W, 33.84°N)

1 International Cable:

- Unity/EAC-Pacific

  Owners:
  Telstra, Google, Global Transit, SingTel, KDDI, Airtel (Bharti)
  Other Country:
  Japan

Landing 35

San Juan, Puerto Rico, United States

Location: (66.11°W, 18.47°N)

7 International Cables:

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- South America-1 (SAm-1)

  Owners:
  Telxius
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

- Global Caribbean Network (GCN)

  Owners:
  Leucadia National Corporation, Loret Group
  Other Country:
  Guadeloupe

- Pacific Caribbean Cable System (PCCS)

  Owners:
  C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
  Other Countries:
  Aruba, Colombia, Curaçao, Ecuador, Panama

- Southern Caribbean Fiber

  Owners:
  Digicel
  Other Countries:
  Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

- BRUSA

  Owners:
  Telxius
  Other Country:
  Brazil

Landing 36 San Luis Obispo, California, United States

Location: (120.7°W, 35.29°N)

1 International Cable:

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

Landing 37 Sarasota, Florida, United States

Location: (82.54°W, 27.34°N)

1 International Cable:

- AURORA

  Owners:
  FP Telecommunications
  Other Countries:
  Belize, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Honduras, Mexico, Nicaragua, Panama

Landing 38

Shirley, New York, United States

Location: (72.87°W, 40.8°N)

2 International Cables:

- AEConnect (AEC)

  Owners:
  Aqua Comms
  Other Country:
  Ireland

- Apollo

  Owners:
  Vodafone
  Other Countries:
  France, United Kingdom

Landing 39

Spanish River Park, Florida, United States

Location: (80.07°W, 26.38°N)

1 International Cable:

- Bahamas Internet Cable System (BICS)

  Owners:
  Caribbean Crossings
  Other Country:
  Bahamas

Landing 40

Spencer Beach, Hawaii, United States

Location: (155.8°W, 20.02°N)

1 International Cable:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

Landing 41

St. Croix, Virgin Islands, United States

Location: (64.82°W, 17.77°N)

5 International Cables:

- South American Crossing (SAC)/Latin American Nautilus (LAN)

  Owners:
  Level 3, Telecom Italia Sparkle
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Panama, Peru, Venezuela

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Pan American (PAN-AM)

  Owners:
  AT&T, Telefonica del Peru, Softbank Telecom, Telecom Italia Sparkle, Sprint, CANTV, Tata Communications, Telefónica de Argentina, Telstra, Verizon, Entel Chile, Telecom Argentina, Telconet, Instituto Costarricense de Electricidad, C&W Networks, Embratel
  Other Countries:
  Aruba, Chile, Colombia, Ecuador, Panama, Peru, Venezuela

- Global Caribbean Network (GCN)

  Owners:
  Leucadia National Corporation, Loret Group
  Other Country:
  Guadeloupe

- Southern Caribbean Fiber

  Owners:
  Digicel
  Other Countries:
  Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

Landing 42

Tanguisson Point, Guam

Location: (-144.8°W, 13.55°N)

2 International Cables:

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

- Australia-Japan Cable (AJC)

  Owners:
  Softbank Telecom, Telstra, Verizon, AT&T
  Other Countries:
  Australia, Japan

Landing 43

Tuckerton, New Jersey, United States

Location: (74.34°W, 39.6°N)

2 International Cables:

- TAT-14

  Owners:
  BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
  Other Countries:
  Denmark, France, Germany, Netherlands, United Kingdom

- GlobeNet

  Owners:
  BTG Pactual
  Other Countries:
  Bermuda, Brazil, Colombia, Venezuela

Landing 44

Tumon Bay, Guam

Location: (-144.8°W, 13.51°N)

2 International Cables:

- Guam Okinawa Kyushu Incheon (GOKI)

  Owners:
  AT&T
  Other Country:
  Japan

- Australia-Japan Cable (AJC)

  Owners:
  Softbank Telecom, Telstra, Verizon, AT&T
  Other Countries:
  Australia, Japan

Landing 45

Vero Beach, Florida, United States

Location: (80.39°W, 27.64°N)

1 International Cable:

- Bahamas 2

  Owners:
  AT&T, Telefonica, Verizon
  Other Country:
  Bahamas

Landing 46

Virginia Beach, Virginia, United States

Location: (76.06°W, 36.76°N)

3 International Cables:

- MAREA

  Owners:
  Facebook, Microsoft, Telxius
  Other Country:
  Spain

- Midgardsormen

  Owners:
  Midgardsormen
  Other Country:
  Denmark

- BRUSA

  Owners:
  Telxius
  Other Country:
  Brazil

Landing 47

Wall Township, New Jersey, United States

Location: (74.06°W, 40.15°N)

2 International Cables:

- Tata TGN-Atlantic

  Owners:
  Tata Communications
  Other Country:
  United Kingdom

- Seabras-1

  Owners:
  Seaborn Group
  Other Country:
  Brazil

International Submarine Cables Landing in the US

Cable 1 AEConnect (AEC)

More info:
http://www.aquacomms.com
Owners:
Aqua Comms
Length:
5,536 km
US Landing Point:

- Shirley, New York, United States

Other Country:
Ireland

Cable 2 America Movil Submarine Cable System-1 (AMX-1)

More info:
http://www.americamovil.com
Owners:
América Móvil
Length:
17,800 km
US Landing Points:

- Hollywood, Florida, United States
- Jacksonville, Florida, United States
- San Juan, Puerto Rico, United States

Other Countries:
Brazil, Colombia, Dominican Republic, Guatemala, Mexico

Cable 3 Americas-II

Owners:
Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
Length:
8,373 km
US Landing Points:

- Hollywood, Florida, United States
- Miramar, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Countries:
Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

Cable 4 Antillas 1

Owners:
AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
Length:
650 km
US Landing Points:

- Isla Verde, Puerto Rico, United States
- Miramar, Puerto Rico, United States

Other Country:
Dominican Republic

Cable 5 Apollo

More info:
http://www.vodafone.com/business/article-cs-apollo-submarine-cable-system
Owners:
Vodafone
Length:
13,000 km
US Landing Points:

- Manasquan, New Jersey, United States
- Shirley, New York, United States

Other Countries:
France, United Kingdom

Cable 6 ARCOS

More info:
http://www.cwnetworks.com/
Owners:
C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
Length:
8,600 km
US Landing Points:

- North Miami Beach, Florida, United States
- Isla Verde, Puerto Rico, United States

Other Countries:
Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

Cable 7 Asia-America Gateway (AAG) Cable System

More info:
http://www.asia-america-gateway.com
Owners:
Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
Length:
20,000 km
US Landing Points:

- Keawaula, Hawaii, United States
- San Luis Obispo, California, United States
- Tanguisson Point, Guam

Other Countries:
Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

Cable 8 Atlantic Crossing-1 (AC-1)

More info:
http://www.level3.com
Owners:
Level 3
Length:
14,301 km
US Landing Point:

- Brookhaven, New York, United States

Other Countries:
Germany, Netherlands, United Kingdom

Cable 9 AURORA

More info:
http://fptelecoms.com/
Owners:
FP Telecommunications
Length:
n.a.
US Landing Point:

- Sarasota, Florida, United States

Other Countries:
Belize, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Honduras, Mexico, Nicaragua, Panama

Cable 10 Australia-Japan Cable (AJC)

More info:
http://www.ajcable.com
Owners:
Softbank Telecom, Telstra, Verizon, AT&T
Length:
12,700 km
US Landing Points:

- Tanguisson Point, Guam
- Tumon Bay, Guam

Other Countries:
Australia, Japan

Cable 11 Bahamas 2

Owners:
AT&T, Telefonica, Verizon
Length:
470 km
US Landing Point:

- Vero Beach, Florida, United States

Other Country:
Bahamas

Cable 12 Bahamas Internet Cable System (BICS)

More info:
http://www.caribbeancrossings.com
Owners:
Caribbean Crossings
Length:
1,100 km
US Landing Points:

- Boca Raton, FL, United States
- Spanish River Park, Florida, United States

Other Country:
Bahamas

Cable 13 BRUSA

More info:
http://www.telxius.com
Owners:
Telxius
Length:
11,000 km
US Landing Points:

- San Juan, Puerto Rico, United States
- Virginia Beach, Virginia, United States

Other Country:
Brazil

Cable 14 Challenger Bermuda-1 (CB-1)

More info:
http://cableco.bm
Owners:
Cable Co.
Length:
1,448 km
US Landing Point:

- Charlestown, Rhode Island, United States

Other Country:
Bermuda

Cable 15 Colombia-Florida Subsea Fiber (CFX-1)

More info:
http://www.cwnetworks.com/
Owners:
C&W Networks
Length:
2,400 km
US Landing Point:

- Boca Raton, FL, United States

Other Countries:
Colombia, Jamaica

Cable 16 Columbus-III

Owners:
Telecom Italia Sparkle, AT&T, Verizon, Telefonica, Portugal Telecom, Tata Communications, Ukrtelecom, Telkom South Africa, Telecom Argentina, Instituto Costarricense de Electricidad, Embratel, Cyta
Length:
9,833 km
US Landing Point:

- Hollywood, Florida, United States

Other Countries:
Italy, Portugal, Spain

Cable 17 Crosslake Fibre

More info:
http://www.crosslakefibre.ca
Owners:
Crosslake Fibre
Length:
131 km
US Landing Point:

- Buffalo, New York, United States

Other Country:
Canada

Cable 18 Deep Blue Cable

More info:
http://www.deepbluecable.com
Owners:
Deep Blue Cable
Length:
12,000 km
US Landing Points:

- Boca Raton, FL, United States
- San Juan, Puerto Rico, United States
- Naples, FL, United States

Other Countries:
Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

Cable 19 FASTER

Owners:
Google, KDDI, SingTel, China Telecom, China Mobile, Global Transit
Length:
11,629 km
US Landing Point:

- Bandon, Oregon, United States

Other Countries:
Japan, Taiwan

Cable 20 FLAG Atlantic-1 (FA-1)

More info:
http://www.globalcloudxchange.com
Owners:
Global Cloud Xchange
Length:
14,500 km
US Landing Points:

- Island Park, New York, United States
- Northport, New York, United States

Other Countries:
France, United Kingdom

Cable 21 Gemini Bermuda

More info:
http://www.cwnetworks.com
Owners:
C&W Networks
Length:
1,287 km
US Landing Point:

- Manasquan, New Jersey, United States

Other Country:
Bermuda

Cable 22 Global Caribbean Network (GCN)

More info:
http://www.globalcaribbean.net
Owners:
Leucadia National Corporation, Loret Group
Length:
n.a.
US Landing Points:

- San Juan, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Country:
Guadeloupe

Cable 23 GlobeNet

More info:
http://www.globenet.net
Owners:
BTG Pactual
Length:
23,500 km
US Landing Points:

- Boca Raton, FL, United States
- Tuckerton, New Jersey, United States

Other Countries:
Bermuda, Brazil, Colombia, Venezuela

Cable 24 GTT Atlantic

More info:
http://www.gtt.net
Owners:
GTT
Length:
12,200 km
US Landing Point:

- Lynn, Massachusetts, United States

Other Countries:
Canada, Ireland, United Kingdom

Cable 25

Guam Okinawa Kyushu Incheon (GOKI)

More info:
http://www.att.com
Owners:
AT&T
Length:
4,244 km
US Landing Point:

- Tumon Bay, Guam

Other Country:
Japan

Cable 26

HANTRU1 Cable System

Owners:
Hannon Armstrong, Federated States of Micronesia Telecommunications Company, Marshall Islands Telecommunications Authority
Length:
2,917 km
US Landing Point:

- Piti, Guam

Other Country:
Federated States of Micronesia

Cable 27 Hawaiki

More info:
http://hawaikicable.co.nz
Owners:
Hawaiki Cable Company
Length:
14,000 km
US Landing Points:

- Kapolei, HI, United States
- Pacific City, OR, United States
- Pago Pago, American Samoa

Other Countries:
Australia, New Zealand

Cable 28 Hong Kong-Guam (HK-G)

Owners:
RTI Connectivity
Length:
3,900 km
US Landing Point:

- Piti, Guam

Other Country:
China

Cable 29 Honotua

More info:
http://www.opt.pf
Owners:
OPT French Polynesia
Length:
4,805 km
US Landing Point:

- Kawaihae, Hawaii, United States

Other Country:
French Polynesia

Cable 30 Japan-U.S. Cable Network (JUS)

Owners:
Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
Length:
22,682 km
US Landing Points:

- Makaha, Hawaii, United States
- Manchester, California, United States
- Morro Bay, California, United States

Other Country:
Japan

Cable 31 JUPITER

Owners:
Amazon, Facebook, NTT, PLDT, PCCW, Softbank Telecom
Length:
14,000 km
US Landing Point:

- Hermosa Beach, California, United States

Other Countries:
Japan, Philippines

Cable 32 MAREA

Owners:
Facebook, Microsoft, Telxius
Length:
6,605 km
US Landing Point:

- Virginia Beach, Virginia, United States

Other Country:
Spain

Cable 33 Maya-1

More info:
http://www.maya-1.com
Owners:
Verizon, AT&T, Sprint, Hondutel, Telefonica, Orbitel, Telecom Italia Sparkle, C&W Networks, Entel Chile, Embratel, ETB, Axtel, Instituto Costarricense de Electricidad, Proximus, Prepa Networks, Orange, Tricom, RSL Telecom, América Móvil
Length:
4,400 km
US Landing Point:

- Hollywood, Florida, United States

Other Countries:
Cayman Islands, Colombia, Costa Rica, Honduras, Mexico, Panama

Cable 34 Midgardsormen

More info:
http://midgardsormen.net
Owners:
Midgardsormen
Length:
7,848 km
US Landing Point:

- Virginia Beach, Virginia, United States

Other Country:
Denmark

Cable 35 Monet

Owners:
Angola Cables, Google, Algar Telecom, Antel Uruguay
Length:
10,556 km
US Landing Point:

- Boca Raton, FL, United States

Other Country:
Brazil

Cable 36 New Cross Pacific (NCP) Cable System

Owners:
China Telecom, China Unicom, Chunghwa Telecom, KT, China Mobile, Microsoft, Softbank Telecom
Length:
13,618 km
US Landing Point:

- Pacific City, OR, United States

Other Countries:
China, Japan, Taiwan

Cable 37

Pacific Caribbean Cable System (PCCS)

Owners:
C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
Length:
6,000 km
US Landing Points:

- Jacksonville, Florida, United States
- San Juan, Puerto Rico, United States

Other Countries:
Aruba, Colombia, Curaçao, Ecuador, Panama

Cable 38

Pacific Crossing-1 (PC-1)

More info:
http://www.pc1.com
Owners:
NTT
Length:
20,900 km
US Landing Points:

- Grover Beach, California, United States
- Harbour Pointe, Washington, United States

Other Country:
Japan

Cable 39

Pacific Light Cable Network (PLCN)

More info:
http://pldc.com.hk
Owners:
Pacific Light Data Communication Co. Ltd., Google, Facebook
Length:
12,871 km
US Landing Point:

- El Segundo, California, United States

Other Countries:
China, Philippines, Taiwan

Cable 40

Pan-American Crossing (PAC)

More info:
http://www.level3.com
Owners:
Level 3
Length:
10,000 km
US Landing Point:

- Grover Beach, California, United States

Other Countries:
Costa Rica, Mexico, Panama

Cable 41 Pan American (PAN-AM)

Owners:
AT&T, Telefonica del Peru, Softbank Telecom, Telecom Italia Sparkle, Sprint, CANTV, Tata Communications, Telefónica de Argentina, Telstra, Verizon, Entel Chile, Telecom Argentina, Telconet, Instituto Costarricense de Electricidad, C&W Networks, Embratel
Length:
7,050 km
US Landing Point:

- St. Croix, Virgin Islands, United States

Other Countries:
Aruba, Chile, Colombia, Ecuador, Panama, Peru, Venezuela

Cable 42 PIPE Pacific Cable-1 (PPC-1)

More info:
http://www.pipenetworks.com/ppc1
Owners:
TPG
Length:
6,900 km
US Landing Point:

- Piti, Guam

Other Countries:
Australia, Papua New Guinea

Cable 43 Saint Maarten Puerto Rico Network One (SMPR-1)

Owners:
TelEm Group, Dauphin Telecom
Length:
375 km
US Landing Point:

- Isla Verde, Puerto Rico, United States

Other Countries:
Saint Martin, Sint Maarten

Cable 44 Samoa-American Samoa (SAS)

Owners:
American Samoa Government, Elandia
Length:
250 km
US Landing Point:

- Pago Pago, American Samoa

Other Country:
Samoa

Cable 45 Seabras-1

More info:
http://www.seabornnetworks.com
Owners:
Seaborn Group
Length:
10,800 km
US Landing Point:

- Wall Township, New Jersey, United States

Other Country:
Brazil

Cable 46 SEA-US

Owners:
RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
Length:
14,500 km
US Landing Points:

- Hermosa Beach, California, United States
- Makaha, Hawaii, United States
- Piti, Guam

Other Countries:
Federated States of Micronesia, Indonesia, Palau, Philippines

Cable 47 South America-1 (SAm-1)

More info:
http://www.telxius.com/
Owners:
Telxius
Length:
25,000 km
US Landing Points:

- Boca Raton, FL, United States
- San Juan, Puerto Rico, United States

Other Countries:
Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

Cable 48

South American Crossing (SAC)/Latin American Nautilus (LAN)

More info:
http://www.level3.com
Owners:
Level 3, Telecom Italia Sparkle
Length:
20,000 km
US Landing Point:

- St. Croix, Virgin Islands, United States

Other Countries:
Argentina, Brazil, Chile, Colombia, Panama, Peru, Venezuela

Cable 49

South America Pacific Link (SAPL)

More info:
http://www.oceannetworks.com
Owners:
Ocean Networks
Length:
17,600 km
US Landing Points:

- Jacksonville, Florida, United States
- Makaha, Hawaii, United States

Other Countries:
Chile, Panama

Cable 50 Southern Caribbean Fiber

More info:
http://www.southern-caribbean.com
Owners:
Digicel
Length:
n.a.
US Landing Points:

- San Juan, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Countries:
Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

Cable 51 Southern Cross Cable Network (SCCN)

More info:
http://www.southerncrosscables.com
Owners:
Spark New Zealand, SingTel Optus, Verizon
Length:
30,500 km
US Landing Points:

- Hillsboro, Oregon, United States
- Kahe Point, Hawaii, United States
- Morro Bay, California, United States
- Spencer Beach, Hawaii, United States

Other Countries:
Australia, Fiji, New Zealand

Cable 52 TAT-14

More info:
https://www.tat-14.com
Owners:
BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
Length:
15,295 km
US Landing Points:

- Manasquan, New Jersey, United States
- Tuckerton, New Jersey, United States

Other Countries:
Denmark, France, Germany, Netherlands, United Kingdom

Cable 53 Tata TGN-Atlantic

More info:
http://www.tatacommunications.com
Owners:
Tata Communications
Length:
13,000 km
US Landing Point:

- Wall Township, New Jersey, United States

Other Country:
United Kingdom

Cable 54 Tata TGN-Pacific

More info:
http://www.tatacommunications.com
Owners:
Tata Communications
Length:
22,300 km
US Landing Points:

- Hillsboro, Oregon, United States
- Los Angeles, California, United States
- Piti, Guam

Other Country:
Japan

Cable 55 Telstra Endeavour

More info:
https://www.telstraglobal.com
Owners:
Telstra
Length:
9,125 km
US Landing Point:

- Keawaula, Hawaii, United States

Other Country:
Australia

Cable 56 Trans-Pacific Express (TPE) Cable System

More info:
http://tpecable.org
Owners:
China Telecom, China Unicom, Chunghwa Telecom, KT, Verizon, NTT, AT&T
Length:
17,000 km
US Landing Point:

- Nedonna Beach, Oregon, United States

Other Countries:
China, Japan, Taiwan

Cable 57 Unity/EAC-Pacific

Owners:
Telstra, Google, Global Transit, SingTel, KDDI, Airtel (Bharti)
Length:
9,620 km
US Landing Point:

- Redondo Beach, California, United States

Other Country:
Japan

Cable 58 Yellow

More info:
http://www.level3.com
Owners:
Level 3
Length:
7,001 km
US Landing Point:

- Bellport, New York, United States

Other Country:
United Kingdom

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix K

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, vs. NATIONAL SECURITY AGENCY, et al., Defendants.	Case No. 1:15-cv-00662-TSE

Deposition of REBECCA J. RICHARDS

Monday, April 16, 2018

Washington, D.C.

Reported by:

Dawn A. Jaques

Job no: 21368

Deposition of:

REBECCA J. RICHARDS,

the witness, was called for examination by counsel for the Plaintiffs, pursuant to notice, commencing at 9:12 a.m., at the offices of the Department of Justice, Civil Division, Federal Programs Branch, 20 Massachusetts Avenue, Northwest, Washington, D.C., before Dawn A. Jaques, CSR, CLR, and Notary Public in and for the District of Columbia.

APPEARANCES:

On behalf of the Plaintiffs:

ALEX ABDO, ESQ.
Knight First Amendment Institute
535 West 116th Street
314 Low Library
New York, New York 10027
PHONE: (212) 854-1128
EMAIL: alex.abdo@knightcolumbia.org

- AND -

DEVON HANLEY COOK, ESQ.
Cooley LLP
101 California Street, 5th Floor
San Francisco, CA 94111-5800
PHONE: (415) 693-2116
EMAIL: dhanleycook@cooley.com

ALSO PRESENT on behalf of Plaintiffs:

Patrick Toomey, Esq., ACLU
Ashley Gorski, Esq., ACLU

APPEARANCES (Continued):

On behalf of the Defendants:

RODNEY PATTON, ESQ.
JAMES J. GILLIGAN, ESQ.
U.S. Department of Justice
Civil Division
Federal Programs Branch
20 Massachusetts Avenue, N.W.
Washington, D.C. 20530
PHONE: (202) 305-7919 (Mr. Patton)
(202) 514-3358 (Mr. Gilligan)
EMAIL: rodney.patton@usdoj.gov
james.gilligan@usdoj.gov

ALSO PRESENT FROM THE NATIONAL SECURITY AGENCY:

JASON PADGETT, ESQ.
KATHLEEN [redacted]
(443) 479-2613
[redacted]
MARY [redacted]
(301) 688-6054
[redacted]

I-N-D-E-X

E-X-H-I-B-I-T-S

INDEX (Continued)

E-X-H-I-B-I-T-S

INDEX (Continued)

E-X-H-I-B-I-T-S

P R O C E E D I N G S

MR. ABDO: Good morning, Ms. Richards. My name is Alex Abdo, and I'm here with the Knight First Amendment Institute and Columbia University, representing the Plaintiff in this case, Wikimedia Foundation.

I think you met everyone down the line, but I'm joined by my colleagues, Patrick Toomey from the American Civil Liberties Union; Devon Hanley Cook from Cooley LLP; and Ashley Gorski, also from the American Civil Liberties Union.

Would you just start out by stating your full name for the record and spelling it for us?

MR. PATTON: Could we just before we begin introduce the other attorneys here just for the record?

MR. ABDO: Please, yeah.

MR. PATTON: I'm Rodney Patton with the Department of Justice representing the NSA.

MR. PADGETT: Jason Padgett, the

Office of General Counsel at the National Security Agency.

MR. GILLIGAN: James Gilligan with the DOJ representing the defendants.

MS. [redacted] Mary [redacted] with the Office of General Counsel at the National Security Agency.

MS. [redacted] And Cathleen [redacted], Office of General Counsel, National Security Agency.

MR. ABDO: Great, I think we're done with appearances.

Ms. Richards, would you just state your full name and spell it for the record?

THE WITNESS: Rebecca Joan Richards, R-E-B-E-C-C-A, J. Richards, R-I-C-H-A-R-D-S.

MR. PATTON: This is Rodney Patton on behalf of Defendants in the case. The parties have agreed to the following rules governing the taking of this deposition.

One, counsel for the government may make such objections as he deems in good faith to

be necessary to prevent the unauthorized disclosure of protected, classified, or privileged information.

Two, counsel for the government may at any time direct the witness not to answer a question or to stop responding to a question if he deems it in good faith that it is necessary to prevent the unauthorized disclosure of protected, classified, or privileged information.

Number three, counsel for the government or the witness may stop the deposition at any time in order to confer privately in a Secure Compartmented Information Facility, known as a SCIF, for the purpose of preventing the unauthorized disclosure of protected, classified, or privileged information.

Four, nothing in the testimony of the witness will constitute or be construed as a waiver of the applicable protections or privileges subject to the plaintiffs -- or subject to the NSA reviewing the transcript.

Five, during the deposition, the

transcript may be displayed only on the court reporter's laptop, and it will not be otherwise transferred to or displayed on anyone else's electronic device during the deposition.

Six, after the deposition, the transcript will be transferred from the court reporter's laptop to counsel for the NSA by a CD or flash drive.

Seven, the transcript of the deposition will not otherwise be copied, except as appropriate by the NSA, or transmitted from the court reporter's laptop until counsel for the NSA provides the Agency's approval to do so.

Finally, in the meantime, the NSA will conduct a review of the transcript for protected, privileged, and classified information, and will redact any such information prior to the release of the transcript to plaintiff's counsel, or anyone other than the NSA and the court reporter.

That's all the ground rules. Thank you.

MR. ABDO: Ms. Jaques, have you sworn

Ms. Richards in? Would you mind doing so?

THE REPORTER: Raise your right hand, ma'am.

(The witness was administered the oath.)

Whereupon,

REBECCA J. RICHARDS,

was called as a witness, after having been first duly sworn by the Notary Public, was examined and testified as follows:

EXAMINATION BY COUNSEL FOR PLAINTIFF

BY MR. ABDO:

Q Ms. Richards, you understand that you're here today to give deposition testimony in the lawsuit of Wikimedia Foundation versus NSA, right?

A Yes.

Q And you understand that you're under oath?

A Yes.

Q Have you been deposed before?

A No.

Q Okay. So you heard a portion of the

procedures described by your counsel, Mr. Patton. I'll go over some other procedures for how the deposition will take place.

So we'll be asking you questions. Our questions and your answers will be recorded by Ms. Jaques. For that reason, it's important that you speak up and give your answers orally so that Ms. Jaques can record them, transcribe them. She won't be able to record a nod or a shake of the head.

Now, I may on occasion ask you a question that isn't clear, or that for some other reason you don't understand. If you don't understand one of my questions, let me know. It's my job to ask you clear questions. So if you say you don't understand one, I'll try to make it clearer. Do you understand that?

A Yes, I do.

Q Good. Your counsel may object at various points. If he does, please go ahead and answer the question that has been objected to unless your counsel specifically instructs you not

to answer. Do you understand that?

A Yes, I do.

Q We'll be taking periodic breaks during the deposition, but if you need to take a break at any other point, let us know. We will accommodate you. And I think you see that there's some water and coffee in the corner. If you need anything, just help yourself at any point during the deposition.

If at any point you realize that an answer you've given is incomplete or inaccurate and you'd like to supplement it or correct it in any way, let me know right away and we'll take care of it right then. Does that sound okay?

A Yes.

Q And if at any point in answering our questions you think of a document that would be helpful in refreshing your recollection, in answering the question, or in recalling what has been publicly disclosed and what hasn't about upstream surveillance, please tell us. We likely have many of those documents here today and would

be happy to provide you them. Is that okay?

A Yes, it is.

Q Great. So your counsel, Mr. Patton, outlined the process that the parties have agreed to for addressing objections based on information the NSA believes to be subject to the state secrets privilege or protected from disclosure under 50 U.S.C. § 3024(i)(1) and/or 50 U.S.C. § 3605(a). We will adhere to that process.

I'm going to use the term "classified" to refer to information the NSA believes is protected by any of those legal authorities. Is that okay with you --

A Yes.

Q -- that shorthand?

MR. PATTON: Can we just state for the record that not all of the information that will be protected by 3605, for example, is necessarily classified, but I understand your shorthand.

BY MR. ABDO:

Q Please take your time when answering

our questions. Our goal is not to trick you into disclosing protected information. We have a process in place to address those sorts of claims, but for that process to work, we need to make a clear record concerning any information the NSA believes is classified.

There are at least three scenarios that may arise. First, if you can answer a question fully without disclosing information that the NSA believes to be classified, you must do so.

Second, if you believe that a response to a question would disclose information the NSA considers classified, you should clearly state that for the record.

And, third, if you believe that a question calls for a response that is classified in part and unclassified in part, please also state that clearly for the record. You must answer and provide the unclassified information even if that does not constitute a complete response because there is also unclassified information.

Do you understand those three scenarios?

A Yes, I do.

Q Now, this case concerns surveillance that has taken place from 2015 to the present. Unless I say otherwise, my questions will apply to that full period.

If your answer would differ based on what specific portion of that period we're talking about, please say so, and please explain how it would differ for the relevant time frames.

We will do our best to make clear what time frame we're talking about, and then I'm sure your counsel will make sure we're making clear what time frame we're talking about, but if we haven't specified, please do your best to answer with respect to the full period.

Is there any reason you can think of why you would not be able to answer our questions fully and accurately today?

A No.

MR. PATTON: Other than that the

answers may be classified.

THE WITNESS: Yeah.

BY MR. ABDO:

Q Sorry, sorry. I mean are you taking any medications or drugs that would make it difficult for you to answer truthfully or accurately?

A No.

Q There's nothing that is affecting your memory today?

A No.

Q Okay. You stated before that you have not been deposed before; is that correct?

A That's correct.

Q Have you ever given testimony in a case?

A No, I have not.

Q Okay. You understand that you're appearing here today as a designated representative of the NSA, right?

A Yes.

(Deposition Exhibit 41 was marked for identification.)

BY MR. ABDO:

Q So you have in front of you what's been marked as Exhibit 41. Do you recognize that document marked as 41?

A Yeah.

Q What is it?

A These are the topics for examination. Do you want me to read more fully?

Q No, no, no.

A How detailed would you like me to be?

Q I'm asking whether that's the deposition notice that the plaintiff served on the defendants in this case.

A Oh, yes, it is. Sorry.

Q And you're appearing here today as a designee of the NSA on topics 2, 3, 4a, 4d and 6 as set forth in Exhibit 41; is that correct?

A Yes, that is correct.

Q Are you prepared to testify today about those topics?

A Yes, I am.

Q Can you tell us what you did to prepare?

A Reviewed the documents submitted, as well as a number of different documents that are already in the unclassified realm, ranging from previous minimization procedures, the NSA Civil Liberties and Privacy Office Report, the Privacy and Civil Liberties Oversight Board's report on 702, FISC opinions, as well as NSA's submissions at different points to the FISC.

Q The FISC opinions that you reviewed, are those all ones that have been disclosed publicly?

A Yes. I only reviewed the unclassified versions, so the redacted versions that are readily available on ODNI's website.

Q Did you also review any classified FISC opinions or other documents in preparing for today's deposition?

A No. We met with a subject -- I met with a subject matter expert. We discussed what

was classified and what was not classified, but otherwise I didn't review any classified documents.

Q So to the extent you talked about classified information, it was with a subject matter expert, but not reviewing any documents?

A Yes, that's correct.

Q Had you previously, unrelated to this litigation, reviewed classified versions of any of the documents that you reviewed in unclassified form?

A Yes.

Q Are you generally familiar with the classified portions of those documents?

A Yes, I am.

Q Did you meet with your counsel in preparing?

A I did.

Q You mentioned that you met with a subject matter expert. That's an NSA employee?

A Yes, it's an NSA employee.

Q What role does that individual have

within the NSA?

A An expert in upstream.

Q Is that the only subject matter expert within the NSA you met with?

A Yes, it is.

Q What's the general nature of what you talked about with that individual in unclassified form?

A We reviewed what was in the classified and in the unclassified to make sure we had a full understanding of how upstream worked and we were clear as to -- I was clear as to exactly where those lines, in terms of classification versus nonclassified information, could be discussed.

Q Okay. Was the primary purpose of that meeting to discuss that line between classified and unclassified information?

A It was more just to make sure that my memory from all of the work we had done over the last four years at NSA on upstream was current and understanding, and that I wasn't mixing and matching different activities.

So it was more of a verification that I knew exactly what it was, and this is what was classified and this wasn't.

Q Aside from preparing for this deposition, have you been involved in this litigation otherwise?

A No, I have not.

Q You've not reviewed any of the government submissions in this case?

MR. PATTON: Objection, vague as to time.

BY MR. ABDO:

Q You can answer the question.

A I reviewed all of the materials that have been provided, most everything in the binders. So, yes, I've read all of that material.

Q Did you review any documents before they were filed by the government in this case? Let me try that again.

Did you review any of the government submissions in this case prior to their being filed in court?

A I did not.

Q Have you been involved in any other litigation concerning Section 702 of the Foreign Intelligence Surveillance Act?

A No, I have not.

Q Are you familiar with other litigation concerning Section 702?

A I am.

Q What other litigation are you familiar with?

A There's at least one other lawsuit having to do -- that goes back quite a few years, sometimes referred to as the Jewel litigation.

Q Okay. So what's your current position at the NSA?

A I'm the Director of the Civil Liberties, Privacy, and Transparency Office.

Q How long have you been in that position?

A A little over four years.

Q What are your roles and responsibilities in that position?

A I set up the office four years ago, and I report directly to the Director of NSA. I'm an adviser on civil liberties, privacy, transparency issues to both the Director, as well as our Senior Leadership Team.

I review programs to identify civil liberties and privacy risks. I identify ways to mitigate them. I also work on transparency issues, publishing reports, meeting with civil society/non-governmental organizations, and then also act as the privacy advocate for NSA agency employees.

Q Are you responsible for that office's oversight of upstream surveillance?

A Could you clarify? I'm not sure what you mean by oversight of that.

Q Sure. Are you involved in your position in reviewing the operation of upstream surveillance as part of that office's mission?

MR. PATTON: Objection, vague.

You can answer.

THE WITNESS: My office reviews the

compliance incidents or other reports, oversight reports, as part of our role as information goes from NSA to ODNI.

BY MR. ABDO:

Q I just want to clarify that last portion. You said as part of your role, information goes from --

A ODNI. So -- sorry.

Our office is at a more strategic level, so we do not review every single compliance incident or every single activity specifically. We have a compliance group that does those types of functions.

My office is more strategic, so as specific reports or assessments are conducted either by ODNI or the Department of Justice, we're in that review process.

I'm also the main interlocutor with the Privacy and Civil Liberties Oversight Board, so to the extent that there are compliance incidences or changes to what -- any changes to how NSA is conducting its mission as it relates to

counterterrorism, we provide that type of information and those types of briefings to the PCLOB.

Q So in that role, you're not involved in the implementation of upstream surveillance?

MR. PATTON: Objection, vague.

THE WITNESS: So certainly at the -- there are decisions that are being made, we're informed, we will help decide, help with providing recommendations about whether it should go A or B or C, depending on specific questions that arise.

I'm not sure I'm answering your -- I'm not sure I'm fully understanding what you're trying to get at.

BY MR. ABDO:

Q Let me try to be clear.

When the government applies for authority from the Foreign Intelligence Surveillance Court to conduct upstream surveillance, is your office involved in that process?

A Yes.

Q And what's the nature of your office's involvement in that process?

A We review the minimum -- the proposed -- we will review any of the procedures. We will review any of the materials to ensure that we think that privacy has been properly protected, and civil liberties.

Q And that review happens prior to submission of an application to the Foreign Intelligence Surveillance Court?

MR. PATTON: Objection, vague.

You can answer.

THE WITNESS: Ask the question again.

BY MR. ABDO:

Q Sure. When the government is applying for authority to conduct surveillance under Section 702 of FISA -- are you familiar with the shorthand FISA for Foreign Intelligence Surveillance Act?

A I am.

MR. PATTON: Could I just interrupt?

I keep objecting to vague because

we're talking about 702, but there's PRISM and Upstream, and so if you want to be more specific, that's the nature of my objection.

MR. ABDO: That's helpful. Thanks, Rodney.

BY MR. ABDO:

Q When the government is applying for authority to conduct upstream surveillance from the Foreign Intelligence Surveillance Court, does your office review those applications prior to their submission to the Foreign Intelligence Surveillance Court?

A I understand. Hold on. Sorry, I'm looking for something specific to make sure I'm --

MR. PATTON: Take your time.

THE WITNESS: Can I talk -- take a break to make sure?

MR. PATTON: Sure.

BY MR. ABDO:

Q I just want to be clear. Just two quick things. Could you please first identify what you're looking at just for the record?

A I'm looking at the Objections and Responses by Defendant National Security Agency and Admiral Michael S. Rogers, Director, Plaintiffs' First and Second Sets of Requests for Admission.

Q And could you tell us whether you're looking to take a break to discuss classified versus unclassified information, or something else? Are you looking to discuss with your counsel the line between classified and unclassified information?

A Yes.

Q Okay. I think let me actually just withdraw that question. I don't think we need to take the time to go there.

MR. PATTON: Just to be clear to Mr. Abdo's point, the purpose of taking a break is not to talk about whatever the response is if it's not a subject of privilege.

The time to take a break and the need to take a break is related to whether to assert the privilege, and the nature and scope of the

privilege.

MR. ABDO: Thanks.

BY MR. ABDO:

Q You said that you had been in your current position for four and a half years?

A Yes.

Q Before that, were you also with the federal government?

A Yes.

Q And what position did you hold before your current one?

A I was the Senior Director for Privacy Compliance at the Department of Homeland Security in the Privacy Office.

Q How long were you in that position?

A Just shy of ten years.

Q And what were your roles and responsibilities there?

A I was in charge of developing the Privacy Impact Assessment process, publishing Privacy Act System of Records Notices, ensuring that the review of all IT systems within the

Department of Homeland Security had been reviewed for privacy considerations.

Q As part of that job, were you involved in any way in upstream surveillance?

A No.

Q As far as you know, did your roles or responsibilities in that job have any bearing on this lawsuit?

A No, not to the best of my knowledge.

Q Can you just briefly explain what a Privacy Impact Assessment is?

A Sure. It's a requirement of both the E-Government Act of 2002, as well as the Homeland Security Act, Section 222, which requires that the chief privacy officer ensure technology sustains and does not erode privacy.

It's the process by which the Department of Homeland Security and other federal agencies review technology to ensure they understand what the impact would be on privacy and how they might be able to mitigate it.

It's also a transparency document to

allow the public to know and understand what the agency is doing with their information.

Q And you were involved in the issuance of those sorts of assessments when you were at the Department of Homeland Security?

A Yes.

Q Prior to holding that position, were you also in the federal government?

A No. I worked for a small nonprofit called TRUSTe, which at the time was a nonprofit reviewing privacy policies and issuing seals of approval at the bottom of websites -- or generally seen at the bottom of websites, indicating that the privacy policy can be trusted.

Q How long were you in that position?

A I think about three years, maybe a little more, maybe a little less.

Q Were the two jobs within the federal government that you've discussed so far the only two jobs you've held in the federal government?

A No. Prior to working at TRUSTe, I worked at the Department of Commerce in the

e-commerce task force helping to negotiate the Safe Harbor Accord, which is the privacy agreement between the European Commission and the Department of Commerce for companies regulated by the Federal Trade Commission or the Department of Transportation to be able to transfer data from the EU to the US if they've agreed to a set of privacy policies.

Q What was your position then?

A I was the intern.

Q How long did you have that internship?

MR. PATTON: Don't knock it.

THE WITNESS: Don't knock it, man.

MR. ABDO: We all did.

THE WITNESS: I was there for a year. During that time frame, I went from being there called a co-op student, which means I was paid, to a full-time employee.

BY MR. ABDO:

Q But the full time you were there was one year?

A Yeah.

Q Okay. Is that the only other job you've had in the federal government?

A Yes.

Q Did that job in any way concern upstream surveillance?

A No. It was before upstream surveillance existed.

Q Can you describe your training in the areas of computer science, computer engineering, telecommunications networks, or network surveillance prior to joining the NSA?

A I do not have --

MR. PATTON: Object. Object to form, relevance.

MR. ABDO: You can answer.

MR. PATTON: You can answer.

THE WITNESS: Okay. I don't have any specific training on those four topics prior to being at NSA.

BY MR. ABDO:

Q Do you have any formal technical training from your -- let me try to be clear.

Do you have any training with respect to those four topics through, you know, college or any other graduate programs?

A No, I do not.

Q Do you have any familiarity with those topics from your time prior to joining the NSA?

MR. PATTON: Objection, vague.

THE WITNESS: Certainly my experience of working on Privacy Impact Assessments at the Department of Homeland Security, as well as working through different Internet activities, has given me a great deal of on-the-job experience.

I have no formal training to speak of in computer science or the other topics you've mentioned.

BY MR. ABDO:

Q Can you describe the on-the-job training you got in your position at the Department of Homeland Security on those four topics? And let me just be clear, on the topics of computer science, computer engineering, telecommunications networks, or network

surveillance.

A The first three are all part of the process by which we were having to review extensively the types of technology that DHS was putting forward and better understanding them to ensure we understood the privacy implications. So how did the computer systems work? Sort of how was the information being moved? Where was the information being moved?

I have no formal experience beyond my work at NSA on network surveillance.

Q For your time still at the Department of Homeland Security, would you consult with technologists to better understand how the conduct that you were reviewing might impact privacy?

A Absolutely.

Q Was that a frequent part of your job?

A Yes. We worked very closely with the chief information officer, the chief information security officer.

We also had external experts to the Department of Homeland Security who did have

experience in all of these different topics who would provide external expertise as part of the Federal Advisory Committee Act, or FACA.

All of those were available if we had questions to ensure that both we were fully understanding the privacy impact, that we had an appreciation of the information we needed to, and were getting those expertise from across -- wherever in DHS we needed.

Q You said that network surveillance was not a topic on which you received on-the-job training during your time at DHS?

A Correct.

Q Is that because there were no network surveillance programs that your office was called upon to review at your time at DHS?

MR. PATTON: Objection.

THE WITNESS: I need --

MR. PATTON: Just a second.

Objection. I'm not sure of the relevance of that particular question, but besides that, it is vague, ambiguous, but the witness can

answer.

THE WITNESS: We're now hitting into an area of classification that I would need to go and discuss any further conversation on this having to do with DHS activities.

BY MR. ABDO:

Q Let me take a step back then.

You said before that you hadn't received any on-the-job training with respect to network surveillance during your time at DHS.

That's correct, right?

A Maybe a better way would be if you could explain what you mean by "network surveillance," and then I can better answer that question.

Q Sure. I mean the use of computers to monitor communications over a telecommunications network.

A I think what I would like to do is revise what my answer is to say that, yes, I did have on-the-job training associated with that, and to go any further into that likely is classified.

Q Okay. I don't think we need to go further.

A Okay.

Q I just wanted to understand the nature of your technical training prior to your joining the NSA.

A Okay.

Q So now let's move to your time at the NSA. Can you describe in unclassified terms your on-the-job training with respect to those four areas, which again are computer science, computer engineering, telecommunications networks, or network surveillance?

MR. PATTON: Objection to the question to the extent it calls for source and methods of the NSA, operational details of Upstream, which are protected by the state secrets privilege and 50 U.S.C. § 3605(a), 50 U.S.C. § 3024(i)(1).

The witness can answer the question to the extent that it's unclassified.

MR. ABDO: And to be clear here, I'm asking just for unclassified information.

And, Rodney, can we agree on a short form of your invocation of the state secrets privilege and the other two statutory claims of protection?

MR. PATTON: I will work on that. We can maybe make a deal that you will shorten your record and I'll shorten mine.

But my concern with in unclassified terms is it may be very difficult for the witness to separate out when it's a broad question like that as opposed to a very specific question.

MR. ABDO: If instead of using the term "classified" we used the term "protected," would that be clearer?

MR. PATTON: For me I think it's just the tell me about everything nature of the question, which is very difficult for her to come up with what is classified and what is unclassified on the spot, whereas specific questions are much easier where she's -- you know, her job is to know where the line is, and she knows where the line is.

This is asking about her entire thing, so that's my concern.

BY MR. ABDO:

Q Ms. Richards, do you think you can answer my question without disclosing classified information?

A I can answer. I'm not sure it will give you what you're looking for, but ...

Q Why don't we start with what you can do.

A My answer is I have extensive ability to talk to and learn from anyone within NSA about how we do our job. To the extent that it means I'm interacting with people in all four of those categories, that's what I do.

Q Do you consider yourself to be well technically versed or conversant in those four areas?

MR. PATTON: Object to the form.

MR. ABDO: You can answer.

THE WITNESS: I do.

BY MR. ABDO:

Q I think that's fine.

As part of your job at NSA, have you ever been required to learn technical concepts relating to the programs you were reviewing that you felt unable to learn or understand?

MR. PATTON: Object to the form.

THE WITNESS: I don't understand your question, so help me.

BY MR. ABDO:

Q Sure, yeah. Your job at NSA involves reviewing NSA surveillance programs, correct?

A Correct.

MR. PATTON: Object to the form.

THE WITNESS: Correct.

BY MR. ABDO:

Q And as part of reviewing those programs, you mentioned that you talk with NSA employees about how those programs work; is that right?

A Yes.

Q When talking with those employees

about NSA surveillance programs, have you ever felt unable to comprehend technical detail that you were being explained?

MR. PATTON: Object to the form, vague. You can answer.

THE WITNESS: No, I have never felt like I couldn't understand what they were saying, or what the concepts that they were explaining to me. Is that what you're asking me?

BY MR. ABDO:

Q Yeah, that's what I'm asking you.

A Okay. No, I've never had -- they have all been able to fully explain it, both in concept and in fact.

Q Okay, great.

(Deposition Exhibit 42 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you now have in front of you what's been marked as Exhibit 42.

Do you recognize Exhibit 42?

A Yes, I do.

Q What is it?

A It is Objections and Responses by Defendants National Security Agency and Admiral Michael F. Rogers, Director, to Plaintiff's Interrogatories.

Q Could you please turn to page 17 of Exhibit 42 and read to yourself the question identified on that page as Interrogatory No. 12?

A (Witness reviewing document.)

Q Have you had a chance, Ms. Richards, to read just the interrogatory, the question itself, No. 12 on page 17?

A I'm sorry. Yes, I have.

Q Could you turn to page 18 of the same document, Exhibit 42, and read the paragraph on that page identified as RESPONSE, which is the response to Interrogatory No. 12 provided by the NSA, and let me know when you're done.

A (Witness reviewing document.) Okay.

Q Did you have any role in drafting or reviewing the NSA's response to Interrogatory No. 12?

MR. PATTON: Object to the form, vague as to time.

THE WITNESS: No, I did not.

BY MR. ABDO:

Q You didn't draft the response?

A I did not draft the response.

Q Did you see this response prior to its having been filed in federal court -- sorry, prior to this having been sent to the Plaintiffs in this lawsuit?

A No.

Q Since this response was provided to Plaintiff, have you reviewed this response?

A Yes.

Q And do you understand this response?

A Yes.

Q To your understanding, does the term "Internet backbone" include high-speed, ultra-high bandwidth data transmission lines between the networks of major Internet service providers?

MR. PATTON: Objection, calls for expert testimony of a telecommunications computer

expert. You can answer.

THE WITNESS: Certainly that is one example of what might be included in the Internet backbone.

BY MR. ABDO:

Q When you say -- what do you mean by "might be"?

A Well, as is noted in the definition, and as is actually when it first comes up in the testimony to the PCLOB, Internet backbone is a -- sort of for want of a better word, there's not a specific term that everyone turns to and says that is the Internet backbone, but rather is a general description.

And so there are a number of things, as is described here, that could be included in the Internet backbone. It's not yes or no.

Q But your understanding is that the high-speed, ultra-high bandwidth data transmission lines between the networks of major Internet service providers are one such example?

A Those could be one such example.

Q And the Internet backbone also includes high-speed, ultra-high bandwidth data transmission lines within the networks of major Internet service providers?

MR. PATTON: Objection to form, calls for expert testimony. You can answer.

THE WITNESS: You're making a distinction between within versus --

BY MR. ABDO:

Q Between, that's right.

A So with -- you're --

Q Sorry. My first set of questions related to data transmission lines between the networks of major Internet service providers -- in other words, those connecting one major Internet service provider to another -- and now I'm asking about the high-speed, ultra-high bandwidth data transmission lines within any given major Internet service provider.

MR. PATTON: Objection, calls for expert testimony. You can answer.

THE WITNESS: It certainly may be. I

wouldn't say -- it could be an example.

BY MR. ABDO:

Q Can you give other examples of high-speed, high bandwidth data transmission lines that would be part of the Internet backbone?

MR. PATTON: Objection, calls for expert testimony. You can answer.

THE WITNESS: There's the terrestrial and undersea circuits are other examples.

BY MR. ABDO:

Q Could you describe just a little bit more what you mean by those?

MR. PATTON: Same objection.

THE WITNESS: So both with Internet backbone, as well as terrestrial and undersea circuits, NSA doesn't have a specific NSA definition. It's what would be generally accepted by a telecom expert. So there's nothing special about what those are.

BY MR. ABDO:

Q And I'm not asking for a special definition of Internet backbone. I'm asking

whether your understanding of that term would encompass the sort of data transmission lines we were just discussing.

MR. PATTON: Objection to form, vague, and calls for expert opinion.

THE WITNESS: So I guess my answer hasn't changed, and to go any further would put us into classified information.

And so to the extent that the information you have in the response -- there's no additional information that is -- I can switch words around, but in essence, those are different types of examples that could be part of what the Internet backbone is, but there's no additional information I can provide to you that's not classified.

BY MR. ABDO:

Q I understand that you may not be able to provide an unclassified response to this question, but could you state whether the NSA considers high-speed, ultra-high bandwidth data transmission lines between and within the networks

of major Internet service providers to be part of the Internet backbone for purposes of upstream surveillance?

MR. PATTON: Objection, asked and answered. Objection, calls for expert testimony. And also objection that it is calling for classified information and information protected by the previously mentioned statutes, so I'll instruct the witness not to answer that question.

BY MR. ABDO:

Q Are you going to follow your lawyer's instruction not to answer the question?

A Yes.

MR. ABDO: Rodney, can we agree that every time you instruct Ms. Richards not to answer a question on the basis of its classification, you will consider us to have noted our objection to it and we can move on?

MR. PATTON: Absolutely.

MR. ABDO: Okay.

MR. PATTON: I mean, there may be other ways to ask the question to get around that.

That's part of the problem.

MR. PADGETT: Maybe we should take a break because I think there is something that could be said, but the question is throwing it off.

MR. PATTON: Right, that's what I was just saying. There may be an answer to the question, depending on how it's phrased, that we could provide an unclassified response, and so we want to try and provide as much of an unclassified response as possible, but the way the question is framed leads us into a classified area.

MR. ABDO: Let me try to ask it one other way.

BY MR. ABDO:

Q Is your understanding that telecommunications networks experts would consider the high-speed, high-bandwidth data transmission lines between and within the networks of major Internet service providers to be part of the Internet backbone?

MR. PATTON: Just take a pause.

(Counsel conferring.)

MR. PATTON: Just object to the form in terms of calling for expert testimony, but you can answer that question.

Do you need the question read back?

MR. ABDO: We can do that if that's easier.

THE WITNESS: Yeah, can you read the question one more time? Sorry. Too many things.

(The reporter read back the question.)

THE WITNESS: I think generally speaking, yes.

MR. ABDO: Rodney, if you want to take a -- if there's more you think that can be provided after a short break, we're happy to do that now.

MR. PADGETT: It might be helpful.

MR. GILLIGAN: Actually, 30 seconds.

MR. ABDO: Go off the record.

(Off the record at 10:02 a.m.)

(Resume at 10:05 a.m.)

MR. PATTON: So we've clarified the

lines as to where the privileged information in that line of questioning is, so you can ask your next question, hopefully get a response.

BY MR. ABDO:

Q Sure. Is there a way that I could have asked the last set of questions I was asking in a way that you could answer with unclassified information?

A To the extent the term "Internet backbone" is what is generally understood, as amorphous as that definition is, by a telecommunications expert, that's how NSA would describe it.

To the extent you are connecting it in some way to upstream, that's where you get to classified information.

So they're sort of differentiating between those two, but NSA doesn't have a special definition.

Q Right. And I think you answered the question with respect to the term "Internet backbone" as understood by telecommunications

networks professionals or experts, but just to be clear, that term, as used by telecommunications networks experts, includes the high-speed, ultra-high bandwidth data transmission lines between and within the networks of major Internet service providers, right?

A Yes.

MR. PATTON: Objection to the extent it calls for an expert opinion.

THE WITNESS: But generally yes, that would be what I believe they would say, and so that would be what NSA would say.

BY MR. ABDO:

Q Okay. Going back to the NSA's response to Interrogatory 12, what does the term "data transmission lines" refer to?

MR. PATTON: Objection, calls for expert opinion.

THE WITNESS: Lines that transmit data. I mean, beyond what a tele- -- so I'm not a telecommunications expert, as we've noted. That doesn't mean I don't understand how they work, but

there's no special definition here that is distinct to what NSA does.

BY MR. ABDO:

Q What I'm getting at is does the term "data transmission lines" refer to the physical means of transmission of data, or something else?

MR. PATTON: Same objection.

THE WITNESS: I will go back to that it has no special particular meaning beyond what a telecommunications expert would expect.

BY MR. ABDO:

Q Is your understanding that a telecommunications network expert will use that term, "data transmission lines," to refer to a physical means of transmission, such as, for example, a cable or a wire or an optical fiber?

MR. PATTON: Object. Object to the form, vague, and calls for expert testimony.

You can answer.

THE WITNESS: As opposed to?

BY MR. ABDO:

Q As opposed to logical or virtual

groupings of data transmitted from one point to another.

MR. PATTON: Same objections.

BY MR. ABDO:

Q I'm really just trying to understand the term that you've used in your response to Interrogatory No. 12, and the term is "data transmission lines," and what I'm trying to understand is whether that refers to physical lines of transmitting data, or other ways of transmitting -- other ways of understanding the transmission of data.

A Oh, okay.

Q Do you understand that question and what I'm trying to understand?

A Do you want to go a little further? What would be the -- I guess I'm tripping over this seems to be logical on its face, and so I'm not sure -- I'm having a hard time -- it sort of defines itself, so ...

Q So in another interrogatory response, the NSA uses the term "virtual circuit." I'm

trying to understand whether this term, "data transmission lines," is limited to physical transmission lines or something else, like virtual circuits?

MR. PATTON: Object to the form, calls for expert testimony.

THE WITNESS: Do you want to point to where virtual circuits is so I can make sure I'm not tripping up or -- I do remember seeing virtual circuits, I just don't --

BY MR. ABDO:

Q Turn to page --

A I want to make sure I'm looking at the same one that you're looking at.

Q If you turn to page 6 of Exhibit 42, it's the response to Interrogatory No. 2, designated on that page by the all caps word RESPONSE.

Do you want to take a second to read those two paragraphs to yourself?

A Yeah. (Witness reviewing document.)

Oh, okay.

Q Having read that, do you now understand what I'm asking with respect to the term "data transmission lines"?

A Yeah, it's physical data transmission lines. There's nothing -- there's nothing virtual or -- there's nothing -- it's a physical transmission line.

Q Okay, okay. Would a fiberoptic cable qualify as a data transmission line as that term is understood by telecommunications network experts?

MR. PATTON: Objection, calls for testimony by a telecommunications expert.

You can answer.

THE WITNESS: Yes, it would. That would be one example. I'm not saying that's the only example, but it's certainly an example of what might be included in that.

BY MR. ABDO:

Q Okay. Would it also include -- let me phrase the question fully.

Would the term "data transmission

line" also include optical fibers within a fiberoptic cable as that term is used by telecommunications networks and network professionals?

MR. PATTON: Objection to the extent it calls for testimony by those telecommunications experts. You can answer.

THE WITNESS: To the extent that's an example of what might be included in that, yes.

BY MR. ABDO:

Q Would a fiberoptic cable be a data transmission line as that term is understood by the NSA?

MR. PATTON: Same objection.

THE WITNESS: Can you repeat the question? I'm not sure I understood.

BY MR. ABDO:

Q Sure. Does the term "data transmission line," as the NSA has used it in response to Interrogatory 12, include fiberoptic cables?

MR. PATTON: Objection to the extent

it calls for expert testimony. You can answer.

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. And the same is true of --

A It's an example. I mean, all of these are examples. NSA doesn't have a special definition for "Internet backbone" or these other well-known telecom-like words that you're bringing up, data transmission line or fiberoptic line.

Q Does the term "data transmission line," again as used in the response to Interrogatory 12, include individual wavelengths of light carried over fiberoptic cables?

MR. PATTON: Object to the form to the extent it calls for expert testimony.

You can answer.

THE WITNESS: Certainly it is an example.

BY MR. ABDO:

Q Would the term include any subdivisions of a wavelength of light carried over a fiberoptic cable?

MR. PATTON: Same objections.

You can answer.

THE WITNESS: Would the subdivision of the light?

BY MR. ABDO:

Q Would any subdivisions of a wavelength of light carried over a fiberoptic cable constitute a data transmission line as the NSA has used that term in responding to Interrogatory 12?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: So to the extent that any of those are an example of what might be part of the Internet backbone, in which case it's providing high-speed, ultra-high bandwidth data transmission lines, the answer would be yes.

MR. ABDO: Okay. Do you mind if we take a five-minute break to use the restroom?

MR. PATTON: No.

(A break was taken at 10:15 a.m.)

(Resume at 10:25 a.m.)

BY MR. ABDO:

Q Ms. Richards, where do you acquire your understanding of the term "Internet backbone"?

A From both experts within NSA, as well as talking to -- or actually reading what's, you know, sort of been written on it in telecommunications just sort of generally.

Q Did you talk to anyone at the NSA about the meaning of the term "Internet backbone" in preparing for this deposition?

MR. PATTON: Objection to the question to the extent it calls for attorney-client privilege or any classified information, but you can answer to the extent that it is not attorney-client privileged.

THE WITNESS: Certainly in preparation for this we reviewed the definitions that have been provided to ensure that I understood them and that nothing had changed.

BY MR. ABDO:

Q Did you talk with any subject matter

experts at the NSA about the meaning of the term "Internet backbone"?

A Yes, I did.

Q Did you talk to them about anything beyond what was provided by the NSA in response to Interrogatory 12 asking for the definition of "Internet backbone"?

MR. PATTON: Object to the form, vague.

THE WITNESS: We discussed the definition and understood it to be the same as the definition that a subject matter expert in the telecommunications industry would use.

I'm not sure I'm understanding or answering what you're asking me.

BY MR. ABDO:

Q Did you talk about the terms used in the definition provided of the term "Internet backbone"?

A Yes.

Q You understand that the definition of the term "Internet backbone" is one of the terms

listed in topic 2 of the deposition notice of the case?

A Yes.

Q And you understand that the NSA has an obligation under the federal rules to provide somebody for this deposition who knows the Agency's understanding of that term?

A Yes.

MR. PATTON: Object to the extent it calls for a legal conclusion.

Just wait for my objection --

THE WITNESS: Sorry.

MR. PATTON: -- or non-objection.

BY MR. ABDO:

Q So you understand what I'm asking about? When I'm asking about the NSA's understanding of certain terms, I'm asking for the NSA's understanding, as you're a designee of the NSA today.

A Yes.

Q Okay. I want to move to a different term used in your definition.

The definition or use of the term "large, strategically interconnected computer network," what does that term mean?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: The words have no specific meaning beyond what you would expect from a telecommunications expert.

They're large, they're strategically connected, and they're computer networks. Perhaps when we --

BY MR. ABDO:

Q Is that the -- well, let me ask by example. Would that term, "large, strategically interconnected computer networks," include the networks of major Internet service providers inside the United States?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: To the extent that that might be one example of what would be included in the Internet backbone, yes, that's an example.

BY MR. ABDO:

Q I'm not sure I understood the first part of your response. Is it or is it not -- sorry, let me start that over.

Would or would not a network of a major Internet service provider constitute a large, strategically interconnected computer network as the NSA has used that term?

MR. PATTON: Object to the form to the extent it calls for expert testimony.

You can answer.

THE WITNESS: Let me clarify what I think you're asking to make sure I understand.

You're saying would a large -- I'm sorry, a communications provider in the United States be considered a strategically interconnected computer network?

BY MR. ABDO:

Q Yes.

A Yes.

Q Okay. Approximately how many data transmission lines are there that satisfy the

definition of "Internet backbone" given by the NSA?

MR. PATTON: Object to the form to the extent it calls for expert testimony.

You can answer.

THE WITNESS: If you go back and look at -- I believe it's the request for admission.

BY MR. ABDO:

Q You're welcome to refresh your recollection using that document, but I'd like your answer to that question.

A Okay, so could you ask your question one more time?

Q Sure. Approximately how many data transmission lines are there that satisfy the definition of "Internet backbone" given by the NSA?

MR. PATTON: Objection to the extent it calls for expert testimony.

THE WITNESS: How many data transmission lines meet the definition -- I'm sorry?

BY MR. ABDO:

Q Yeah, sorry, let me say it one more time. Approximately how many data transmission lines are there that satisfy the definition of "Internet backbone" given by the NSA?

MR. PATTON: Just object, first again to the extent it calls for expert testimony, and second, to the extent it is beyond the 30(b)(6) deposition notice.

Just to be clear, to the extent it's beyond the deposition notice, she'll be answering in her personal capacity as opposed to her capacity as a 30(b)(6) NSA designee.

I'll shorten that next time.

MR. ABDO: Just for the record, would you let us know what you're looking at?

THE WITNESS: I am looking at the Request for Admission response -- Request for Admission No. 1 and No. 2, just to try and make sure I'm -- I don't think that this -- how many data transmission lines are there that satisfy the definition.

MR. PATTON: The definition is Interrogatory Response 12; is that right?

THE WITNESS: Correct.

BY MR. ABDO:

Q If you don't know the answer, you don't know the answer. I'm asking whether you know the answer.

A I don't know the answer. I'm sorry.

Q Is there anyone at the NSA who would know the answer to that question?

A So to the extent that the answer to that question is available to the public -- so I guess to the extent that that information may be available in the public, we didn't -- I don't know, I mean, actually.

Q Do you know whether anyone at the NSA would know the answer to that question even if based on information not available to the public?

MR. PATTON: Well, object.

THE WITNESS: So I think --

MR. PATTON: Object to the form to the extent it calls for classified and otherwise

protected information.

The witness can answer the question if she's confident that the answer is unclassified. I'm not. I am not.

THE WITNESS: The answer to your question, to the extent it's unclassified, and to the extent it is known, would be in the public sphere and not something specific to NSA's -- to how NSA functions or what NSA does.

BY MR. ABDO:

Q Just so I understand it, is your response then that there's a further answer you could give, but will refuse to on the basis of its classification?

In other words, is there more you would say but for your belief that answering my question would disclose classified information or protected information?

MR. PATTON: Objection. The answer I believe calls for classified information and information otherwise protected by the statutory privileges, and I instruct the witness not to

answer.

BY MR. ABDO:

Q Are you going to follow your --

A I am going to follow my lawyer's --

Q -- instruction not to answer?

A -- instruction not to answer.

Q Is your understanding then that even answering my question of whether providing an answer to my question would disclose classified information is itself classified?

MR. PATTON: Same objection.

Just a second.

(Counsel conferring.)

THE WITNESS: I think it would --

MR. PATTON: Just a second.

MR. PADGETT: Could you read back the question?

THE WITNESS: I just wanted to read back the question, yeah, or you can restate the question.

BY MR. ABDO:

Q Let me restate the question. I'll go

back to what I think started us down this path.

I originally asked whether there's somebody at the NSA who knows how many data transmission lines there are that satisfy the definition of "Internet backbone" provided by the NSA. I believe you said you don't know the answer, so I asked whether somebody at the NSA would know the answer to that question.

Then I believe you said, please correct me if I'm wrong, that to the extent there's an answer that you can provide publicly to that question, it was provided in the NSA's responses to our requests for admission.

A Can we go out on a classified -- could we take a --

Q Sure.

MR. PATTON: Yes. I just want to say before we go off the record that object to the extent it misstates the prior testimony, and that she also said that it doesn't mean anything different in an unclassified sense than what telecommunications experts would say.

BY MR. ABDO:

Q Okay. You understand that I was asking about knowledge that the NSA has irrespective of whether that information is available to the general public.

A I did understand. What I said was I was not answering about what NSA knew or didn't know because there's a classification issue, but to the extent there was an answer to your question, it would be whatever you could find in the public.

And so similar to what you see in response to RFA 1, where we give the information that TeleGeography publishes, to the extent they have information that would say -- provide the answer to this question, but I don't think that the answer to RFA 1 was the same as what you were asking.

MR. PATTON: And so we'll go off the record and see if there's more information that can be provided unclassified.

MR. ABDO: That's fine, although I'm

also trying to establish whether there's somebody at the NSA who would be able to provide a classified response, even if not here today, whether there's somebody who could provide that response if we were to move to compel that response.

It sounds as though you're not that person from what you're saying. I'm trying to understand if there's somebody else who is that person.

THE WITNESS: And so could we please --

MR. PATTON: Wait a second.

And we're trying to figure out whether we can tell you that.

THE WITNESS: Yes, so let us go have that --

MR. ABDO: We'll go off the record for a few minutes.

(Off the record at 10:38 a.m.)

(Resume at 10:47 a.m.)

MR. PATTON: Have we got a question

pending?

MR. ABDO: Yes, we have a question pending, and as I understand it, Ms. Richards, you went out to consult with counsel about whether you could respond to my question without disclosing classified information.

Have you arrived at a conclusion?

MR. PATTON: Yes. It's like a jury, we have arrived at a verdict.

So just to put my objections on the record, one is that it calls for expert testimony; two, it is beyond the 30(b)(6) notice, and therefore the witness's answer, if she were to give one, would be in her personal capacity as opposed to her capacity as a 30(b)(6) witness.

And if I understand the question correctly, anything beyond the unclassified information that's already been provided in the RFA, we can neither confirm nor deny whether or not --

MR. PADGETT: I'm sorry.

(Counsel conferring.)

MR. PATTON: So striking the last part, whether NSA has any nonpublic information going beyond what's already in the RFA we can neither confirm nor deny, so on that basis, instruct the witness not to answer the pending question.

BY MR. ABDO:

Q And you'll follow your lawyer's instruction not to answer?

A I will follow my lawyer's advice not to answer.

Q Okay. Could you please turn to page 5 of Exhibit 42 -- sorry, page 6 of Exhibit 42. You were here a moment ago, but if you need to, would you please re-read the two paragraphs designated as "RESPONSE" on that page.

A I'm sorry, to clarify, we're on the interrogatories?

Q Yes. Exhibit 42 are the NSA's Responses and Objections to Plaintiff's First Set of Interrogatories, page 6.

A Page 6, yes.

Q If you need to, just refresh your memory of that response.

A Yes.

Q Is an international submarine cable that connects two stations a circuit as the NSA has defined that term in response to Interrogatory No. 2?

MR. PATTON: Objection to the extent it calls for expert testimony.

THE WITNESS: As with Internet backbone, "circuit" has no specific NSA meaning. It is the meaning that a telecommunications expert would expect it to mean. There's nothing something special. So I just want to make sure that that's clear, there's not some other definition out there.

To the extent that you asked whether two submarine cables would be -- I'm sorry, I just want to make sure.

BY MR. ABDO:

Q Whether an international submarine cable that connects two stations is a circuit.

A Yeah.

MR. PATTON: Same objection.

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. Is an international submarine cable that connects two stations a circuit on the Internet backbone?

MR. PATTON: Object to the form, vague. Objection to the extent it calls for expert testimony.

THE WITNESS: Say it one more time.

BY MR. ABDO:

Q Do you want me to repeat that?

A Yes, please.

Q Sure. Is an international submarine cable that connects two stations a circuit on the Internet backbone?

MR. PATTON: Objection to the extent it calls for expert testimony.

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. Is each optical fiber within an

international submarine cable that connects two stations a circuit?

MR. PATTON: Objection. Same objection as before.

THE WITNESS: Each of these is an example of what might be a circuit and what might be considered the Internet backbone.

So to the extent an optical fiber is given as an example of a circuit, then the answer would be yes, but they're an example.

BY MR. ABDO:

Q That's right. I'm not asking -- let me try to be clear.

A Okay.

Q Each of these questions is asking whether a particular data transmission line connecting two stations constitutes a circuit. I'm not asking for you to confirm that that's the only sort of circuit out there.

A Okay.

Q So I am asking whether these are examples of a circuit, not whether they are the

sum total of what might be a circuit.

A Okay.

Q With that understanding, is your answer to my last question -- what is your answer to my last question, which was is each optical fiber within an international submarine cable that connect two stations a circuit?

MR. PATTON: Objection to the extent it mischaracterizes the prior testimony. Objection, calls for expert testimony.

THE WITNESS: Circuit could -- the definition of "circuit" being two stations, instruments transmitting information, could be an example of -- could be an example. So it could be, yes.

BY MR. ABDO:

Q When you say it could be, you're referring again to an optical fiber within an international submarine cable?

A Yes, it could be.

Q If an optical fiber within an international submarine cable has been

multiplexed, would each of the subdivisions created by that multiplexing be a circuit?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: It could be.

BY MR. ABDO:

Q In what circumstance would it be, and in what circumstance would it not be?

A I'm trying to think if there's an example where it wouldn't be. I think the definition --

MR. PATTON: Same objection to that question and this line of questioning.

THE WITNESS: Yeah. So a telecommunications expert would undoubtedly consider it to be a circuit.

BY MR. ABDO:

Q Would the NSA also consider it to be a circuit?

A To the extent that there's no --

MR. PATTON: Object. Objection to the form to the extent it calls for expert testimony.

THE WITNESS: To the extent that there's no difference in the definition that NSA takes versus what a telecommunications expert takes, there's no special meaning to the word "circuit." So if they would consider it to be a circuit, then NSA would consider it to be a circuit.

BY MR. ABDO:

Q Okay. Can a single circuit span multiple physical paths between two stations?

MR. PATTON: Objection, vague. Objection, calls for expert testimony.

THE WITNESS: Can a single --

BY MR. ABDO:

Q Can a single circuit span multiple physical paths between two stations?

And I understand you'll make the same objections.

MR. PATTON: Same objections. And I would just add beyond the scope of 30(b)(6), and therefore the witness will be testifying in her personal capacity as opposed to her 30(b)(6)

designee capacity.

MR. ABDO: Rodney, if it's okay with you, can we shorten that objection to it's beyond the scope?

MR. PATTON: As long as you understand that what that means here is that she's testifying as Becky Richards and not testifying as a 30(b)(6) witness for the NSA.

MR. ABDO: Thanks. I will so understand it.

THE WITNESS: And I will --

BY MR. ABDO:

Q Let me restate the question.

A I've now lost what the question is as Becky answering.

Q Let me restate it, okay?

Can a single circuit span multiple physical paths between two stations?

MR. PATTON: Objection, calls for expert testimony. Objection, beyond the scope of 30(b)(6).

THE WITNESS: I'm going to answer I

don't know.

BY MR. ABDO:

Q Do you know whether there's anybody else at the NSA who would know the answer to that question?

MR. PATTON: You can answer if you have an unclassified --

THE WITNESS: I don't know.

BY MR. ABDO:

Q You don't know whether there's somebody else at the NSA who would know the answer to that question?

A Correct.

Q Did you talk to any subject matter experts at the NSA about the meaning of the term "circuit" prior to this deposition?

A I did.

Q As part of that conversation, did you do anything beyond reviewing the definition of "circuit" provided by the NSA in response to our Interrogatory No. 2?

MR. PATTON: Objection, vague.

THE WITNESS: We discussed generally what is meant by "circuit" in the context of a telecommunications expert.

We did not get to the specific whatever you just asked of a single circuit having multiple physical paths.

BY MR. ABDO:

Q Okay. What's your understanding of the term "virtual circuit"?

MR. PATTON: Object to the form, calls for expert testimony, and beyond the scope of 30(b)(6).

THE WITNESS: As described in the -- are we still on the interrogatories on page 6 in response to No. 2?

BY MR. ABDO:

Q Yes. Let me try to be clear.

What is your understanding of the term "virtual circuit" as used by the NSA in its response to Interrogatory No. 2?

A My understanding is that there's a way in which to use different techniques to divide the

circuits so that you have more than one -- multiple circuits on one circuit.

Q Let me just try to understand that.

Do virtual circuits -- let me start over. Can a virtual circuit traverse multiple physical circuits?

MR. PATTON: Objection to the extent it calls for expert testimony, and beyond the scope of 30(b)(6).

THE WITNESS: I'll respond I don't know.

BY MR. ABDO:

Q Is there anyone at the NSA who would know the answer to that question?

A I don't know.

Q Did you talk with any subject matter experts at the NSA about the definition of or the meaning of the term "virtual circuit" as used in the NSA's response to Interrogatory No. 2?

A I did.

Q Is there anything about the meaning of the term "virtual circuit" that you can provide

beyond what is in the NSA's response to Interrogatory No. 2?

A Since I'm not the telecommunications subject matter expert, my answer is confined to what you see on the piece of paper.

Q Is there a telecommunications subject matter expert at the NSA who could more fully answer that question?

Let me restate the question.

Is there anyone at the NSA who could more fully define what the term "virtual circuit" means as used by the NSA in response to Interrogatory No. 2?

MR. PATTON: To the extent that the answer is yes or no, she can answer, but I'll note for the record that she's testified multiple times that the NSA does not mean anything different by the term "virtual circuit" other than what is understood within the telecommunications industry.

BY MR. ABDO:

Q What is the meaning of "virtual circuit" as understood within the

telecommunications industry?

MR. PATTON: I'm going to object to the question to the extent it calls for expert testimony, and beyond the scope of 30(b)(6).

BY MR. ABDO:

Q You can answer.

A I don't have anything further to define for you.

Q Is there anyone at the NSA who better understands the definition of "virtual circuit" as used by those in the telecommunications industry?

MR. PATTON: You can answer the question if it's unclassified.

THE WITNESS: I don't know.

MR. PATTON: You can't provide a name.

THE WITNESS: I don't know.

BY MR. ABDO:

Q You don't know whether there's anyone at the NSA?

A Correct.

Q It's true -- well, let me ask you.

Is it true that each Internet protocol

packet sent on the Internet is routed to its destination independently?

MR. PATTON: Object to the form of the question to the extent it calls for expert testimony, and outside the scope of 30(b)(6).

You can answer.

THE WITNESS: I'm sorry, can you ask the question again?

BY MR. ABDO:

Q Sure. Is it true that each Internet protocol packet sent on the Internet is routed to its destination independently?

MR. PATTON: Same objections.

THE WITNESS: Generally speaking, yes, that is my understanding.

BY MR. ABDO:

Q Are there circumstances you can think of where Internet protocol packets would not be routed independently on the Internet?

MR. PATTON: Object to the form to the extent it calls for expert testimony, and beyond the scope of 30(b)(6). You can answer.

THE WITNESS: Not off the top of my head, but I'm sure there are examples.

BY MR. ABDO:

Q Why are you sure there are examples?

A Just because every rule seems to have some sort of exception to it, so to say something is hard and fast to be always the case is not something I would like to do.

Q Okay. When Internet packets that constitute a single communication take different paths to a common destination, are those packets traversing different circuits or the same circuit?

MR. PATTON: Object to the form, lacks foundation, object to the vagueness of the term "single communication." Object that it calls for expert testimony, and it is beyond the scope of 30(b)(6). You can answer.

THE WITNESS: The question was if packets take a different path, are they on different circuits?

BY MR. ABDO:

Q Yes.

A I would say it depends. There's not, again, a hard and fast rule. Depending, it might be on the same circuit, it might be on a different circuit.

Q What does it depend on?

MR. PATTON: Same set of objections.

THE WITNESS: I guess it would depend on how -- what would it depend on?

It would depend on the nature of the circuit.

BY MR. ABDO:

Q What do you mean by the nature of the circuit?

MR. PATTON: Same objections.

THE WITNESS: Depending on how the packets were going and how you -- how is it routed? Do they take different paths, or are they on the same circuit?

So to the extent the circuit can be meant in a big sense or in a small sense, it's going to decide whether it's on the same circuit or not.

So you asked in a separate set of line, had a whole bunch of distinctions as to what was data transmission line and what were they, and was it a wavelength, or something further into that. So it will depend on how you define "circuit," which is why you were asking me to define "circuit."

BY MR. ABDO:

Q Let me just try to understand.

Does the answer to my question depend on whether the separate paths being taken by packets are being routed over one physical circuit or not?

MR. PATTON: Same set of objections.

THE WITNESS: One physical circuit?

BY MR. ABDO:

Q Suppose two packets that are part of the same communication traverse different optical fibers.

A Okay. Are those different circuits?

Q Yes, that's my question.

MR. PATTON: Object to the extent it

calls for expert testimony in a hypothetical, and also beyond the scope of 30(b)(6).

THE WITNESS: So --

MR. PATTON: Also asked and answered.

THE WITNESS: So if it's on two different circuits, then it's on two different circuits. I feel like I'm having a circular conversation, so I'm not sure. Can two packets be on the same circuit and take different paths?

MR. PATTON: I don't think that's the question.

THE WITNESS: Is that --

BY MR. ABDO:

Q My original question was whether packets that are traversing different paths to their common destination are traversing different circuits. And I believe, please correct me if I'm wrong, you said, generally, yes.

MR. PATTON: That's a misstatement of her prior testimony.

BY MR. ABDO:

Q Could you please tell us what your

answer is to that original question?

MR. PATTON: Do you want the question to be read back?

MR. ABDO: No. I mean, let's move on.

Would you mind, Ms. Jaques, marking this as Exhibit 43?

(Deposition Exhibit 43 was marked for identification.)

BY MR. ABDO:

Q So you have in front of you what's been marked as Exhibit 43.

Do you recognize that document?

A Absolutely.

Q And what is Exhibit 43?

A Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2nd, 2014.

Q What was the NSA's relationship to the drafting or review of the report marked Exhibit 43?

MR. PATTON: Objection as vague, and

objection to the extent it may call for deliberative process privilege that might be invoked by the PCLOB that we don't represent. So maybe if you could ask a more narrow question, we can avoid most of the deliberative process.

She can speak in general terms on that, that would be good, in answer to your question, but I don't want to too broadly object on deliberative process grounds to protect PCLOB's privilege.

BY MR. ABDO:

Q Let me ask a different related question. Was the NSA involved in the drafting of Exhibit 43?

MR. PATTON: Objection, vague.

THE WITNESS: NSA provided expert testimony to the Board as is described on page 4 of the report. We provided documentation, we provided presentations, and we answered questions throughout their process.

We then for the fact section reviewed -- we reviewed the document for factual

accuracy, as well as we reviewed the entire document for classification to ensure there was no classified material in it.

BY MR. ABDO:

Q So I believe that you said that the NSA provided testimony, documentation, and presentations to the members of the PCLOB in drafting Exhibit 43, right?

A That is correct.

Q Do you know how many sessions the NSA provided testimony about the subject matter of the report that's marked Exhibit 43?

A It was a handful. I don't remember the exact number, but certainly they came to NSA, and we went to the PCLOB a number of times, both ways. We had conference calls, and we had email exchanges.

Q And did that testimony involve both classified and unclassified information?

A Yes, it did.

Q Is the same true of the documentation that the NSA provided to the PCLOB?

A Yes, it was both classified and unclassified.

Q And is that also true of the presentations provided?

A Yes, all was classified and unclassified.

Q And you say that the NSA reviewed the factual section of the report marked Exhibit 43 for accuracy; is that correct?

A That is correct.

Q When you say "fact section," what specific pages are you referring to, or page range are you referring to?

A Page 16 to 79. In essence, Part 3, Description and History.

Q Did the NSA review any other portion of the report marked Exhibit 43 for factual accuracy?

MR. PATTON: Objection to the form, vague as to time.

THE WITNESS: NSA otherwise did a classification review of the document.

To the extent these documents have the opinions of the various board members, NSA was not reviewing that information beyond ensuring there was no classified material in it.

BY MR. ABDO:

Q If the NSA, during its classification review of the portions of the report, other than Part 3, noticed a factual inaccuracy, would the NSA have notified the PCLOB of that inaccuracy?

A NSA conducted a classification review of the document. As part of that classification review, to the extent that something would be described in some of the other pieces of the document that was not not, we would notify them as part of that, as is noted again on page 4.

Q Let me just make sure I understand.

A Yeah.

Q The NSA reviewed Part 3 of the report marked Exhibit 43 for accuracy, right?

A That is correct.

Q It reviewed the entire document for classification, right?

A Correct.

Q And if in the process of reviewing the entire document for classification it noticed an inaccuracy outside the portion that it reviewed solely for accuracy -- sorry, outside the portion that it reviewed when it was conducting its review for accuracy, your testimony is that the NSA would have notified the PCLOB of that inaccuracy?

A Correct.

Q Was the NSA's review for accuracy of the factual section of the report thorough?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q The NSA would have reviewed every sentence?

A Absolutely.

Q And what would the NSA have done if it noticed an inaccuracy in any portion of the report?

MR. PATTON: Objection, vague.

THE WITNESS: NSA would provide a

response explaining either why it was inaccurate or why the information in the classification review was classified, and there was -- as is important to remember in the Upstream, large portions of that program remain classified, and so necessarily with this report, with this NSA Civil Liberties and Privacy Office Report, the information is incomplete.

And so a lot of the conversation was a mixture of how do you provide an accurate representation of how Upstream works while keeping the sources and methods classified? And so a lot of the conversation, particularly around the accuracy and the classification, were tied together because of those reasons.

And so this gives, as does our report, and continues to, a broad accurate description of the outline of how the program runs, but does not get into some of the much more specific aspects to it.

BY MR. ABDO:

Q In the course of the review for

accuracy of the report, did the NSA notice inaccuracies and make recommendations to the PCLOB about how to fix those inaccuracies in what's now marked Exhibit 43?

A Yes.

Q Are you aware -- sorry, strike that.

Did the PCLOB generally accept those recommendations?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Could you read the question back?

(The reporter read back the question.)

MR. PATTON: Just object to beyond the scope of the 30(b)(6).

And if the answer to that question is yes or no, you can answer. If the answer to that question is going to be a narrative description of what the PCLOB did or did not accept, then we're concerned that we might be in the deliberative process.

MR. ABDO: I just want to state for

the record, Rodney, you don't represent the PCLOB, correct?

MR. PATTON: I do not, but I am with the Department of Justice, and we do represent the United States, so here we would be preserving their ability to later assert that privilege if need be. I certainly am not in a capacity to waive it on their behalf.

MR. ABDO: I'm just not sure you're in a position to assert it though. I'm not sure we're asking for anything that's going to reveal the deliberations anyway, but I note that we object to your quasi-invocation of the PCLOB's deliberative process.

MR. PATTON: I can rephrase it as a preservation of their right to assert the deliberative process privilege, since they are not here to invoke that themselves.

MR. GILLIGAN: I would add that our function as Department of Justice attorneys is to represent the interests of the United States in this proceeding, and PCLOB is an independent

establishment of the United States government, but I understand your objection.

MR. ABDO: Sure, but you also know that we had -- you know, Topic 6 very clearly included this report as a subject of this deposition.

MR. PATTON: I doubt, again, that you will be delving into the details of that. There's an awful lot --

MR. GILLIGAN: The facts, not recommendations.

MR. PATTON: There's an awful lot of questions that the witness is perfectly capable of answering, so I don't think we're going to be in any --

BY MR. ABDO:

Q Ms. Richards, can you answer the question?

A Yes, I'll answer the question.

What I would do is point you to, again, page 4 that specifically says that they considered the Intelligence Community's comments

regarding the operation of the program to ensure accuracy. None of the changes resulting from that process affected the Board's substantive analysis and recommendations.

So I would point you to that to avoid this whole conversation about what is or isn't sort of privileged between it to say that they accepted our changes, they didn't change substantively what they were doing. We went through a back-and-forth to ensure that everybody understood how the program worked, what was classified.

In some instances, they asked for information to be declassified in order to make the record full, and that didn't change. So we went through that process.

Q Let me ask my question again because I don't think that answered it.

A Sure, okay.

Q If the NSA identified an inaccuracy in the report marked as Exhibit 43 to the PCLOB, would the PCLOB generally fix that factual

inaccuracy, generally have fixed it?

MR. PATTON: Object to the form, vague.

THE WITNESS: Yes. The PCLOB was not interested in having an inaccurate description of how Section 702 -- it was not within -- they didn't want to have that, and so they worked closely with us to ensure that they -- I don't know if "closely" is the right word, but they worked with us extensively in order to ensure that they had an accurate representation that could be made unclassified, which was -- up until -- there had -- the record had been not as extensive.

BY MR. ABDO:

Q Okay. Are you aware of any inaccuracies, factual inaccuracies, in the report marked as Exhibit 43?

MR. PATTON: Object to form, vague.

THE WITNESS: If there's particular sentences you would like me to look at or there's particular questions that you have, I'd be happy to look at those and walk through.

As a general matter, the information in here is accurate as a description, but necessarily, as I mentioned before, not a full description of the program because many of those facts still remain unclassified. But if there's particular sentences that you would like to point me to, I'm happy to review.

I would also note that, as of 2017, NSA changed one of the ways it was doing its collection, so it was no longer getting "abouts" collection. And so to the extent the material in here accurately reflects what was happening in 2014, the general matter, there may be, you know, slight, slight differences, but this is true.

That information has changed, so we are no longer doing a collection that gets the, quote, "abouts" collection in upstream. So to the extent that that's no longer accurate, that would be the case.

BY MR. ABDO:

Q But at least as the NSA was conducting upstream surveillance as of July 2nd, 2014, which

is the date of that report, you're not aware of inaccuracies in the report?

A Again, I would ask --

MR. PATTON: Sorry, just object to asked and answered. Go ahead, you can answer.

THE WITNESS: Again, if there are specific sentences you would like me to go to that you think maybe are not accurate, I'm happy to talk about those particular sentences. It's a 191-page document.

As a general matter, NSA considers this to be an accurate outline of the unclassified portions of Upstream. There may be particular sentences as they describe them, but the facts we believe to be accurate.

BY MR. ABDO:

Q Okay. I want to turn your attention to page 36 of the report marked Exhibit 43. Could you please read the first sentence of the very last paragraph that starts on that page? It begins "once tasked." Again, that's at the bottom of page 36 of Exhibit 43, and that sentence ends

on the next page, 37.

A Okay, yes.

Q Is that sentence factually accurate?

MR. PATTON: Object to the form, vague.

BY MR. ABDO:

Q As of the time -- let me start over.

Is the sentence that I just asked you to read at the bottom of page 36, carrying over onto page 37 of Exhibit 43, an accurate description of how upstream surveillance operated as of July 2nd, 2014?

A Well, what I would do is I would point you, rather than to the sentence that's on page 36 of the PCLOB report, and instead suggest that the RFA, Request for Admission, on page 9, in response to RFA for No. 8, that describes how this is -- how the government describes it.

The other place I would suggest, which is the government's description, is also in the NSA Civil Liberties and Privacy Office Report at page 5.

Those are both more accurate descriptions of how we would talk about Upstream. The description on page 36 is necessarily vague.

Q What's inaccurate about the sentence at the bottom of page 36, carrying over onto page 37, in Exhibit 43?

MR. PATTON: Objection, mischaracterizes prior testimony. And just a second, there might be a classified response.

We will need to find out what her answer is going to be on this to determine whether the answer is partially classified, fully classified, or wholly unclassified. At this point, I don't know what her answer is going to be.

MS. HANLEY COOK: Why don't we take a five-minute break.

MR. ABDO: Go off the record, Dawn, please.

(Off the record at 11:30 a.m.)

(Resume at 11:56 a.m.)

MR. ABDO: Ms. Jaques, do you mind

reading back the last question before we broke?

(The reporter read back the question.)

MR. PATTON: Objection to the extent it misstates prior testimony, and objection to the extent that the answer calls for classified information and information subject to the statutory privileges.

You can answer to the extent your answer is unclassified.

THE WITNESS: Okay. So this sentence, as I mentioned about the entire document and the sort of public description of Upstream, is necessarily incomplete because of the classification of information.

This sentence is accurate as of 2014, but I would point you to the description that's provided in the RFA, Request for Admission No. 8, in the response. That provides an accurate description of how upstream Internet collection works today, with, again, the understanding that it's necessarily incomplete.

To provide you a description of what

is different between those two and why necessarily gets into the classified realm, and so I can't go any further into that.

BY MR. ABDO:

Q Let me just make sure I understand.

A Yep.

Q Is it true that the sentence we've been focusing on, the carryover sentence between pages 36 and 37 of Exhibit 43, is accurate as of 2014?

MR. PATTON: Objection, mischaracterizes prior testimony.

THE WITNESS: It is accurate, but incomplete, and that's a very important fact.

BY MR. ABDO:

Q And the reasons why it is incomplete you are saying are classified; is that correct?

A That is correct.

Q Is it incomplete because it omits additional information about the operation of upstream surveillance that is classified?

MR. PATTON: Let me just check to find

out whether the answer is yes or no.

(Counsel conferring.)

THE WITNESS: Ask your question one more -- can you repeat the question for me?

BY MR. ABDO:

Q I can ask it again.

Is the sentence that carries over between pages 36 and 37 of Exhibit 43 incomplete, which is the word you used --

A Correct.

Q -- because it omits information about the operation of upstream surveillance that is classified?

MR. PATTON: Just a second.

You can answer yes or no.

THE WITNESS: Okay, yes.

BY MR. ABDO:

Q Is it incomplete for any other reason other than that it omits additional information that is classified about the operation of upstream surveillance?

MR. PATTON: Object to form, but you

can answer.

THE WITNESS: It is incomplete because it omits classified information.

I'm not sure I understood your second question, what you were trying to -- what my other -- what other options you're providing for.

BY MR. ABDO:

Q A statement could be incomplete for a number of reasons. It could be incomplete because it omits relevant information, it could be incomplete because it includes information that is inaccurate or misleading, and I'm trying to understand why the NSA believes this sentence is incomplete?

A It's incomplete because it omits the classified information.

Q And for no other reason?

A Not that I can think of. I'm pausing because I can't -- I guess maybe you can be more specific, but I guess you said I could have added more information in -- they could have added more information into it and that's what makes it

incomplete? I'm not sure I understand. I guess I don't understand beyond omitting.

I'm willing say to say it's incomplete because it's omitting information. I'm not sure I understand the remainder of what you're trying to get at, so maybe you can rephrase it.

Q Let me ask it another way.

Is any of the information included in this sentence -- again, the sentence carrying over from pages 36 to 37 of Exhibit 43 -- inaccurate?

MR. PATTON: Objection, vague as to time.

MR. ABDO: As to the operation of upstream surveillance in 2014.

THE WITNESS: As I've said, it's incomplete.

BY MR. ABDO:

Q I'm asking if it's inaccurate.

A No. I've stated it's accurate. It's just incomplete.

Q Is it inaccurate as to the operation of upstream surveillance today?

MR. PATTON: Objection, calls for information that is classified and subject to the state secrets privilege, the other statutory privileges. I instruct the witness not to answer the question.

BY MR. ABDO:

Q Are you going to follow your lawyer's instruction not to answer?

A I'm going to follow my lawyer's direction not to answer.

Q Do you know the answer to the question that I asked? In other words, if you were to answer, could you?

A It would be classified, so I can't answer it because it's classified.

Q But do you know the information that you would provide in response but for --

A The classification?

Q Yes.

A Yes.

Q Is there anything you can say in response to the question without revealing

information you've been instructed not to provide?

A I would point you to the answer to the response that's on page 9 of the RFA, which accurately, to the extent possible given the classified nature, describes the current way Upstream works. And so I would -- that's how I would answer.

Q But specifically with respect to this sentence, is there anything you can say in response to my question, which was is the sentence accurate as to the operation of upstream surveillance today?

Is there anything you can say, aside from pointing me to other testimony or other information, that would not require you to disclose classified information?

A No.

Q Can you describe -- well, let me ask you this. Do you agree with your lawyer's instruction that answering the question would harm national security?

MR. PATTON: I'm going to object to

the form of the question as it seeks a legal conclusion, and as my colleagues just pointed out, beyond the scope of 30(b)(6).

MR. ABDO: You should take a look at guideline 7 of Appendix A of the local rules, which clearly contemplates counsel asking for the basis of assertions of privilege.

So my question is --

MR. PATTON: Same objection. That calls for a legal conclusion.

BY MR. ABDO:

Q Do you believe that answering the question would result in harm to national security?

A Yes.

Q Can you describe that harm?

MR. PATTON: No. I'm going to object to that question, as it would call for classified information and information subject to the statutory privileges, and I'll instruct her not to answer the question.

BY MR. ABDO:

Q Do you agree that describing the harm would itself result in harm to national security?

A Yes.

Q Have you discussed the invocation of the state secrets privilege with respect to this question with Admiral Michael Rogers?

MR. PATTON: With respect to this particular question?

MR. ABDO: Yes.

THE WITNESS: The question being -- I'm sorry, so just explain to me. The question is whether describing the difference between the sentence on page 36 and the interrogatory -- or the Request for Admission on page 9, whether describing what is different between those two would be a national security harm with him specifically?

BY MR. ABDO:

Q No. The original question was whether the carryover sentence from page 36 to 37 of Exhibit 43 is accurate with respect to upstream

surveillance as it is conducted today.

Have you discussed with Admiral Rogers whether answering a question seeking that information requires invocation of the state secrets privilege?

MR. PATTON: You can answer the question.

THE WITNESS: No, I have not.

BY MR. ABDO:

Q Have you more generally discussed the invocation of the state secrets privilege in this deposition with Admiral Rogers?

A I spoke to him extensively prior to the issuance of both the NSA Civil Liberties and Privacy Office Report, as well as the PCLOB Report, for him to understand what information was going to be in that.

So whether for today's testimony -- I did not go back to him and ask him specifically about any of this information, as that had largely been covered when we were issuing those reports back in 2014.

Q Okay. Is there anything else you can tell us about this assertion of the state secrets privilege?

MR. PATTON: Objection, vague.

THE WITNESS: I don't know what you're asking me.

BY MR. ABDO:

Q Is there anything that you can say that would be unclassified about the nature of the state secrets privilege invocation, or the reason for it, or the harm that would come about by answering the question?

A No, other than to say that this is sources and methods. You're getting into sources and methods, which is what we have -- we protect extensively.

Q Okay. As of 2014, did the NSA conduct upstream surveillance on at least one Internet backbone circuit?

MR. PATTON: Object to the question to the extent it calls for a classified answer, subject to the state secrets privilege, prior

statutory privileges.

You can answer the question to the extent not classified.

THE WITNESS: The question is at least one?

BY MR. ABDO:

Q Internet backbone circuit.

A One Internet backbone circuit.

MR. PATTON: This is probably another one of those questions where a yes-or-no answer would be unclassified, but --

MR. ABDO: That's what I'm looking for, a yes or no.

MR. PATTON: Any narrative answer we would have to break for.

THE WITNESS: At least one Internet --

BY MR. ABDO:

Q Let me restate the question.

A Okay.

Q As of 2014, did the NSA conduct upstream surveillance on at least one Internet backbone circuit? Yes or no.

MR. PATTON: Same classified objections to the extent that the question seeks classified information. To the extent it's yes or no, you can answer the question.

THE WITNESS: Yes.

BY MR. ABDO:

Q As of 2014, did the NSA conduct upstream surveillance on more than one Internet backbone circuit?

MR. PATTON: Object to that question to the extent it calls for classified information protected by the state secrets privilege, statutory privilege.

Instruct the witness not to answer the question.

THE WITNESS: I will follow my lawyer's direction.

BY MR. ABDO:

Q Your view is that stating a yes in response to that question or a no in response to that question would disclose state secrets?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: Still following my lawyer's description -- direction.

BY MR. ABDO:

Q Is --

MR. GILLIGAN: Excuse me, Counsel, just one moment.

MR. ABDO: Yeah, sorry.

(Counsel conferring.)

BY MR. ABDO:

Q Is your view that the sentence we've been discussing between pages 36 and 37 of Exhibit 43 discloses any classified facts or facts protected by the statutory authorities your counsel has cited?

A The sentence is unclassified.

Q Is that true notwithstanding the fact that the sentence states that upstream surveillance involves the acquisition of communications transiting through circuits -- that's a quote -- on the Internet backbone?

MR. PATTON: Object to the form of the

question, vague as to time.

MR. ABDO: As of 2014.

MR. PATTON: Same objections, vague as to time.

THE WITNESS: My answer remains the same.

BY MR. ABDO:

Q What's your answer?

A That the fact that the word "circuits" is plural does not change any of my previous answers.

Q You don't view that as inconsistent with the assertion of the state secrets privilege in response to my question of whether, as of 2014, upstream surveillance involved more than one Internet backbone circuit?

MR. PATTON: Objection, asked and answered, argumentative. Go ahead.

THE WITNESS: I don't see that as inconsistent.

BY MR. ABDO:

Q Why not?

MR. PATTON: Same objections.

THE WITNESS: As we've stated, we've stated that we were on at least one, and the fact that there's a plural there isn't dispositive one way or the other.

BY MR. ABDO:

Q As of 2014, were multiple electronic communication service providers compelled to assist the NSA in the operation of upstream surveillance?

MR. PATTON: Objection, calls for classified information, sources and methods, operational details, and subject to state secrets and statutory privileges.

I instruct the witness not to answer the question.

THE WITNESS: I will follow my lawyer's --

BY MR. ABDO:

Q Can you please turn to page 12 of what's marked Exhibit 43 and read, if you would, what is marked as Recommendation 6, which is the

final paragraph of page 12.

MR. PATTON: Read it to herself or out loud?

MR. ABDO: To yourself, yeah.

THE WITNESS: Yes.

BY MR. ABDO:

Q Do you understand -- well, strike that.

Is it true that in the operation of upstream surveillance in 2014, there were -- and I'm quoting from this recommendation -- affected telecommunication service providers?

MR. PADGETT: Could you read back the question?

(The reporter read back the question.)

MR. PATTON: I'm going to object to vagueness in terms of time, and object to the question to the extent it calls for classified information, sources and methods information protected by the statutory privileges.

The witness can answer the question to the extent unclassified.

BY MR. ABDO:

Q Let me specify with respect to time that I'm talking about July 2nd, 2014, the date of this report.

MR. PATTON: Same objections.

THE WITNESS: I'd like to go in the SCIF before I answer this question.

MR. PATTON: Okay.

MR. ABDO: Take a break.

(Off the record at 12:16 p.m.)

(Resume at 12:19 p.m.)

MR. PATTON: Same objections.

THE WITNESS: So as I said earlier, providing any information as to the number of telecommunication service provider beyond one is classified. Because this is temporally at one point, we can neither confirm nor deny that information, whether it was more than one. To the extent there was more than -- to the extent there is a program, there must be one.

BY MR. ABDO:

Q Can you tell us whether there have

been more than one provider involved, even if not more than one at the same time?

MR. PATTON: Objection, calls for classified information pursuant to the state secrets privilege. Instruct the witness not to answer, and to the statutory privileges.

THE WITNESS: I will follow my lawyer's direction.

MR. ABDO: Rodney, are you okay shortening that objection to something?

MR. PATTON: I'm trying.

MR. ABDO: Okay.

Ms. Jaques, do you mind marking this as Exhibit 44?

(Deposition Exhibit 44 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you have in front of you what's been marked as Exhibit 44. Do you recognize that document?

A Yes, I do.

Q Did you draft this document?

A I did.

Q What is the document?

A The document is the NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of Foreign Intelligence Surveillance Act, Section 702, dated April 16th, 2014. It's exactly four years old.

Q Did the NSA review this document for accuracy and classification?

A Did the NSA?

Q Yes.

A Yes, it did.

Q Was that review thorough?

A Yes, it was.

MR. PATTON: Objection, vague.

THE WITNESS: Sorry, too fast.

BY MR. ABDO:

Q What was the purpose of issuing this report?

A The purpose of issuing the report was to put on the public record a description from NSA's perspective of what the privacy protections

were in place as it relates to Section 702.

Q Was it important to the NSA in issuing Exhibit 44 that the report be accurate?

A Absolutely.

Q And why is that?

A Because this was submitted to the Privacy and Civil Liberties Oversight Board as part of their request for comment as part of their report on Section 702, and we wanted to put on the record an unclassified description that NSA stood behind as to how the program worked.

Q And was it also important that the report, to the extent publicly disclosed, not reveal classified information?

A Yes.

Q Could you turn to page 5 of the report, again what's marked as Exhibit 44? I want to direct your attention to the first sentence of the last paragraph of the page, which starts, "In the second."

A Mm-hmm.

Q Could you read that sentence to

yourself, please, and let me know when you're done.

A (Witness reviewing document.) Okay.

Q Is this sentence referring to upstream surveillance as it operated as of April 16, 2014?

A Yes, it is.

Q Does this sentence confirm that service providers, plural, are compelled to assist the NSA in the lawful interception of electronic communications to, from, or about task selectors as of April 16th, 2014?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PADGETT: Can you read back the question?

(The reporter read back the question.)

BY MR. ABDO:

Q Let me ask it differently.

Is this sentence accurate as of April 16, 2014?

A To the extent, as with the PCLOB report, it's necessarily incomplete. It is

accurate to the outline of how the program works.

Q When you say it's incomplete, is it incomplete because it omits classified information about the operation of upstream surveillance as of April 16, 2014?

A Yes.

Q Is it incomplete for any other reason?

A No.

Q Do you understand this sentence to confirm that service providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about task selectors as of April 16th, 2014?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: We need to take just, I promise, a very short break to make sure the answer is unclassified. Thanks.

(Off the record at 12:26 p.m.)

(Resume at 12:40 p.m.)

MR. ABDO: Do you mind reading back the last question to us, Ms. Jaques?

(The reporter read back the question.)

MR. PATTON: Objection, vague as to time, and objection to the extent it seeks classified and otherwise statutorily privileged information.

You can answer to the extent it's unclassified.

THE WITNESS: So this sentence -- here's the thing. Would it have been clearer if we had put parens between the S? Yes. But we're not here -- we can't confirm or deny whether -- we've said that there was one service provider, at least one service provider in Upstream. The fact that this is plural does not -- is not an indication that it was more than one at that point in time or less than one at that point in time.

And so this is just -- it probably would have been clearer if we had put the parens. We didn't put the parens, so you've found the S's in our report, but it's not meant to have provided classified information, the fact that the numbers are classified.

BY MR. ABDO:

Q You understand that at the time that this report was issued -- and for the record, we're talking about Exhibit 44 -- there was a relatively small amount of unclassified information available from the government about the operation of upstream surveillance, right?

MR. PATTON: Objection, vague.

THE WITNESS: Yes, that's why I wrote the report.

BY MR. ABDO:

Q And you understand that the public and the PCLOB, which received this report, would regard it as an authoritative source of public information from the government about the operation of upstream surveillance?

MR. PATTON: Objection, calls for speculation about others and their thought processes.

THE WITNESS: Yes.

BY MR. ABDO:

Q And that was precisely one of the

reasons that you drafted it and disclosed the report, right?

A Correct.

MR. PATTON: Objection.

BY MR. ABDO:

Q Were you careful throughout to ensure that the factual assertions in this report were accurate?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q And was that in part at least so as not to mislead the public or the PCLOB as to the operation of upstream surveillance at the time the report was issued?

A Yes.

Q Did you take great care throughout the rest of the report in every word used to ensure that what the words conveyed were accurate and unclassified?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q Was this sentence reviewed with that same level of care?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q Are you aware of any factually incorrect statements in Exhibit 44 as to the operation of upstream surveillance at the time that the report purports to describe the operation of upstream surveillance?

MR. PATTON: Objection, ambiguous.

MR. ABDO: I'm sorry, I didn't hear.

MR. PATTON: Objection, ambiguous.

THE WITNESS: Again, to the extent that the information in here is unclassified, and therefore is necessarily incomplete, yes, this is an accurate description.

This was also really one of the first times that the NSA had written, so to the extent we've gotten better at this as we've gone along, the first time is always -- we were doing our

best.

BY MR. ABDO:

Q Setting aside the question of incomplete information, are you aware of any factual inaccuracies in Exhibit 44 as to the operation of upstream surveillance at the relevant time periods described in the report?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Go ahead.

THE WITNESS: No, I'm not.

BY MR. ABDO:

Q Also setting aside the question of incompleteness, are you aware of any factual inaccuracies in Exhibit 43, the report of the PCLOB, as to the operation of upstream surveillance for the periods of time described in that report?

MR. PATTON: Objection, vague.

THE WITNESS: As I said earlier, and as we just then described going through these different sentences, the answer is I am not

generally aware of any inaccuracies.

To the extent you have a question about a particular sentence, I'm happy to, as we did on page 36, walk you through and understand whether there was classified information that makes that sentence more or less complete.

BY MR. ABDO:

Q I appreciate that, and we may do that for a few more sentences, but my question is whether, as you sit here today, you are aware of any inaccuracies, factual inaccuracies, in Exhibit 43 with regard to the operation of upstream surveillance as the report describes?

MR. PATTON: Objection, asked and answered.

THE WITNESS: My answer is still the same. You know, the information in it is, generally speaking, accurate.

If there's a particular sentence you want to discuss -- it's necessarily incomplete, and describing Upstream, which is classified, in an unclassified sentence is difficult, as you're

seeing with us having to walk back and forth and make sure that we're hitting those lines so that we are providing an accurate general description of the program without going into the classified sources and methods of the program.

So, you know, it still remains accurate to the extent that it was true in 2014. I'll just re-remind you that we are no longer do the "abouts" collection as it was described starting in 2017, and so that piece of this report is not accurate.

BY MR. ABDO:

Q The report doesn't purport to describe surveillances operated years later, correct?

A Correct. I'm just re-reminding that to the extent that we've changed certain aspects of the program, that's no longer accurate.

Q Okay. I'm going to ask you similar questions that I just asked you about Exhibit 44, but about Exhibit 43.

Did the NSA, as it did with Exhibit 44, also review each and every factual

disclosure in Exhibit 43 to ensure that it was accurate?

MR. PATTON: Object to the form, vague, asked and answered.

THE WITNESS: To the extent that NSA scrubbed through the facts provided in the historical, as we mentioned, section from 16 to roughly 79, and also looked at from a classification purpose, yes.

We were, again, doing our best to try and help provide an unclassified description of a classified program, and so it was necessarily incomplete.

BY MR. ABDO:

Q And at the time that report was issued, is it also fair to say that there was relatively little public information from the government describing the operation of upstream surveillance?

MR. PATTON: Object to the form, vague.

THE WITNESS: I'm pausing because I

don't exactly remember when a number of the different FISC opinions were declassified. So I believe that there were a number of -- they were actually issued -- that they were declassified prior to -- or they were reviewed and redacted.

So Judge Bates -- which are mentioned. There are a number of reports that are footnoted in here that are -- that were declassified. I just -- some of the timing.

BY MR. ABDO:

Q Is it fair to say that at the time this report was issued, it was the most comprehensive description from the government of how upstream surveillance operated at the time the report was issued?

MR. PATTON: Objection, vague.

THE WITNESS: Yes, to the extent, though -- I would just offer that to the extent that these are the words of an independent executive agency with oversight over the Intelligence Community as it relates to CT functions, you know, these are their words.

They're not NSA's words. They're not NSA submissions.

And so sometimes they may describe things slightly differently than we may have chosen to do so, and so I would refer you back to the NSA or the government submissions on the descriptions of the programs.

BY MR. ABDO:

Q Okay. Is it fair to describe the report marked Exhibit 43 as an exhaustive description of upstream surveillance as it operated in 2014?

MR. PATTON: Objection, vague.

THE WITNESS: I suppose that's one. I'm guessing that you have something over there that -- are you referring to a specific document where NSA may have said that?

BY MR. ABDO:

Q Well, I'm asking you first whether that's fair, setting aside what the NSA has otherwise said?

A Yes, I think it's fair.

MR. PATTON: In unclassified terms.

THE WITNESS: In unclassified terms.

MR. PATTON: I guess that's probably what that's talking about, right?

MR. ABDO: Yeah, no, I think -- let me ask the question clearly.

Is the PCLOB's description of the operation of upstream surveillance exhaustive?

MR. PATTON: Same objection.

THE WITNESS: So, again, I think what I would say is I think that their study was exhaustive. To the extent that there's classified information, they had access to that information, which makes the study probably exhaustive, but to the extent that the report is necessarily incomplete, it's as much information as possible without going into the classified material.

BY MR. ABDO:

Q Okay. I want to ask you a question that I've tried different versions of, so forgive the repetition. I'm asking it multiple ways because I'm looking for what I think you ought to

be able to provide, which is a clean yes or no.

Setting aside the incompleteness of the report marked Exhibit 43, are you aware now of any factual inaccuracies in the report and its description of upstream surveillance as Upstream was conducted at the time the report was issued?

MR. PATTON: Objection, asked and answered. Go ahead.

THE WITNESS: I am not aware of any inaccurate -- known inaccuracies in the document as described other than the fact that there's classified information that has been omitted.

BY MR. ABDO:

Q What is the number, or approximate number, of Internet backbone circuits on which upstream surveillance is conducted --

MR. PATTON: Objection.

MR. ABDO: -- as of June 2015?

MR. PATTON: Objection, calls for classified information, sources and methods, operational details subject to state secrets and the statutory privilege.

Instruct the witness not to answer.

THE WITNESS: I will follow my lawyer's direction.

MR. ABDO: Rodney, I think it might be in our interest to come up with a shortened version of that, at least for the next few minutes.

MR. PATTON: Yes, you have my word.

BY MR. ABDO:

Q What is the number, or approximate number, of Internet backbone circuits on which upstream surveillance is conducted today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Still following those directions.

BY MR. ABDO:

Q Okay. What is the average bandwidth of the Internet backbone circuits on which upstream surveillance was conducted in June 2015?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Following the instruction.

BY MR. ABDO:

Q What is the average bandwidth of the Internet backbone circuits on which upstream surveillance is conducted today?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Still following the instructions.

BY MR. ABDO:

Q What is the approximate combined bandwidth of the Internet backbone circuits on which upstream surveillance was conducted in June of 2015?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Still following instructions.

BY MR. ABDO:

Q What is the approximate combined bandwidth of the Internet backbone circuits on

which upstream surveillance is conducted today?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What are the categories of circuits that were subject to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What are the categories of circuits that are subject to upstream surveillance today?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any individual optical fibers on the Internet backbone subjected to upstream surveillance in June 2015 and/or any individual optical fibers on the Internet backbone subjected

to upstream surveillance today?

MR. PATTON: Just a second.

MR. PADGETT: Could you read back the question?

MR. ABDO: Sure. Let me --

MR. PATTON: I really am listening to your questions.

BY MR. ABDO:

Q I appreciate that. In the interest of speed, I was combining two, but let me be clear.

Are any individual optical fibers on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any individual optical fibers on the Internet backbone subjected to upstream surveillance as of June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Are any subdivisions of optical fibers on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any subdivisions of optical fibers on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Are any wavelengths of light carried on optical fibers on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any wavelengths of light carried on optical fibers on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What is the smallest subdivision by bandwidth of an optical fiber on the Internet backbone that was subjected to upstream surveillance in June 2015 and that is subjected to upstream surveillance today?

MR. PATTON: Objection, compound. Objection, same as before, classified.

MR. ABDO: We might go quicker if you would withdraw the compound objection.

MR. GILLIGAN: I like this pace, actually.

BY MR. ABDO:

Q Let me rephrase the question.

What is the smallest subdivision by

bandwidth of an optical fiber on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What was the smallest subdivision by bandwidth of an optical fiber on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same instruction, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What was the largest circuit by bandwidth on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What is the largest circuit by

bandwidth on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Is now a good time for you to break, Ms. Richards?

A Sure.

Q Okay, why don't we take a lunch break and go off the record, Dawn.

(Lunch break taken at 12:59 p.m.)

(Resume at 2:06 p.m.)

BY MR. ABDO:

Q We're back from lunch.

Ms. Richards, what does the term "Internet link" refer to?

MR. PATTON: Objection, vague.

THE WITNESS: Is there a specific place where you want me to look for "Internet link," or are you looking for the general telecommunications definition?

BY MR. ABDO:

Q That's right, the general definition.

A So it's similar to a circuit, and there's no special NSA meaning.

Q So the NSA's understanding of that term is consistent with the general understanding of the term within the telecommunications industry?

A That is correct.

Q Okay. What does the term "international Internet link" refer to?

MR. PATTON: Objection, vague, calls for expert opinion.

THE WITNESS: I'm sorry, international --

BY MR. ABDO:

Q International Internet link.

A Is there, again, something specific? I'm not sure of it.

Q The question is whether that term has a meaning to the NSA.

MR. PATTON: Just a second.

I'm just going to object to the extent that any response might call for a classified answer, subject to state secrets, statutory privileges.

If the witness has an unclassified answer, she can provide it.

THE WITNESS: I'm just going to take a minute to make sure I --

(Witness reviewing document.)

So just for clarification, you're looking for the definition of "international Internet link" --

BY MR. ABDO:

Q That's right.

A -- as was originally described in Judge Bates' order?

Q I'm asking for your understanding of it, not for Judge Bates' understanding.

A Okay, I just want to make sure.

So I'll say there's no special NSA meaning.

Q What is the meaning of it though, even

if there's not a special NSA one?

MR. PATTON: Objection to the extent it calls for expert opinion, and to the extent it may call for classified information and statutory privileges.

The witness can answer if the answer is unclassified.

Are you concerned that there's --

THE WITNESS: I'm concerned whether I'm going into classified. I'm just trying to under- -- I'm clicking through my head as to what's classified and what's not classified, so I'm sorry I'm taking a little bit more, and so maybe --

MR. PATTON: Do you need to talk about that?

THE WITNESS: Maybe we should just take a quick minute, go off the record.

MR. ABDO: Okay.

(Off the record at 2:11 p.m.)

(Resume at 2:28 p.m.)

MR. ABDO: Ms. Jaques, do you mind

re-reading the last question asked?

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for expert testimony.

THE WITNESS: I'm going to clarify my answer, which is the logical definition of an international Internet link would be an Internet link between two countries, but it's not I think a well -- it's not a telecommunications -- unlike some of the other descriptions that we provided in terms of "circuit" or "cable" or "Internet backbone," this is not a commonly understood telecommunications word -- or set of three words, I guess.

BY MR. ABDO:

Q Okay. But your understanding of it is a link between two countries essentially?

MR. PATTON: Same objection.

THE WITNESS: Yes, in the broad context of those three words, not in the context of anything specific.

BY MR. ABDO:

Q Okay. I want to go back for a moment to Internet link -- not international Internet link, just Internet link.

You said, I believe, and please correct me if I'm wrong, that it is similar to a circuit. Is that correct? Am I characterizing your previous testimony accurately?

MR. PATTON: Object to the extent it calls for expert opinion.

THE WITNESS: Yes.

BY MR. ABDO:

Q When you say "similar" -- or when you said "similar," did you mean analogous to, or did you mean identical to? I'm trying to understand, if there are differences between an Internet link and a circuit, what you believe those differences to be.

MR. PATTON: Same objection.

THE WITNESS: I don't see them -- I see them as being analogous. So sometimes you use "circuit," sometimes you use "link." I don't see

them as having any real difference between them.

BY MR. ABDO:

Q Okay. Would "interchangeable" be a better word than "analogous" then?

A Yeah.

MR. ABDO: Ms. Jaques, would you mind marking this Exhibit 45?

(Deposition Exhibit 45 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you have in front of you what's been marked as Exhibit 45.

Do you recognize that document?

A I do.

Q What is it? I should say, sorry, it's marked Exhibit 45, and it is Bates numbered NSA-WIKI 149 to NSA-WIKI 229. Wiki is spelled W-I-K-I. What is this document, Ms. Richards?

A This is the Judge Bates' Memorandum Opinion from October 3rd, 2011.

Q Could you turn to page 45, or NSA-WIKI 193 of Exhibit 45, and read the sentence

that begins, "Indeed, the government readily concedes." It is about halfway down the page.

A Got it.

Q "Indeed, the government readily concedes that NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server."

Is that sentence true?

Let me rephrase that. Was that sentence true at the time Judge Bates issued this opinion?

MR. PATTON: Just a moment.

You can answer.

THE WITNESS: Okay. Yes, that sentence is accurate.

BY MR. ABDO:

Q What do you understand the Foreign Intelligence Surveillance Court to mean in its use of the term "international Internet link" in that sentence?

MR. PATTON: Objection, the question calls for classified information, information subject to the state secrets and the statutory privileges previously mentioned.

I instruct the witness not to answer the question.

BY MR. ABDO:

Q Do you --

A Hold on.

MR. PATTON: Do you have an unclassified response?

THE WITNESS: I have an unclassified response, at least in part.

MR. PATTON: So long as you're comfortable and it's unclassified.

THE WITNESS: NSA -- so unlike the other words that you had me go through in terms of definitions that were telecom provider -- you know, sort of generally what a teleco expert would be, NSA has an understanding of this term that is specific to how Judge Bates described it, but it's classified to provide any further information.

BY MR. ABDO:

Q I understand. Is the NSA's understanding of the term different from the general meaning of the term you described in response to an earlier question as a link between two countries?

MR. PATTON: Objection, calls for information subject to the statutory privilege, and instruct the witness not to answer the question.

THE WITNESS: I will follow instructions.

BY MR. ABDO:

Q Is it your understanding that in using the term "international Internet link," the Foreign Intelligence Surveillance Court meant an Internet link that terminates in a foreign country?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Is it your understanding that an international Internet link is an Internet backbone circuit with one end in the United States and the other end in a foreign country?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Is there anything you can tell us unclassified about the nature of the harm that would arise were you to provide an answer to the question of what the term "international Internet link" means as used by the Foreign Intelligence Surveillance Court in Exhibit 45?

MR. PATTON: Object to the question. The witness is not an official classification authority, nor is she the Director of the NSA or the Director of National Intelligence, who would invoke and assert the state secrets privilege to that.

You can answer the question to the

extent it's unclassified.

THE WITNESS: Sources and methods.

BY MR. ABDO:

Q Do you believe that disclosing the NSA's understanding of that term would harm national security?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Which was to not answer, or to answer to the extent --

MR. PATTON: To answer to the extent that you're able. You're not a classification authority, you're not asserting the state secrets.

THE WITNESS: So the question is whether I believe it would harm national security?

BY MR. ABDO:

Q Yes.

A Yes.

Q Do you believe it would substantially harm national security?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Yes.

BY MR. ABDO:

Q Are you familiar with the process through which the government seeks approval from the Foreign Intelligence Surveillance Court to conduct upstream surveillance?

MR. PATTON: Object to the form of that question as vague, and objection, beyond the scope of 30(b)(6).

THE WITNESS: Yes.

BY MR. ABDO:

Q Does the NSA provide information to the Foreign Intelligence Surveillance Court about the operation of upstream surveillance in support of the government's applications to that court to conduct upstream surveillance?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Is the information that the NSA provides in support of the government's applications to the Foreign Intelligence

Surveillance Court supposed to be accurate?

MR. PATTON: Objection. Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Is that information, in fact, accurate?

MR. PATTON: Objection, calls for speculation.

THE WITNESS: To the extent the government's job is to provide the Court with as accurate as information as possible at the time, that is what the NSA does.

BY MR. ABDO:

Q Does the NSA verify, under penalty of perjury, that its submissions to the Foreign Intelligence Surveillance Court are true and correct?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Does the NSA review the Department of

Justice's submissions to the Foreign Intelligence Surveillance Court seeking authority to conduct upstream surveillance?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Does it review the technical explanations of the way that upstream surveillance operates and drafts of those submissions before they are filed with the Foreign Intelligence Surveillance Court?

MR. PATTON: Same objections.

MR. PADGETT: Excuse me, could you read back the question?

(The reporter read back the record.)

THE WITNESS: Okay, yes.

BY MR. ABDO:

Q If there are mistakes in the drafts of the Department of Justice's submissions to the Foreign Intelligence Surveillance Court, would the NSA identify those mistakes to the Department of Justice?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q Would it identify any inaccuracies in the explanations of the technical operation or implementation of upstream surveillance to the Department of Justice?

A Yes.

MR. PATTON: Objection, vague and ambiguous, and also beyond the scope of 30(b)(6).

THE WITNESS: Yes.

BY MR. ABDO:

Q To your knowledge, does the Foreign Intelligence Surveillance Court acquire information about the operation of upstream surveillance from anyone aside from representatives of the NSA or the Department of Justice?

MR. PATTON: Objection, calls for speculation. Objection, beyond the scope of 30(b)(6).

THE WITNESS: What time frame would

you be asking about? Just in general? Over a specific time frame?

BY MR. ABDO:

Q Why don't we -- if you can answer in general, please do. If you can't, let me know.

MR. PATTON: Are you asking -- I'm sorry, does this include just Upstream?

MR. ABDO: Just Upstream.

MR. PATTON: Same objections.

THE WITNESS: To the extent that the new law that was passed, and actually some previous ones over the last couple years, allow for an Amicus, there's certainly that opportunity for the Court to include that type of additional expert outside advice. Similarly -- yeah.

BY MR. ABDO:

Q The new law you're referring to is the USA Freedom Act?

A Yes. I'm sorry, yes, USA Freedom Act, and then the --

Q The reauthorization --

A -- reauthorization for 702 also has

the Amicus portion of it.

Q Is there anyone else, to your knowledge, from whom the Foreign Intelligence Surveillance Court might acquire information about the operation of upstream surveillance?

MR. PATTON: Same. Hold on.

(Counsel conferring.)

MR. PATTON: So same objections as before. There are, as you know, some ex parte communications, and while I'm a Department of Justice Civil Division attorney, I'm not a Department of Justice national Security Division attorney, and so there may be other things that the witness is not aware of.

Again, I'd objected before to the fact that the it was beyond the scope of 30(b)(6), so she may not be aware of certain other things that may go on that I'm not aware of as well. I don't want the record to be unclear. That's potentially beyond her personal knowledge.

MR. ABDO: Understood. To the extent you know the answer --

THE WITNESS: So his answer was exactly what I was about to say before we -- before my lawyer said that, which is fantastic, so I've given you the information I know.

I don't work for the FISC, I don't do anything before the FISC, so what the FISC -- what else the FISC has at their disposal is up to the FISC.

BY MR. ABDO:

Q Do you know whether the NSA reviews or participates in any review of opinions of the Foreign Intelligence Surveillance Court concerning upstream surveillance before those opinions are signed or issued?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Would you just read that back? I think it's fine, but I just want to be double sure.

(The reporter read back the question.)

MR. PATTON: Object as beyond the scope of 30(b)(6), but if you have personal

knowledge, you can give it.

THE WITNESS: To the best of my knowledge, no.

BY MR. ABDO:

Q If the NSA identifies an inaccuracy in an opinion of the Foreign Intelligence Surveillance Court concerning upstream surveillance after that opinion is issued, would the NSA notify the Foreign Intelligence Surveillance Court of that inaccuracy?

MR. PATTON: Objection. Same as before, beyond the scope of 30(b)(6).

You can answer if you know.

THE WITNESS: I think that's when you would go to the FISC Review Board. You would do an appeal.

BY MR. ABDO:

Q What if it were not a judgment that the Department of Justice or the NSA disagreed with, but a factual misstatement in the opinion that would not give rise to or necessitate an appeal?

MR. PATTON: Same objection.

THE WITNESS: It would be fact specific. I can't speak to one way or another.

BY MR. ABDO:

Q Okay. Do you imagine that it would be good practice for the NSA to correct factual misstatements in the Foreign Intelligence Surveillance Court's opinions if and when they identify them?

MR. PATTON: Objection, calls for a legal conclusion, opinion, speculation, and beyond the scope of 30(b)(6).

THE WITNESS: Again, I think it would have to be very fact specific -- you know, the sort of situation and fact specific would have to decide what to do next, but, I mean, it's an Article III judge signing something. We're not really one part of the government saying something to the other part of the government. You may want to be thoughtful about how to do that.

BY MR. ABDO:

Q Understood. Are there any

inaccuracies that you're aware of relating to the operation of upstream surveillance in Exhibit 45, October 3rd, 2011, Foreign Intelligence Surveillance Court opinion?

MR. PATTON: Objection, vague as to time, and object to the extent it calls for classified information or statutory privileges information.

The witness can answer to the extent unclassified.

THE WITNESS: So you're asking if there's any information as of October 3rd, 2011, that we believe would have been inaccurate in Judge Bates' Memorandum and Opinion?

BY MR. ABDO:

Q Yes.

A To the extent that there are certain opinions that the judge makes as it relates to different aspects of this, those are the opinions of the Court and not necessarily those of NSA.

To the extent that there are facts in here, I believe we stand behind those facts, as

they're based off of the submission from June 1st that the government made in the subsequent submissions.

Q Okay. Did the NSA conduct a declassification review of Exhibit 45?

A Yes.

Q I assume that was a thorough review?

A Yes.

Q And anything that would disclose classified information, the NSA would identify as classified to the FISC so as not to release it to the public?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: I'm sorry, could you read that question back?

BY MR. ABDO:

Q Let me rephrase it. That's all right.

Did the NSA -- sorry.

If the NSA identified classified information -- let me -- sorry, let me start over.

Who actually disclosed Exhibit 45 to

the public?

MR. PATTON: Objection, vague.

THE WITNESS: It's a FISC document, so while the government has -- while the Executive Branch reviews it for classification, I believe the FISC issues it, although I know that the documents actually sit on ODNI's website.

BY MR. ABDO:

Q Are the redactions in this opinion in Exhibit 45 the government's redactions or the FISC's redactions?

A So the process is with all these documents that the government -- the Executive Branch will review them for classification and suggest redactions, and then the FISC has the opportunity to say no, I think these should be put out, and there was a conversation. But as a general matter, I guess they're really the FISC's document.

Q Do you know whether there's any dispute between the NSA or the Department of Justice with the FISC relating to the

classifications in Exhibit 45?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: My colleague was just getting warm. You can keep answering the question.

THE WITNESS: Okay.

MR. PATTON: I think there's some confusion back and forth as to this particular document, when it was declassified, and then the standard way that it's now under USA Freedom Act taken care of.

But this was, as you know, declassified prior to USA Freedom Act, and so I want to make sure the witness's answers are both accurate and reflective of what occurred.

BY MR. ABDO:

Q Right. I'm asking specifically about this opinion, Exhibit 45.

A And to which I don't know. I was not working at NSA. This I believe was declassified in 2013, and I was not working at NSA at that

point, so I don't have any specific knowledge on that fact.

Q Is there somebody at NSA who would know the answer to that question?

A I imagine the answer is that there wasn't any disagreement, that this is the document that went out.

Q Just to confirm though, you say you imagine that. Is that a guess, or is that --

A No, that's a statement. I mean, this is the document that went out. If there were any disagreements, those were resolved.

Q Okay.

A There's no further information that can be provided as to what those would be or not be.

Q Okay. Would the NSA treat statements in a FISC opinion as classifiable if they revealed information that the government considered classified?

MR. PATTON: Objection to the question. It calls for the expertise of an

original classification authority, and it's beyond the scope of 30(b)(6). You can answer.

THE WITNESS: I'm not sure I understand your question, so ...

BY MR. ABDO:

Q Let me ask it a slightly different way.

Would the NSA treat a statement in a FISC opinion as classifiable if it revealed information the government considered classified even if the FISC were not quoting a statement made by an Executive Branch agent?

MR. PATTON: Objection.

BY MR. ABDO:

Q In other words, if the FISC were to make a factual statement using its own words about the operation of upstream surveillance, and the NSA believed that statement revealed classified information, would the NSA consider that statement to be classifiable?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. Does the NSA conduct upstream surveillance on one or more international Internet links? I'm looking for a yes or no, not a specific number.

(Counsel conferring.)

MR. PADGETT: Could you read it back?

(The reporter read back the question.)

MR. PATTON: I misheard, so object to that as seeking classified information, subject to state secrets and statutory privileges.

Instruct the witness not to answer the question.

THE WITNESS: I'll follow the --

BY MR. ABDO:

Q Did the NSA conduct upstream surveillance on one or more international Internet links in 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Does the NSA conduct upstream surveillance today on more than one international Internet links?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q Did the NSA conduct upstream surveillance on more than one international Internet links in June of 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instruction.

BY MR. ABDO:

Q What is the number or approximate number of international Internet links on which the NSA conducted upstream surveillance in June of 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the direction.

BY MR. ABDO:

Q What is the approximate number of international Internet links on which the NSA today conducts upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Okay. Is upstream surveillance conducted on any international submarine cables?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instructions.

BY MR. ABDO:

Q Was upstream surveillance conducted on any international submarine cables in June of 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q What is the number or approximate number of cables on which the NSA conducted upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q What is the number or approximate number of cables on which the NSA today conducts upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Okay. In the context of upstream surveillance, can you tell me what an international chokepoint is?

MR. PATTON: Just a second.

Will you just read it back, please?

(The reporter read back the question.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q Is upstream surveillance today conducted at one or more international chokepoints?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Was upstream surveillance in June 2015 conducted at one or more international chokepoints?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q What number, approximate number, of international chokepoints was upstream

surveillance conducted on in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q What number, approximate number, of international chokepoints is upstream surveillance conducted on today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q I want to go back to page 45 very briefly of Exhibit 45, the sentence we were talking about before, the one that begins, "Indeed, the government readily concedes."

A Yes, okay.

Q Is there a term -- well, let me scratch that for a moment.

A moment ago I asked you whether the government conducts upstream surveillance on one or more international Internet links in 2015, then

I asked about today.

Is there a way I could phrase that question that would allow you to respond with an unclassified response more fully than you've responded so far?

MR. PATTON: For any given time period?

MR. ABDO: For June 2015 to today, and in 2011, at the time of -- let me try rephrasing one thing.

As of October 3rd, 2011, did the NSA conduct upstream surveillance on one or more international Internet links?

MR. PATTON: Same objection, same instruction.

BY MR. ABDO:

Q Is there a way that I could rephrase that question to use a term other than "international Internet link" that would allow you to provide an unclassified response?

(Counsel conferring.)

MR. PATTON: We don't think she can.

This is Rodney Patton, counsel for government.

We don't think she can answer that as to specific time periods for anything related to international Internet link. There may be a more general statement that she can make, but I feel like she's probably already provided that to you.

MR. ABDO: Okay.

MR. PATTON: Perhaps if we could go out and check, we might be able to come up with --

MR. ABDO: Maybe at the next break. You can add this to --

MR. PATTON: That's fine.

BY MR. ABDO:

Q So back to page 45 very briefly of Exhibit 45. Do you understand the sentence we've been discussing, the one that begins, "Indeed, the government readily concedes," to confirm that, as of October 3rd, 2011, that the government in fact conducted upstream surveillance at at least one international Internet link?

MR. PATTON: Objection, mischaracterizes the language of page 45 of

Exhibit 45.

BY MR. ABDO:

Q You can answer.

A Do you want me to answer?

MR. PATTON: Not as it's phrased, no, she can not answer that question. It would call for a classified answer.

MR. ABDO: I'm sorry, I didn't hear that. So you're instructing the witness not to answer?

THE WITNESS: Yeah, that's classified.

BY MR. ABDO:

Q Okay. Do you understand the sentence to confirm that if a transaction -- that as of October 3rd, 2011, the NSA would in fact acquire a wholly domestic -- sorry, would in fact acquire a wholly domestic "about" communication if the transaction containing the communication were routed through an international Internet link being monitored by the NSA?

MR. PATTON: Objection as not exactly what the language of the sentence said. Let me

see if she can answer that question.

To avoid us having to go out to the SCIF and come back again, she can answer whether or not the statement in this, as exactly written, is correct as of October 3rd, 2011, in a yes-or-no answer. I believe she's already answered that, but --

MR. ABDO: I think you did already answer that this sentence, as written, is true as of October 3rd, 2011.

MR. PATTON: That she can answer.

MR. ABDO: Okay.

THE WITNESS: Do you want me to say it again?

BY MR. ABDO:

Q Sure.

A Yes, that sentence is accurate as of October 3rd, 2011.

Q Okay. Let me go back to Exhibit 42.

A Which one is 42?

Q The NSA's Responses and Objections to Plaintiffs' First Set of Interrogatories.

I direct your attention to page 7 to 8.

A 7 to 8, oh, yes.

Q The paragraph that carries over between the two, which is labeled "RESPONSE."

Would you mind just reading that to yourself?

MR. ABDO: Why don't we take a break right now. Can we go off the record for a minute?

(A break was taken at 3:06 p.m.)

(Resume at 3:15 p.m.)

BY MR. ABDO:

Q Ms. Richards, have you had a chance to look at page 6 of Exhibit -- sorry, page 7 to 8 of the carryover paragraph on pages 7 to 8 of Exhibit 42, the NSA's response to Interrogatory No. 3?

A Yes.

Q Is there anything beyond that response in Exhibit 42 that isn't classified that you could provide us about the NSA's understanding of the term "filtering mechanism," both in June 2015 and

today?

A Those are pretty good definitions you've got right there. I don't have anything else to add.

Q Does that mean that there isn't anything unclassified that you could add to those definitions?

A There's nothing unclassified I can add to those descriptions.

Q Okay. With respect to upstream surveillance as it operated in 2015, did the term "filtering mechanism" include the use of, quote, an Internet protocol filter to ensure that the person from whom the NSA seeks to obtain foreign intelligence information is located overseas?

A In 2015, filtering mechanism would have -- one of the examples that was used -- I'm sorry.

An example of a filtering mechanism was an IP address -- sorry. (Reviewing document.)

Okay, let me revise -- I'm sorry, let me just revise my answer.

Q Sure.

A So I would actually add from the Civil Liberties and Privacy Office Report, which is Exhibit 44, on page 5, where we give an example that, in certain circumstances, NSA's procedures require that it employ an Internet protocol filter to ensure that the target is located overseas.

Q Does that mean the answer to my question is yes, that the filter you just described is part of the filtering mechanism described in the NSA's response to Interrogatory No. 3?

A Yes, and so I was correcting the fact that when I said that was everything you could say in an unclassified.

What I'm saying is I'm correcting the record to say I could have additionally added the fact that that would include the IP -- that could include -- could include --

Q Could include, understood.

A -- as an example of what the filtering mechanisms are, so ...

Q In June of 2015, did the term "filtering mechanism" include the use of an Internet protocol filter? I'm trying to understand "did" versus "could" include.

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Object to form, vague.

You can answer.

THE WITNESS: Okay. To the extent that the information is classified -- to the extent that how this exactly works is classified, I use the term "could" as one of the examples of what a filtering mechanism is.

I can neither confirm nor deny exactly what was happening in 2015 as it relates to the specificity of the filtering mechanism. I can just tell you that it could include that as an example.

BY MR. ABDO:

Q Can you confirm whether it did include an Internet protocol filter as of the date of Exhibit 44, April 16th, 2014?

A As is specifically stated on page 5, it's a "could." It's not a "did."

Q Just for the record, could you tell us where you're reading from on page 5?

A Sure. It's the very last sentence on page 5 of Exhibit 44 that begins with "for example."

Q "In certain circumstances, NSA's procedures require that it employ an Internet protocol filter to ensure that the target is located overseas."

So in certain circumstances, they're required to.

A Mm-hmm.

Q Can you tell us what those certain circumstances would be in unclassified terms?

MR. PATTON: No, she can't. Object to the question to the extent it calls for classified information --

THE WITNESS: The information -- oh.

MR. PATTON: -- subject to the state secrets and statutory privileges, and instruct the

witness not to answer.

THE WITNESS: I'll follow.

BY MR. ABDO:

Q With respect to upstream surveillance as it operated in 2015, did the term "filtering mechanism" include, quote, the use of a screening device in the upstream Internet collection process to acquire only Internet transactions containing at least one task selector?

A It appears you're reading from something. Could you just refer me to where those words exactly are to make sure I have the full context?

Q Sure. The last portion of my question was a direct quote from the NSA's response to Interrogatory No. 5 in Exhibit 42 on page 10, the text marked "RESPONSE."

A Okay. And so could you read your question once more?

Q With respect to upstream surveillance as it operated in 2015, did the term "filtering mechanism" include, quote, the use of a screening

device in the upstream Internet collection process to acquire only Internet transactions containing at least one task selector?

A So I would look at Interrogatory 4. I understand you pointed me to the response to Interrogatory 5, but the process is we filter for wholly domestic communications, and then we do the scanning to ensure that we're only -- we're doing a scan using a screening device designed to identify for acquisition Internet transactions.

And in 2015, it would have been to, from, or about persons targeted; today, it's to or from persons targeted, in parens, with our targeting procedures.

Q Okay. What I'm trying to understand is whether the use of a screening device is part of the filtering mechanism process described in NSA's response to Interrogatory 3?

MR. PATTON: Objection, calls for information that's classified, subject to state secrets and statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Follow instruction.

BY MR. ABDO:

Q Would you be able to answer the question if I asked whether the use of a screening device could be part of the filtering mechanism described in the NSA's response to Interrogatory 3 on pages 7 to 8 of Exhibit 42?

MR. PATTON: Just a second.

Can you read back that question?

BY MR. ABDO:

Q Let me state it more clearly because that's a bit fragmentary.

With respect to upstream surveillance as it operated in 2015, could the term "filtering mechanism" include, quote, the use of a screening device in the upstream Internet collection process to acquire only Internet transactions containing at least one task selector?

MR. PADGETT: I'm sorry, I need to hear that one more time.

(The reporter read back the question.)

MR. PADGETT: I guess I would ask,

before we instruct the witness whether they can answer or not, are you referring to filtering mechanism as used in the document that's referred to by Interrogatory No. 3?

MR. ABDO: Yes.

MR. PADGETT: So can we see?

MR. ABDO: It's one of your briefs from the Fourth Circuit.

MR. PATTON: Let's go off the record.

(Off the record at 3:26 p.m.)

(Resume at 3:38 p.m.)

(The reporter read back the question.)

MR. PATTON: Objection, vague.

You can answer.

THE WITNESS: Okay. So I think the best description for how the process works in the unclassified realm is going to be on page 37 of the PCLOB Report, which is Exhibit 43.

To the extent that the -- so where it says -- the sentence starting, "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 task 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 task selector."

Now, my understanding is that there's this other brief that comes up with a new term called "filtering mechanisms"; that's not meant to be something special or otherwise different from the process that was described in PCLOB.

To the extent that you have specifics about the how and the when and the what, that would be classified, but those were not designed to be somehow describing something different.

BY MR. ABDO:

Q Okay. And for the record, you're reading from the top of page 37 of Exhibit 43, correct?

A That is correct.

Q The sentence beginning, "To identify and acquire"?

A That is correct.

Q So would the use of an IP filter fall within the description of that sentence in which it says, "Internet transactions are first filtered to eliminate potential domestic transactions"? Is that where an IP filter could be used?

A Yes, that is an example of where -- an IP filter is an example of something that could be used to do that filter.

Q Okay. And is the use of a screening device described in the NSA's response to Interrogatory 5 in Exhibit 42, is that use of a screening device what could be used to accomplish what is described in the second portion of the sentence that you were reading from page 37 of Exhibit 43, that second part saying, quote, then our screened capture only transactions containing a task selector?

A Yes.

Q Okay. And with respect to upstream surveillance as it operated in 2015, what else could the term -- sorry, what else -- what other

processes could be used to accomplish either the filtering or the screening described in the sentence you were reading from page 37 of Exhibit 43?

MR. PATTON: Objection, calls for classified information, information subject to the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Okay. Are all transactions that were subject to upstream surveillance in June 2015 subjected to Internet protocol filtering --

MR. PATTON: Objection.

BY MR. ABDO:

Q Sorry, let me just finish the question real quick.

-- to eliminate potential domestic transactions from upstream surveillance?

MR. PATTON: Objection, calls for classified information, information subject to the

statutory privileges.

Instruction not to answer the question.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Can you please describe all the ways in which the NSA could determine in 2015 or could determine today whether a transaction is wholly domestic in order to filter it out from upstream surveillance?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Could you break that down into 2015 to 2017 to make it clear?

BY MR. ABDO:

Q Could you please describe all the ways in which the NSA could determine in 2015, as part of upstream surveillance, whether a transaction is wholly domestic so as to filter it out?

MR. PATTON: Objection, calls for classified information in order to respond fully

to that question.

There may be an unclassified response to that question, but without knowing what the witness's answer would be, I'm not comfortable just turning that over to her, but I believe there is an unclassified response, but it's also one that she has given you already.

BY MR. ABDO:

Q Okay. If there's nothing more that you could say that's unclassified, let me know that you'll follow your counsel's instruction not to provide any further information.

A There's no additional information that can be provided. What you see here is as much unclassified information as available.

Q And by "here," you're referring to Exhibit 43, page 37?

A Page 37, or the interrogatories.

Q The responses we've been discussing?

A The responses, yeah. There's no additional information to be provided.

Q Okay. What does it mean to say, as

the NSA's response to Interrogatory 3 does, that wholly domestic Internet transactions are, quote, eliminated? And that's in Exhibit 42, I think at page 7 to 8.

MR. PATTON: Object to the extent it calls for classified information and information protected by the statutory privileges.

There is an unclassified answer that the witness can give.

THE WITNESS: So you're asking what does it mean to eliminate?

BY MR. ABDO:

Q Yes.

A So I think if you look at the response, it's important to understand that it starts with -- the sentence is that the devices utilized in the upstream Internet collection process that were designed to eliminate wholly domestic transactions.

So they were -- it's important to recognize it was designed, not that it was actually done.

Q Understood. So let me then be clear.

What does it mean to say -- what were they designed to do in eliminating wholly domestic --

A So that they wouldn't --

Q -- transactions?

MR. PATTON: Same objection, same instruction.

THE WITNESS: They're designed so that they don't make it through to being ingested by NSA's -- into NSA's repository. That's what it means to be designed to eliminate.

BY MR. ABDO:

Q And the repository is what holds communications that contain a selector and are not wholly domestic as of June 2015?

MR. PATTON: Object to the extent it calls for classified information and statutory privileges. You can answer to the extent unclassified.

THE WITNESS: So --

BY MR. ABDO:

Q I'm just trying to understand.

When you say "ingested," you're referring to the databases or the places in which the NSA stores communications that are ultimately authorized by Section 702 to collect?

A Yes, yes. It's when NSA collects it.

MR. PATTON: Same objections.

THE WITNESS: Yes. NSA collects, acquires, ingests. It's the point at which NSA now has it.

BY MR. ABDO:

Q Understood. Can an e-mail address be a selector under upstream surveillance?

A Yes.

Q Can a phone number be a selector under upstream surveillance?

A Yes.

Q Can an Internet protocol address be a selector under upstream surveillance?

MR. PATTON: Objection, calls for classified information and privileged information

pursuant to the statutes aforementioned, and instruct the witness not to answer the question.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Can a URL, or uniform resource locator, be a selector under upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

MR. PATTON: Just a moment.

MR. PADGETT: Let's go off the record to discuss.

(Off the record at 3:49 p.m.)

(Resume at 3:53 p.m.)

BY MR. ABDO:

Q We're back from break, and the question was can a URL be a selector under upstream surveillance?

MR. PATTON: Objection, calls for

classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will not answer.

BY MR. ABDO:

Q Could a URL be a selector under upstream surveillance as of June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q Are the selectors used for upstream surveillance the same as those used for PRISM surveillance as of June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Wait, I'm sorry. Can you ask the question again?

BY MR. ABDO:

Q Sure. I'll modify it slightly to make it grammatically correct.

Were the selectors used for upstream surveillance the same as those used for PRISM surveillance in June 2015?

MR. PATTON: Same objection, same instructions.

THE WITNESS: Can you just --

MR. ABDO: Ms. Jaques, would you mind marking this as Exhibit -- you're still looking at something for this question?

THE WITNESS: Yes, I am.

The only thing I would state which is definitely not classified is on page 6 of the Civil Liberties and Privacy Office Report, Exhibit 44. At the very top of page 6 it says, "The process for approving the selectors for tasking is the same for both PRISM and upstream collection."

I realize that's not exactly the question you were asking, but I just wanted to make sure you had that piece of information.

BY MR. ABDO:

Q Thank you. Ms. Jaques, would you mind

marking this 46? And it's the entire folder.

(Deposition Exhibit 46 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards --

A Oh, this is fabulous, okay.

Q You have in front of you what's marked as Exhibit 46. Do you recognize that document?

A I do.

Q And what is that document?

A This is the Privacy and Civil Liberties Oversight Board Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, March 19, 2014.

Q Did employees of the NSA testify at that hearing?

A Yes.

Q And they were testifying in their official capacity as NSA employees?

A Yes.

Q Could you turn to page 57 of the

transcript? Do you see at lines 17 to 20 there's a statement that's labeled as coming from Mr. De, spelled D-E?

Do you understand that to be -- who do you understand that to be?

A I'm sorry, we're at line?

Q Lines 17 to 20 of page 57.

A 17 to 20, okay.

Q Of Exhibit 46.

A Mr. De. Oh, let me just --

Q Before getting to the substance of that sentence, which we'll give you a chance to read in a second, do you know who this Mr. De is who is being referred to?

A Yes. He was the general counsel at the time of NSA.

Q And for the record, his full name is Rajesh De?

A Yes.

Q Could you now read those two lines -- those four lines, 17 to 20 on page 57, to yourself?

A (Witness reviewing document.) Okay.

Q What do you understand Mr. De to have been communicating in this first sentence? And the first sentence was, quote, "And it's the same selectors that are used for the PRISM program that are also used for upstream collection."

MR. PATTON: Objection to form, vague.

MR. ABDO: You can answer.

THE WITNESS: I think similar to what I just read to you, the words on the face of it seem accurate.

I'm not sure what you're trying to ask me. Maybe you can help clarify.

BY MR. ABDO:

Q What I'm trying to understand is whether the selectors that are used for PRISM are also used for Upstream collection, and that seems to be on the face of the statement what Mr. De said at the hearing transcribed in Exhibit 46, but I understood you to refuse to answer the question of whether the selectors that are used for the PRISM program are also used for Upstream

collection, so I'm trying to understand what the difference is between my question and this statement.

A I think I need to go -- sorry.

MR. PADGETT: Can I ask a clarifying question? Because it might involve an instruction.

MR. PATTON: Right. There's also a difference of what we're talking about here, so I don't know whether the witness is aware of that, the differences.

MR. ABDO: Are you saying you need to talk in the SCIF?

MR. PATTON: I don't know that we need time to talk in the SCIF, but the objection was to something A, and this is meaning something B, if you know what I mean, and therefore I want to get you that answer because I think that answer is unclassified.

MR. ABDO: Is there an answer that the witness --

MR. PATTON: Because I can understand

why you're having this question, but I'm trying to figure out the best way to get you that unclassified answer.

BY MR. ABDO:

Q Ms. Richards, do you understand the distinction your counsel is drawing between this statement by Mr. De at the hearing transcribed in Exhibit 46 and the question that I asked a few moments ago about whether selectors used for Upstream are the same as those used for PRISM surveillance?

If you know the answer to my question, could you please answer it?

A So let me see if I can restate the two different questions, and maybe I need to have you read back to me what you asked before and we objected to on classified, which is this statement states, "it's the same selectors that are used for the PRISM program that are also used for upstream collection."

A few minutes ago, you had asked whether this was true, and I declined to comment

for classified purposes.

Q Right.

A That's the --

Q Well, let me phrase it this way.

Is the statement that Mr. De made at this hearing in March of 2014 true, or was it true at that time that, quote, it's the same selectors that are used for the PRISM program that are also used for upstream collection?

A I would like to confer in the SCIF before I give you the answer to both of those questions.

MR. PATTON: I just want to seek clarification for the record.

Are you concerned that there's a privilege issue, a classification issue? Is that your concern?

THE WITNESS: Yes.

MR. PATTON: Okay.

THE WITNESS: Not with this sentence.

MR. PATTON: Not with the sentence, but whether or not you can answer --

THE WITNESS: With the other question that was asked.

BY MR. ABDO:

Q I see. If I were to rephrase my previous question to be were the selectors used for PRISM surveillance in June 2015 the same as those used for Upstream surveillance?

MR. PATTON: I have to object to the question as to its vagueness. There is an unclassified answer and there's a classified answer, and --

THE WITNESS: And I'm tripping over which one, so I just need to go --

MR. PATTON: -- and I want to get you the unclassified answer.

MR. ABDO: Okay. Can we take a break and go off the record while you guys confer in the SCIF?

(Off the record at 4:03 p.m.)

(Resume at 4:13 p.m.)

BY MR. ABDO:

Q We're back on the record.

The question we left with, Ms. Richards, was what Mr. De meant in the hearing in March 2014, transcribed in Exhibit 46, when he said, "And it's the same selectors that are used for the PRISM program that are also used for upstream collection."

MR. PATTON: Objection to the extent it calls for classified information and information protected by the statutory privileges.

You can answer to the extent unclassified.

THE WITNESS: Okay. So in looking at page 57, it's important to roll back to roughly around page 55 and understand what they were talking about at this point. And, specifically, I would bring you to -- okay, I'm sorry, go back to 54. Where did the language just go? Okay, I'm sorry, page 56.

So Mr. Wiegmann says, "About that selector, correct."

And then Mr. De says, "It is always focused on that account, so I think the key is,

the misperception that some may have that 'about' collection is somehow about a key word or about the person that may be behind that account.

"But all collections under Section 702, whether it's upstream abouts, which is a subset of upstream, or PRISM is all based on the selectors at issue."

Then we have Ms. Brand says, "Just to follow-up on that because that's a good line of inquiry, just to make sure that everyone understands. So you're saying that if someone is emailing about Rachel Brand or about explosives that would not be a permissible about query under your explanation?"

And Mr. De goes on, and what he's explaining then, when we get down to lines 17 to 20, is the type of selectors is the context for this exchange back and forth, which is then how this is -- in talking about the types of selectors, as opposed to "bomb" or "explosive" or a name, he's explaining that these are the same types of selectors.

That is what's the unclassified fact, and then it's furthered by the sentence I mentioned in the Civil Liberties and Privacy Office Report, as opposed to your question you asked earlier where we said that's classified.

BY MR. ABDO:

Q I think I understand.

A Okay.

Q Moving on a bit.

As of 2015, did the procedures approved by the FISC for upstream surveillance permit the NSA to collect an international HTTP transmission of a website if the text of that website contained a selector?

MR. PATTON: Objection, calls for classified information and information subject to the statutory privileges.

Instruct not to answer the question.

THE WITNESS: I will follow the instruction.

BY MR. ABDO:

Q Okay. Sorry, just one second.

(Deposition Exhibit 47 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you have in front of you what's been marked as Exhibit 47.

Do you recognize this document?

A Yes.

Q What is it?

A This is the government's response to the Court's briefing order of May 9th, 2011.

Q With the Court being the Foreign Intelligence Surveillance Court?

A Yes.

Q Do you know which agency of government authored this document?

A It's submitted by the National --

MR. PATTON: Objection to form, vague.

THE WITNESS: -- National Security Division of the Department of Justice, and verified by National Security Agency.

BY MR. ABDO:

Q Okay. When you say "verified," you

mean verified as to the accuracy of the statements within it?

A Yes, to the best of the knowledge of the individual doing it.

Q Would you mind turning to page 30 of Exhibit 47? And I should have mentioned at the outset, Exhibit 47 is Bates stamped NSA-WIKI 237 -- sorry, I may not have the full version in mine. Sorry, NSA-WIKI 234 to 277.

Okay, if you turn to page 30, which is marked NSA-WIKI 266, toward the bottom there's a sentence that begins "this figure," and I'll read it. "This figure was then compared to the total take of Section 702 upstream collection of web activity for the month."

Do you know the context in which this sentence was written in unclassified terms?

A Can you clarify your question? I'm not sure I know what you're asking.

Q Was the context of this sentence an effort to respond to the FISC's inquiry of the NSA about the volume of certain forms of the NSA's

upstream collection?

A Can you repeat?

Q I'll repeat that.

Does this sentence come in a paragraph responding to the FISC's inquiry of the NSA about the volume of certain forms of the NSA's upstream collection activity?

A Yes.

Q And was this sentence explaining how the Department of Justice and the NSA arrived at certain figures it was relaying to the FISC in responding to the question?

A Yes.

Q What does "web activity" mean in the context of Internet communications?

MR. PATTON: Object to the form of the question to the extent it calls for a classified answer or an answer that would be subject to the statutory privileges.

The witness can answer if there's an unclassified answer.

THE WITNESS: I'm going to read this

answer over once more before I give you --

BY MR. ABDO:

Q Please. Maybe I can rephrase the question for you.

A Sure.

Q Do you understand "web activity" to refer to activity of the World Wide Web -- or activity on the World Wide Web?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: I'm just going to object to the vagueness.

THE WITNESS: I would refer that to meaning as a way of generally talking about the collection of discrete Internet communications.

BY MR. ABDO:

Q Would you understand it to refer to collection -- let me ask this.

Would Internet web browsing constitute web activity?

MR. PATTON: Objection, calls for classified information to the extent that it's

being asked in the context of upstream collection in this particular document, and subject to that objection and to the statutory privileges that would protect that.

I instruct the witness not to answer the question.

THE WITNESS: I will follow the instruction.

BY MR. ABDO:

Q Do you understand the meaning of the term "web activity" generally, not with regard to this document?

A Yes.

MR. PATTON: Object. Object that it's beyond the scope of the 30(b)(6), but the witness can answer.

BY MR. ABDO:

Q What does it mean generally beyond -- you know, outside of the context of this document, Exhibit 47?

MR. PATTON: Same objection.

THE WITNESS: You say activity on the

Internet?

BY MR. ABDO:

Q Any activity on the Internet. You don't understand "web activity" to be distinct from "Internet activity"?

MR. PATTON: Same objection.

THE WITNESS: I think it's a vague enough term it could be meant any number of different things.

BY MR. ABDO:

Q You don't understand it to mean specifically the protocol referred to as the World Wide Web, which encompasses HTTP and HTTPS communications? That's not how you understand an Internet professional would understand that term?

MR. PATTON: Same objection, adding objection that it calls for expert opinion, and also object that it's asked and answered.

THE WITNESS: I don't think there's a set definition for "web activity." I think it could mean Internet activity, it could mean World Wide Web activity. It could mean any of those

different -- those particular different ones.

I think you have to look at the context for the sentence, and then make a decision accordingly.

BY MR. ABDO:

Q Do you have any reason to believe that this sentence was inaccurate, "this sentence" again in Exhibit 47 beginning, "This figure was then compared"?

A No.

Q Does it disclose classified information?

MR. PATTON: As redacted?

MR. ABDO: As it appears in Exhibit 47.

THE WITNESS: I don't think so.

BY MR. ABDO:

Q To your knowledge, is the term "web activity" ever otherwise used by the NSA in publicly disclosed documents interchangeably with "Internet activity" at large?

MR. PATTON: Object to the form,

vague.

THE WITNESS: I don't know that I've seen "web activity" used in other documents that are unclassified -- that have been declassified. To the extent you're going to show me one next --

BY MR. ABDO:

Q I don't have one. I'm asking.

A So if this is the only instance of this and you're -- you know, I don't have -- I haven't seen it in any of the other documents I've read in the last few weeks, or since we've been prepping for this, so --

Q I'm not trying to play a game of gotcha. I'm asking because your answer suggested that you believe "web activity" to be essentially used interchangeably with the very generic term "Internet traffic" or "Internet communications," and I would assume, if that were the case, then the NSA would in fact use that term interchangeably, but I don't believe that to be the case. I'm asking why that is.

MR. PATTON: Object to the extent it

mischaracterizes prior testimony.

THE WITNESS: I don't have any specific further information that would help elucidate this conversation.

Anything further I might say would go into a classified discussion, and so I can't give you any further explanation as to the use of the word "web" there.

BY MR. ABDO:

Q Under upstream surveillance, as conducted in June 2015, was the NSA permitted to collect the communications of a foreign target with a website in the United States?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Object to the form, vague and ambiguous, and also object that it could call for classified information and information protected by the statutory privileges.

Depending on what the question means, there might be an unclassified answer.

BY MR. ABDO:

Q Do you have an unclassified answer, Ms. Richards?

MR. PATTON: And if she does, I'd like to hear it before she gives it to make sure that it is unclassified.

BY MR. ABDO:

Q Let me give you another question to consider.

A I was just going to say, do you have a whole bunch of them, and then we can go and confer on what those might be?

Q I have one other.

A Okay, but could you repeat that one again?

Q Let me repeat that one, and I'll tell you the other one.

A Yeah.

Q The first one is, under upstream surveillance as approved as of June 2015, was the NSA permitted to collect the communications of a foreign target -- that is, somebody who is a

foreign target of upstream surveillance -- abroad with a website in the United States?

Do you understand my question?

A I do understand.

I don't think there's an unclassified answer, but to the extent --

Q Okay. The second question that I hope you'll consider in the SCIF, under upstream surveillance as it was implemented in June 2015, was the NSA permitted to collect the transactions or communications of a non-targeted foreigner abroad with a website in the United States if the website contained a selector tasked for collection?

A A non-targeted foreigner abroad on a U.S. --

Q With a website in the United States.

A With a website in U.S.

Q If the website contained a selector task for collection. You're generally --

MR. GILLIGAN: I'm baffled by the question.

MR. ABDO: A non-foreign target -- I'm sorry, a non-targeted foreigner abroad communicating with a website in the United States, and the website contains a selector.

MR. GILLIGAN: You mean communicating with a website?

MR. ABDO: Yeah. They visit the website, for example. They're communicating with a website.

MR. GILLIGAN: Yeah, that's what was baffling, what you meant by "with."

MR. ABDO: Communications to and from.

THE WITNESS: So the selector is looking at the website?

BY MR. ABDO:

Q Suppose a non-targeted foreigner abroad is viewing a website, and the website is stored on a web server in the United States, and it contains a task selector --

A The website?

Q The website. And that task selector is being communicated back to this non-targeted

foreigner abroad, and it passes through something being monitored by the NSA in upstream surveillance, did the NSA have the authority in 2015 to collect that communication?

MS. HANLEY COOK: Should we go off the record now?

MR. ABDO: Okay, thanks.

MR. PATTON: Thank you.

(Off the record at 4:30 p.m.)

(Resume at 4:46 p.m.)

MR. PATTON: The witness has reviewed in the interim the applicable targeting procedures, the declassified public version of those, and is prepared to make a statement on that particular point, but we don't believe that anything beyond what she's going to say can be said on the public record.

So to the extent not covered by what she's about to say, we object to the questions to the extent they call for a classified response subject to state secrets and subject to the statutory privileges.

THE WITNESS: The examples you provided are classified. How the targeting might or might not occur is all classified on page 5. It's all black, so we can't go any further into that information.

If you would like to -- I'm sorry. I'm looking at Exhibit A, the procedures used by the National Security Agency for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978 as amended. These are dated June 2014.

BY MR. ABDO:

Q What page were you looking at of those?

A 5.

Q If I understand, page 5 relates to the NSA's method for assessing whether there would be a foreign intelligence purpose for collecting certain Internet communications, right?

A Yes.

Q My question didn't deal with whether the NSA in fact had reason to or would want to collect Internet communications.

My question was, did the NSA, in June of 2015, have the authority to collect the communications of a foreign target abroad with a website in the United States?

MR. PATTON: The answer to that question is classified and subject to statutory privileges.

Instruct the witness not to answer the question.

THE WITNESS: I'll follow the instructions.

BY MR. ABDO:

Q And under upstream surveillance as conducted in 2015, did the NSA have the authority to collect the transactions of a foreigner abroad with a website in the United States if the website contained a selector task for collection?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: I'll follow the instruction.

BY MR. ABDO:

Q Are you aware that the Office of Director of National Intelligence has acknowledged that there was a time when overcollection of webmail in-boxes had contributed to the -- had occurred under upstream collection?

MR. PATTON: Just a second.

(Counsel conferring.)

THE WITNESS: Can you point to the document or provide whatever that is?

BY MR. ABDO:

Q I'm asking whether you're aware that that's the case.

A I would want to see where exactly ODNI had said that information to make sure that I wasn't somehow going into some sort of classified discussion.

Without the context of what you're saying, as we've seen a few times, sometimes the

information on its face looks like it says one thing, as we just went through with Raj De's back and forth. So without seeing the context of whatever that is, I don't know how to answer.

Q Let me ask a different question then.

Do you know the answer to the question I asked? Well, let me ask that. Do you know the answer to the question I asked?

MR. PATTON: Objection, vague as to which question.

MR. ABDO: The question being whether you're aware that the Office of Director of National Intelligence has acknowledged that one of the overcollection problems that the NSA had with upstream surveillance involved the collection of webmail in-boxes? Do you know the answer to that question?

THE WITNESS: Again, without confirming or denying, I need to see the document you're referring to to better understand. I'm just concerned I'm in classified territory.

BY MR. ABDO:

Q I'm not asking you for an answer to that question. I'm asking whether you know the answer to that question first.

A I'm sorry, I don't know how to answer what you're saying.

MR. GILLIGAN: It's circular. The question is whether she knows, so I don't know whether she knows the answer to that question is the same question.

MR. ABDO: If forced to answer that question, do you know whether you would say yes or no? I'm not asking you to say yes or no, I'm asking whether you know which one you would say if you were forced to answer the question?

THE WITNESS: And so I'm sorry, I don't know what document you're referring to. I assume you're referring to some document somewhere that ODNI published, and if I could see that so that I could look at it, I would be able to tell you whether I know the answer or not.

But in the abstract question of, "Do

you know this?," I can't answer one way or the other. So without sort of having some basis in what we're looking at, I'm having a hard time answering.

BY MR. ABDO:

Q Okay. Was the collection of webmail in-boxes in fact one of the overcollection problems the NSA had with upstream surveillance specifically with regard to multi-communications transactions?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: I just want to state for the record that neither the witness nor I are trying to be difficult here. We are concerned about providing responses to information that we haven't seen, and so I don't want to instruct the witness not to answer the question if there's a public document out there.

I think it would be better if you show it to her. It will either refresh her recollection and she'll be able to explain whether

she's seen it before or anything like that, but at this point, she's not wanting to answer the question, and I'm concerned that the answer may be classified.

MR. ABDO: Are you able to determine whether the answer is classified without knowing whether there's a physical document in the world that contains the information? Is that the definition of "classified"?

MR. PATTON: No, it really gets to, at this particular point, we don't know what it is that you're referring to, and it may be an unclassified document that the Director of National Intelligence has said X, Y or Z. If that's it, it provides the context and some form of comfort for the witness, who is being asked to determine what's on one side of the classified line and what's not on the other.

She signed a Non-Disclosure Agreement and is -- I mean, her responses to you so far have tried to give you as much unclassified information as possible. She's evidently concerned that if

she provides a response to this outside of any context that she might be violating that NDA.

BY MR. ABDO:

Q Are you aware that the Office of Director of National Intelligence, on August 21st of 2013, held a conference call with reporters in which the Office of Director of National Intelligence described the overcollection of webmail in-boxes as an example of the overcollection problem the NSA experienced under upstream surveillance with regard to multi-communication transactions?

MR. PATTON: Again, that may have occurred on August 21st, 2013. It may be a document that is a newspaper article that may or may not be accurately depicting what ODNI said at that time. And so our concern again, in the abstract, is whether or not the information you're providing is both accurate and unclassified.

MR. ABDO: Okay. So can I confirm, at least for the time being, are you instructing the witness not to answer the question?

MR. PATTON: At the moment, I don't think the witness is in a position to answer the question. Factually, I don't know what it is that you're referring to. And given the amount of information that has been provided through unofficial sources, our concern, and my duty here, and the witness's duty, is to protect classified information, and we want to provide as much unclassified information as we can --

MR. ABDO: I understand. I'm just asking a simple question, Rodney. Are you instructing the witness not to answer?

MR. GILLIGAN: Tell you what, if we step outside, I might be able to suggest a way around this.

MR. ABDO: Can we go off the record?

(Off the record at 4:57 p.m.)

(Resume 5:04 p.m.)

THE WITNESS: Is there an outstanding question? Where are we?

BY MR. ABDO:

Q There was. Let me start with the

question outstanding, which was are you aware that the Office of Director of National Intelligence has acknowledged that the NSA has collected webmail in-boxes under upstream surveillance?

MR. PATTON: Object to the form as beyond the scope of the 30(b)(6) notice, and the witness can answer in her personal capacity.

THE WITNESS: I'm not aware.

BY MR. ABDO:

Q Has the NSA collected webmail in-boxes as part of upstream surveillance?

MR. PATTON: Object to the question, calls for classified information and information protected by the statutory privileges, and instruct the witness not to answer the question.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Okay. Are you familiar with the fact that the contents of Internet communications are transported in what is known as the application layer of Internet packets?

MR. PATTON: Object to the question to the extent it calls for classified -- I'm sorry, I'm so used to that -- to the extent it calls for expert opinion, and that it's beyond the scope of 30(b)(6).

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. Are you aware of the fact that the contents of an email communication are transported within the application layer of Internet packets?

MR. PATTON: Same objections.

THE WITNESS: Yes.

Isn't that what you just asked me?

BY MR. ABDO:

Q The first question was with respect to Internet communications generally, and the second question was with respect to email communications specifically.

A Okay.

Q Is your answer to both yes?

A Yes. It sounded like the same one,

and I worried I was missing something.

Q And are you aware of the fact that the contents of a website are transported within the application layer of Internet packets?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Are the filtering or screening processes that you've described with respect to upstream collection as it operates -- or excuse me, upstream surveillance as it operated in June 2015 -- forms of deep packet inspection?

MR. PATTON: Objection.

(Counsel conferring.)

MR. PATTON: I'm sorry, could you read that back?

BY MR. ABDO:

Q Sure. Are the filtering or screening processes that you've described under upstream surveillance as conducted in June 2015 forms of deep packet inspection?

MR. PADGETT: I'm sorry, one key thing

I didn't get. Could you read that back?

(The reporter read back the question.)

MR. PATTON: Object to the question because it calls for classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Are you familiar with the term "deep packet inspection"?

MR. PATTON: Object to that question, beyond the scope of 30(b)(6), and it calls for an expert opinion.

THE WITNESS: In the general sense of the word, as in not specific to anything in particular, but known as the outside world?

BY MR. ABDO:

Q Not specific to upstream surveillance, but --

A Yes.

Q You are familiar with it?

A Yes.

Q What does it mean?

MR. PATTON: Same objections.

THE WITNESS: It's the concept of -- I'm sorry, I'm --

BY MR. ABDO:

Q Is it the process of examining or analyzing the application layer of packets traversing the network?

MR. PATTON: Same objections.

THE WITNESS: Yeah, I'm -- yes. Yes, that's a fine description.

BY MR. ABDO:

Q Tell me again your position at the Department of Homeland Security.

A I was the Senior Director for Privacy Compliance in the Privacy Office.

Q And you participated in the drafting of Privacy Impact Assessments?

A I did.

Q Were you involved in the Privacy Impact Assessments conducted for the Einstein 2 or

Einstein 3 programs?

A Yes, which is why I changed the answer when you asked about the four types of sort of --

Q Ah, got it.

A When I rechanged it, I realized that would probably constitute what you were considering to be surveillance.

Q Network surveillance?

A Network surveillance.

Q Did Einstein 2 involve deep packet inspection?

A I honestly don't remember.

MR. PATTON: Just object to that question as beyond the scope of 30(b)(6). I'm not sure whether the answer is unclassified or not since I have not consulted with the Department of Homeland Security, but if the witness knows of an unclassified answer, the witness can give an unclassified answer.

BY MR. ABDO:

Q Sorry, please go ahead.

A I apologize, but I don't remember what

is classified or unclassified about the Einstein 2 PIA, so unless you have a copy of what was published, I can't speak to the specifics of what was in it.

Q Okay. Are you familiar with Einstein 3? Generally, not anything specific, but are you aware of the Department of Homeland Security's intrusion detection and intrusion prevention program known as Einstein 3 Accelerated?

MR. PATTON: Objection to beyond the scope of 30(b)(6), potentially classified. I'll have to rely on the witness, who may be more familiar with the DHS program certainly than me. If there's a unclassified answer, you can give it in your personal capacity.

MR. ABDO: Surely the existence of this program is unclassified, but --

MR. PATTON: I'm not willing to take the risk.

BY MR. ABDO:

Q Did you work on the Privacy Impact

Assessment for Einstein 3?

MR. PATTON: Same set of objections.

THE WITNESS: Generally speaking, yes, because every PIA that was approved by the Department of Homeland Security at that point was reviewed by me.

BY MR. ABDO:

Q Okay. Are you aware that Einstein 3 was part of the comprehensive cybersecurity initiative announced by the Obama administration?

A Yes.

MR. PATTON: Same objections.

THE WITNESS: Oh, sorry.

BY MR. ABDO:

Q And are you aware that, in announcing that, the administration also made clear that Einstein 3 was implemented with the technological support of the NSA?

MR. PATTON: Same objections.

THE WITNESS: Do you have a document that provides that information?

MR. ABDO: Sure.

(Deposition Exhibit 48 was marked for identification.)

BY MR. ABDO:

Q You have what's been marked as Exhibit 48 in front of you, Ms. Richards.

Do you recognize this document?

MR. PATTON: Object to this document as beyond the scope of 30(b)(6), but the witness can answer this and any other series of questions you have that have unclassified answers and are within her personal knowledge.

THE WITNESS: Yes, I've seen this document before. It's been quite some time.

BY MR. ABDO:

Q Can you tell us what it is?

A It's the Comprehensive National Cybersecurity Initiative.

There it is. Look at that.

Q Would you turn to page 3 of it, about halfway down, two-thirds of the way down, the sentence beginning, "DHS is currently conducting a[n] exercise" -- I think they meant an

exercise -- "to pilot the EINSTEIN 3 capabilities described in this initiative based on technology developed by NSA to solidify processes for managing and protecting information gleaned from observed cyber intrusions."

A Yes.

Q So is it true that the Einstein 3 program was piloted based on technology developed by the NSA?

MR. PATTON: Just a moment.

(Counsel conferring.)

THE WITNESS: Do you have the date of this document?

BY MR. ABDO:

Q I believe it's 2010, but I don't know off the top of my head.

A Could I see your Einstein 3 PIA?

Q We've got another copy of it. Can we mark this too, Dawn?

(Deposition Exhibit 49 was marked for identification.)

BY MR. ABDO:

Q So just for the record, you're now looking at what's been marked as Exhibit 49.

Do you recognize that?

A Yes.

Q What is that document?

A The Privacy Impact Assessment for the National Protection and Programs Directorate, Department of Homeland Security, Einstein 3 Accelerated (E3A), dated April 19th, 2013.

Q Okay. And for the record, you participated in the drafting of that assessment?

A I reviewed it.

Q Okay. If you're not quickly familiar with the answer to a question, that's fine, we can move on. I was just asking whether the Comprehensive National Cybersecurity Initiative --

A So my answer to you --

MR. PATTON: Just a second.

THE WITNESS: I'm sorry.

MR. PATTON: Just preserving my objection that both Exhibit 48 and Exhibit 49,

that series of questions are outside the scope of 30(b)(6), and the witness is answering in her personal capacity.

THE WITNESS: To the extent that the CNCI information is from 2010, stating something specific about NSA-developed technology, and not having reviewed this in almost five years, I would have to look at those and really understand whether what was described in 2010 actually got implemented in 2013.

MR. ABDO: Understood. Okay.

MR. GILLIGAN: Sorry, is that 49 there?

MR. ABDO: 49, yeah.

THE WITNESS: I can read it if you would like me to, but --

BY MR. ABDO:

Q No, that's okay.

Is it correct that in upstream collection that NSA obtains what it calls transactions?

A Internet transactions.

Q Internet transactions. Sorry, yes, internet transactions.

A Yes.

Q Do the Internet packets that constitute a single Internet transaction have a common destination?

MR. PATTON: Objection. Just a second.

(Counsel conferring.)

MR. PATTON: We're just trying to see if there's an unclassified response to that.

THE WITNESS: Uh-uh.

MR. PATTON: Objection, calls for a classified response and information subject to the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Instructions will be followed.

BY MR. ABDO:

Q Okay. Do the Internet packets that constitute a single Internet transaction have a common source?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MR. ABDO:

Q Are you familiar with the term "flow" or "network flow" as used in the context of Internet communications?

MR. PATTON: Objection, it's beyond the scope of 30(b)(6), and it's calling for an expert opinion.

THE WITNESS: I am, but don't make me define them.

BY MR. ABDO:

Q Is an Internet transaction, as understood by the NSA, the same as a flow or network flow as used in the context of Internet communications?

MR. PATTON: Just a moment. I don't think she can answer that.

THE WITNESS: Uh-uh, no. No, I can't answer that.

(Counsel conferring.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: And will follow the instruction.

BY MR. ABDO:

Q And the reason you can't answer is because it would disclose classified information?

A No.

Q Not because you're not familiar with the definition of "flow"?

A No, not because -- no, that is correct. I know what flow is, I just don't -- that's classified.

Q Okay. Is the definition of "flow" classified?

MR. PATTON: Objection, beyond the scope.

BY MR. ABDO:

Q In general as that term is commonly used in the network communications industry?

MR. PATTON: Objection, it's beyond

the scope, and calling for telecommunications expert opinion.

THE WITNESS: As you've just described, it's the general meaning. There's no specific definition. Internet transaction is an NSA definition. It's not a commonly understood telecommunications one.

So it, like -- there was one another we had earlier today. So there's sort of different groups of NSA-specific versus the outside world would know what they are. "Internet transaction" is one of those.

BY MR. ABDO:

Q What about network flow, flow or network flow?

A Those would be the normal everyday use of the words.

Q In other words, the NSA doesn't have a special definition of that term?

A Correct.

Q Okay. Can we take a five-minute break?

MR. PATTON: Sure.

(A break was taken at 5:21 p.m.)

(Resume at 5:35 p.m.)

EXAMINATION BY COUNSEL FOR

WIKIMEDIA FOUNDATION AND THE ACLU

BY MR. TOOMEY:

Q Ms. Richards, so I'm going to be asking some --

MR. ABDO: Why don't you introduce yourself.

BY MR. TOOMEY:

Q I'm Patrick Toomey. I'm counsel for Wikimedia Foundation from the American Civil Liberties Union.

So carrying on, in the course of upstream surveillance, does the NSA review the contents of communications as they are in transit on the Internet backbone?

MR. PATTON: Objection, calls for information that's classified, subject to state secrets, and the other statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q Let's focus on the period of June 2015 for the questions that follow.

In the course of upstream surveillance in June 2015, did the NSA review the contents of communications as they were in transit on the Internet backbone?

MR. PATTON: Same objections, same instructions.

THE WITNESS: Will follow the -- oh.

MR. PATTON: There are unclassified facts that could come out with different questions, but for that particular phrasing, instruct her not to answer.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June 2015, did the NSA scan the contents of communications as they were in transit on the

Internet backbone?

MR. PATTON: Let me just confer, because there's a specific phrase that you're using that I think is causing both NSA counsel and I as a basis to object on classified information. So I don't want to appear we're overclassifying Einstein 3.

MR. GILLIGAN: So we can go off the record.

MR. TOOMEY: Let's go off the record for a minute.

(Off the record at 5:37 p.m.)

(Resume at 6:23 p.m.)

MR. PATTON: Can remind us of where we were?

MR. TOOMEY: Yes. We're going back on the record, and, Ms. Jaques, if you could read back the previous question, please.

(The reporter read back the question.)

MR. PATTON: Objection to the question to the extent it calls for classified information and information protected by the statutory

privileges. The witness can answer the question to the extent unclassified.

THE WITNESS: So I think what you're asking is sort of a two-part question, and so I wanted to unpack and provide the unclassified aspects of it, and then sort of acknowledge that we've got the classified.

So as part of the upstream, we scan the content of the Internet transactions, and we did that in 2015.

As to the question of basically the in transit or the location, that piece is classified.

BY MR. TOOMEY:

Q Thank you. In June of 2015, in the course of upstream surveillance, did the NSA scan the application layer data of communications that transit the Internet backbone?

MR. PATTON: I'm just listening to your question. There's a slight difference in that that I just need to consult.

(Counsel conferring.)

MR. PADGETT: Could you read the

question?

(The reporter read back the question.)

THE WITNESS: It's classified.

MR. PATTON: There's something unclassified.

MR. PADGETT: Can we just go off the record for a second?

(Off the record at 6:26 p.m.)

(Resume at 6:28 p.m.)

MR. PATTON: And there may be a lot of these back and forth on this, so ...

THE WITNESS: Can you repeat the question, please?

(The reporter read back the question.)

MR. PATTON: Objection to the extent it calls for classified information or information protected by the statutory privileges.

The witness can answer to the extent unclassified about June 2015.

THE WITNESS: So to make sure I'm accurately -- I want to make sure I'm understanding the question and making the

distinction.

So what you're saying is what I just said was part of upstream in 2015, we scanned the content of Internet transactions.

Your next question is are we -- is NSA scanning the application layer of the Internet -- of the Internet -- that doesn't make sense -- if we're scanning the Internet -- I'm sorry, the application layer?

BY MR. TOOMEY:

Q Yes. The question is, in June 2015, did the NSA scan the application layer data of communications that transit the Internet backbone?

MR. PATTON: Same objection, same instruction.

THE WITNESS: The answer is yes for 2015, that we scan certain application data of communications that transit the Internet backbone.

BY MR. TOOMEY:

Q When you say certain --

A Mm-hmm, that's important.

Q -- application layer data, what you

mean by "certain"?

MR. PATTON: Objection, misstates prior testimony. Same objections as before, same instruction.

THE WITNESS: I can't go any further. It's classified.

BY MR. TOOMEY:

Q In unclassified terms, in June 2015, how did the NSA determine whether an Internet transaction contained a selector?

MR. PATTON: Object to the extent it calls for -- the whole answer would be classified. The witness can answer to the extent unclassified.

THE WITNESS: I just want to refer to see if there's any additional information I can provide to you beyond what we've already given to you.

There's no additional information beyond what was provided in the Interrogatories 3, 4 and 5, so there's no additional unclassified information beyond the fact that that's conducted.

BY MR. TOOMEY:

Q Is there any classified information that would be responsive to that question?

A Yes. This is necessarily incomplete because of the classified nature of the program.

Q And you're --

MR. PATTON: We're still talking about June 2015?

MR. TOOMEY: That's correct, yes.

THE WITNESS: Still June 2015, yes.

BY MR. TOOMEY:

Q And you're refusing to provide that information on the basis of an instruction from your lawyer?

MR. PATTON: I haven't instructed her on that, but her answer did indicate what was unclassified, which was the interrogatory responses to 3, 4 and 5, I believe she said, and I believe she also said that anything else beyond that was classified.

And there wasn't a pending question, but to the extent that you asked her a question

such as tell me what that classified information is, I would instruct her not to answer.

BY MR. TOOMEY:

Q Understood. Thank you.

Today does the NSA scan the application layer data of communications that transit the Internet backbone?

MR. PATTON: Objection, calls for information that's classified, subject to the statutory privileges before mentioned, and instruct the witness not to answer.

THE WITNESS: I follow those instructions.

BY MR. TOOMEY:

Q In June of 2015, if a transaction was scanned by the NSA in the course of upstream surveillance, and the NSA determined that it did not contain a selector, was the communication eliminated?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PADGETT: Can you read the

question back?

(The reporter read back the question.)

MR. PATTON: Can we just go off the record for a second?

MR. TOOMEY: Can we go off the record?

(Off the record at 6:34 p.m.)

(Resume at 6:37 p.m.)

(The reporter read back the question.)

MR. PATTON: Object to that question to the extent it calls for classified information or otherwise privileged information.

The witness can answer to the extent unclassified.

THE WITNESS: So the process by which Internet transaction is filtered, and then scanned, if it doesn't have a test selector or isn't about the target, then that means that information will not be ingested into the NSA repository.

BY MR. TOOMEY:

Q And is that communication eliminated?

MR. PATTON: Objection. The question

calls for a classified answer, as well as an unclassified one, which the witness has already given.

The witness can answer again and provide the unclassified answer.

THE WITNESS: I have nothing additional beyond. If you'd like me to repeat what I said, I'd be happy to.

BY MR. TOOMEY:

Q No need to repeat.

And to the extent there is -- is there classified information that you are not providing in response?

A Yes.

Q Today, does the NSA seek to acquire email communications to and from its targets using upstream surveillance?

MR. PATTON: Object to the question. It calls for classified information and information protected by the statutory privileges.

I instruct the witness not to answer.

THE WITNESS: I will follow

instructions.

BY MR. TOOMEY:

Q Could you please describe as fully as possible how, in June 2015, the NSA determined whether an Internet transaction contained a selector?

MR. PATTON: Objection to the extent it calls for classified information, or information otherwise protected by the statutory privileges.

The witness can answer if she can regarding the unclassified response to that question.

THE WITNESS: There's no additional unclassified information beyond what I've already said.

BY MR. TOOMEY:

Q Thank you. Beyond what you've already said or what appears in the NSA's discovery responses, could you please describe as fully as possible how the NSA today determines whether an Internet transaction contains a selector?

MR. PATTON: Objection. The question calls for classified information and information protected by the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will --

MR. ABDO: Rodney, can we just try to compress if it's the same objection? Thanks.

MR. PATTON: If you ask the same -- exactly those kind of questions, I will do my best. Thank you.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June 2015, did the NSA scan communications in bulk?

MR. PATTON: Objection, calls for classified information. Just check and see if there's a --

(Counsel conferring.)

MR. PATTON: Just a second. Can we go off the record?

(Off the record at 6:40 p.m.)

(Resume at 6:43 p.m.)

MR. TOOMEY: Can you please repeat the question?

(The reporter read back the question.)

MR. PATTON: Objection. We'd need to go into the SCIF to discuss whether or not there's an unclassified response to this.

THE WITNESS: But before we do that, can you give a definition of what you mean by "bulk," scanning communications in bulk?

BY MR. TOOMEY:

Q Does the NSA ever use the term "bulk" in connection with surveillance activities?

A Yes.

Q And what do you understand the NSA to mean by the term "bulk"?

A To do collection without -- let's see, the definition is in Presidential Policy Directive No. 28, which I don't have with me, but it's something roughly along the lines of collection without discriminates.

Q That document describes bulk collection to the best of your recollection?

A Yeah.

Q Yes?

A Or it has a general description of it, and then carries on to provide when NSA can conduct bulk -- for what purposes the information can be used.

Q And so my question here is about whether in June 2015, in the course of upstream surveillance, the NSA scanned communications in bulk?

MR. PATTON: Go off the record.

(Off the record at 6:45 p.m.)

(Resume at 6:57 p.m.)

(The reporter read back the question.)

MR. PATTON: Objection to the extent it calls for classified information and information protected by the statutory privileges.

Instruct the witness to answer the question to the extent able in unclassified terms.

THE WITNESS: So in terms of

unclassified, the best information I can give to you is in the PCLOB report, which is Deposition Exhibit 43, page 103. The last line of the first paragraph that states the program does not operate by collecting communications in bulk.

BY MR. TOOMEY:

Q Could you please answer my question about whether in June 2015 the NSA scanned communications in bulk?

MR. PATTON: Objection. The answer to that question, to the extent not already provided by the witness, is classified and subject to statutory privileges.

Instruct the witness not to answer.

MR. GILLIGAN: And state secrets. Did you say state secrets?

MR. PATTON: I said classified. I'm trying to shorten it.

MR. GILLIGAN: Oh, okay. We're all for that.

MR. PATTON: Also subject to the state secrets privilege.

THE WITNESS: I will follow the instructions of my counsel.

BY MR. TOOMEY:

Q In the context of upstream surveillance, is scanning a communication different from collecting a communication?

A Yes.

Q In the course of upstream surveillance today, does the NSA scan communications in bulk?

MR. PATTON: Objection. The question calls for information that's classified, subject to the state secrets, and to the statutory privileges. Instruct the witness not to answer.

THE WITNESS: I will not answer.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA scan the metadata of communications in bulk?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance in 2015, did the NSA copy communications in bulk?

MR. PATTON: Same objection, same instructions.

THE WITNESS: Follow instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA copy communications in bulk?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June of 2015, did the NSA deliberately attempt to filter out any of Wikimedia's international communications?

MR. PATTON: Objection. Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA deliberately attempt to filter out any of Wikimedia's international communications?

MR. PATTON: Same instruction, same objections.

THE WITNESS: Will follow instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June of 2015, did the NSA deliberately attempt to filter out all of Wikimedia's communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA deliberately attempt to filter out all Wikimedia communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow

instructions.

BY MR. TOOMEY:

Q Does the NSA contend as a factual matter in this case that it deliberately filters out all Wikimedia communications?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Could you go off the record?

(Off the record at 7:01 p.m.)

(Resume at 7:08 p.m.)

MR. TOOMEY: Could you read back the last question?

(The reporter read back the question.)

MR. PATTON: Object to the question as beyond the scope of 30(b)(6), improper 30(b)(6) question. The witness can answer in her personal capacity.

THE WITNESS: In my personal capacity, I have no idea, but to the extent that we do or do not filter something out would be classified in any event.

BY MR. TOOMEY:

Q Does anyone at the NSA know whether the NSA contends in this case, as a factual matter, that it deliberately filters out all Wikimedia communications?

MR. PATTON: Same objections, same instruction.

THE WITNESS: It's classified. I mean --

MR. PATTON: That's not the question he's asking.

THE WITNESS: That's not the question.

MR. PATTON: That's not the question he's asking.

THE WITNESS: So same answer, which I have no idea, and to the extent it is or isn't would be classified.

BY MR. TOOMEY:

Q To the extent it is or isn't what?

A Filtering out Wikimedia, as you were contending in your question.

Q My question is whether the NSA

contends that it is filtering out Wikimedia's communications. Do you know the answer to that question?

MR. PATTON: Objection. Same objections as before, and adding asked and answered.

THE WITNESS: I have nothing else to say on the topic.

MR. TOOMEY: Ms. Jaques, could you mark as the next exhibit this document, please?

(Deposition Exhibit 50 was marked for identification.)

BY MR. TOOMEY:

Q So the court reporter has handed Ms. Richards Exhibit 50, which is titled Memorandum of Points and Authorities in Support of Defendant's Motion to Compel Discovery. Sorry, we don't have as many copies of this one, sorry.

Could you please tell me what this document is?

MR. PATTON: Objection, lacks foundation.

BY MR. TOOMEY:

Q You can answer.

Have you seen this document before?

A I have not seen this document before.

Q Can you read the title of the document, please?

A Sure. Memorandum of Points and Authorities in Support of Defendant's Motion to Compel Discovery, dated March 26, 2018.

Q Thank you. Could you please turn to page 11 --

A Sure.

Q -- of Exhibit 50?

I'm going to read a sentence from the document in the last paragraph toward the bottom of the page.

"An entity seeking to conduct surveillance on the Internet that lacks the ability to decipher encrypted HTTPS communications may well decide to program its surveillance equipment to disregard such communications altogether."

Has the NSA programmed its surveillance equipment to disregard HTTPS communications altogether?

MR. PATTON: Objection, the question calls for classified information protected by the state secrets privilege and information protected by the statutory privileges.

Instruct the witness not to answer the question.

THE WITNESS: I'll follow the instructions.

BY MR. TOOMEY:

Q Can we now turn to page 12 of Exhibit 50. I'm going to read a passage from the first paragraph toward the top of the page.

"If the NSA lacked the ability to decipher HTTPS communications," dot dot dot, "then nothing --

MR. PATTON: It's an important dot dot dot.

MR. TOOMEY: We'll get there. I'm going to start again. I'm going to read the

passage again.

"If the NSA lacked the ability to decipher HTTPS communications ... then nothing in the 'technical rules of how the Internet works' ... would prevent the configuration of devices used in connection with Upstream surveillance to exclude HTTPS communications."

Does the NSA have the ability to decipher HTTPS communications?

MR. PATTON: Objection, outside the scope of 30(b)(6), and the question calls for classified information protected by the state secrets privilege, statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q I'm going to read a passage now from page 12 of Exhibit 50 in the second paragraph toward the bottom of the page.

"If the NSA deemed communications to and from Wikimedia's websites to be of low

foreign-intelligence value, then nothing in the technical rules of the Internet would prevent the configuration of equipment used in connection with Upstream surveillance to ignore all communications having source or destination IP addresses associated with Wikimedia."

Has the NSA configured its surveillance equipment to ignore all communications having source or destination IP addresses associated with Wikimedia?

MR. PATTON: Objection, beyond the scope of 30(b)(6), and objection, it calls for classified information, subject to state secrets, statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Does the NSA deem communications to and from Wikimedia's websites to be of low foreign intelligence value?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: Will follow instruction.

BY MR. TOOMEY:

Q Would the NSA be permitted under upstream surveillance today to collect a targets communications with a U.S.-based website?

A How is this question different than the last one?

MR. PATTON: I'm not sure it is.

THE WITNESS: Okay.

MR. PATTON: Can we go off the record?

(Off the record at 7:16 p.m.)

(Resume at 7:23 p.m.)

BY MR. TOOMEY:

Q Back on the record.

Ms. Jaques, could you please read back the prior question?

(The reporter read back the question.)

MR. PATTON: We object to that question. It calls for a classified answer.

The witness has reviewed during the break the currently applicable declassified and

public targeting procedures, and there's no unclassified answer we can give. So as a result, we object to the question, it calls for classified information, subject to the state secrets and subject to the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I'll follow the instructions.

BY MR. TOOMEY:

Q Is it possible that a targets communications with Wikimedia could contain foreign intelligence information that would be of interest to the NSA?

(Counsel conferring.)

MR. PATTON: You'll like this one.

Object as beyond the scope of 30(b)(6) and speculative. The witness can answer in her own capacity to the extent the answer is unclassified.

THE WITNESS: It's speculative. I can't speak to who would or wouldn't be, what particular individual might be targeted. If an

analyst decides a particular selector or person meets the targeting standards, then that would be appropriate.

BY MR. TOOMEY:

Q Could the term "foreign intelligence information" encompass information that a person surveilled using upstream surveillance is reading on one of Wikimedia's websites?

MR. PADGETT: Could I get that read back?

(The reporter read back the question.)

MR. PADGETT: Do you want to talk about it? Let's go off the record.

(Off the record at 7:26 p.m.)

(Resume at 7:28 p.m.)

MR. TOOMEY: Ms. Jaques, could you please read back the last question?

(The reporter read back the question.)

MR. PATTON: Objection, beyond the scope of 30(b)(6), speculative, and calls for legal conclusion. The witness can answer in her personal capacity.

THE WITNESS: I'm sorry, can you read that question one more time?

(The reporter read back the question.)

MR. PATTON: Same objections.

THE WITNESS: Can we go off the record? Sorry.

(Off the record at 7:30 p.m.)

(Resume at 7:32 p.m.)

MR. PATTON: Same objections, same instruction.

THE WITNESS: So you have a couple of different things, which is why we kept having to walk outside to unpack that, and so I want to unpack what's classified and what's unclassified.

So the first part of your question would be is there possibly foreign intelligence information on the Wikimedia sites, to which the answer, from my perspective, is there could be. I don't actually know. I haven't trolled through the Wikimedia websites, but it's possible.

The second part of that question had to do with how it would function in the upstream

context, and that piece of it is what's classified.

BY MR. TOOMEY:

Q Similar question, could the term "foreign intelligence information" encompass information that a person surveilled using upstream surveillance is contributing to one of Wikimedia's websites?

MR. PATTON: Same objections, same instruction.

THE WITNESS: I would give the same answer, which is I would separate those two pieces to say it's possible that somebody at one of your contributors is creating foreign intelligence information in a hypothetical. I don't actually know.

To the extent it has anything to do with upstream, any piece of that would be classified.

BY MR. TOOMEY:

Q And you're not answering that portion to that aspect of the question based on your

lawyer's instruction?

A Correct.

MR. PATTON: Not based on my instruction. When we broke the last time, the witness had a question as to what aspect of this that she could talk about. She provided the information that she could talk about and indicated to you there's another classified component, and the nature of that classified information, and she declined to answer based on that.

Had you asked her a follow-up question as to the content of that classified information, I would have instructed her not to answer.

BY MR. TOOMEY:

Q Could you please provide any classified information that you believe my question calls for?

MR. PATTON: I respect that question. It keeps our record clean.

Object to the question to the extent it calls for classified information, information

subject to the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow those instructions.

BY MR. TOOMEY:

Q Today, does the NSA intentionally attempt to filter out all HTTPS communications from upstream surveillance?

MR. PATTON: Objection, the question calls for classified information, subject to the state secrets and to the statutory privileges.

Instruct not to answer.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Same question, but for June 2015. Did the NSA at that time intentionally attempt to filter out all HTTPS communications from upstream surveillance?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Will follow the

instruction.

BY MR. TOOMEY:

Q Today, does the NSA intentionally attempt to filter out all Internet communications that use TCP port 443?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally attempt to filter out all Internet communications that used TCP port 443?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q Today, does the NSA intentionally filter out all encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally filter out all encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q Today, does the NSA intentionally filter out all open VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally filter out all open VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Today does the NSA intentionally filter out Wikimedia's encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally filter out Wikimedia's encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Can you please describe in as much detail as necessary to provide a complete answer how the NSA implemented any changes to "about" collection during or after April 2017?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Object to the question to the extent it calls for classified information and information protected by the statutory privileges.

If there is an unclassified response, the witness can provide it.

MR. TOOMEY: Rodney, to be clear, just so we can try to consolidate things, are you also instructing the witness not to provide any unclassified information?

MR. PATTON: No. I'm instructing --

MR. TOOMEY: Sorry, any classified information, just so --

MR. PATTON: I would love her to provide any unclassified information, but if there's any classified information, I'm instructing her not to answer.

There may be some unclassified information that she can provide, and that's what I'm authorizing her to do.

THE WITNESS: As of 2017, April 2017, NSA changed the way it did its upstream collection

so that it no longer collected the "abouts" collection.

There's not any additional information beyond the information that was either in the 2017 opinion or our associated unclassified information that NSA put out on its website.

MR. PATTON: That's the April 2017 FISC opinion?

THE WITNESS: Sorry, yes, the April 2017 FISC opinion.

BY MR. TOOMEY:

Q Besides the information you just identified, is there any other unclassified information that you could provide to this question?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Not that I'm aware of.

BY MR. TOOMEY:

Q Is there classified information that would answer the question that you are not providing at the instruction of your attorney?

MR. PATTON: Objection to the extent it calls for classified information.

If the witness's answer is yes or no, she can provide that information.

THE WITNESS: Yes.

BY MR. TOOMEY:

Q Apart from the information you identified in response to my last question, could you please describe how the NSA attempts to avoid collecting communications that are solely about a selector?

MR. PATTON: Object to the form of the question, vague as to time. Potentially classified.

(Counsel conferring.)

MR. PATTON: Would you mind rephrasing to specify the time period?

MR. TOOMEY: Sure, I'll rephrase.

MR. PATTON: Thanks.

BY MR. TOOMEY:

Q Apart from the unclassified information that you provided in response to my

last question, could you please describe in as much detail as necessary to provide a complete answer how, after April 2017, the NSA attempts to avoid collecting communications that are solely about a selector?

(Counsel conferring.)

MR. PATTON: Can we go off the record?

(Off the record at 7:42 p.m.)

(Resume at 7:43 p.m.)

MR. PATTON: Would you mind reading back the question, please?

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for classified information.

If the witness's answer is yes or no, she can answer that.

THE WITNESS: There's no additional information beyond what I've pointed to. I have no additional --

BY MR. TOOMEY:

Q There's no additional unclassified information?

A No additional unclassified information.

Q And is there classified information that you're not providing at the instruction of your counsel?

A Yes.

Q Apart from the unclassified information that you provided in response to my question, my previous question, please describe in as much detail as necessary to provide a complete answer how the change in April 2017 affected the filtering of communications subject to upstream surveillance?

(Counsel conferring.)

MR. PATTON: Can we go off the record?

(Off the record at 7:45 p.m.)

(Resume at 7:59 p.m.)

MR. TOOMEY: Could you please read back the last question?

(The reporter read back the question.)

MR. PATTON: Objection to the question to the extent it calls for classified information

and information subject to the statutory privileges.

To the extent the witness is aware of an unclassified answer, she may provide a response.

THE WITNESS: The only point I would provide to you on this, which is not necessarily anything new, but we still stand behind the information about how the filtering works in our Civil Liberties and Privacy Office Report, and that remains true today as it did in 2014, when we wrote the report.

BY MR. TOOMEY:

Q Is there classified information you're not providing in response to my question at the instruction of your lawyer?

A Yes.

Q Thank you. Similar question, apart from the unclassified information that you've already provided today, could you please describe in as much detail as necessary to give a complete answer how the change in April 2017 affected the

scanning of communications subject to upstream surveillance?

MR. PATTON: Object to the question, calls for classified information and information subject to statutory privileges, and instruct the witness not to answer the question.

THE WITNESS: I will not answer.

BY MR. TOOMEY:

Q Apart from the unclassified information you've already provided today, please describe in as much detail as necessary to give a complete answer which portions of an Internet transaction are scanned for selectors after April 2017?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA first scan the contents of communications for selectors, and then discard those that are solely about a

selector?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA copy the contents of communications prior to scanning those communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA copy the application layer data of packets prior to scanning the communications to which they belong?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the

instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA review any portion of the contents of communications for selectors?

MR. PATTON: Object to the form, vague as to "review," and object to the question as seeking classified information, subject to the state secrets and statutory privileges, and instruct the witness not to answer.

THE WITNESS: Will follow the directions.

BY MR. TOOMEY:

Q Would your answer have been the same if I had said does the NSA scan any portion of the contents of communications for selectors --

MR. PATTON: One moment.

MR. TOOMEY: -- since April 2017?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Could you rephrase the question in terms of an Internet transaction?

It's fine if you don't, but that might take care of something.

MR. TOOMEY: Sure, let me rephrase.

BY MR. TOOMEY:

Q Since April 2017, does the NSA scan any portion of the contents of Internet transactions for selectors?

(Counsel conferring.)

MR. PATTON: I think we need to go off the record.

MR. TOOMEY: Let's go off the record.

(Off the record at 8:04 p.m.)

(Resume at 8:18 p.m.)

MR. TOOMEY: Could you please read back the prior question?

(The reporter read back the question.)

MR. PATTON: Objection to the question to the extent it seeks classified information and information protected by the statutory privileges.

The witness can answer the question to the extent that it's unclassified.

THE WITNESS: So NSA scans a portion

of the Internet transaction to identify the task selector in order to acquire the Internet transaction that is to or from the target.

To go any further in terms of whether it's in the content or the metadata, or any of those further things, is classified.

MR. PATTON: And I instruct her not to answer beyond that unclassified answer.

BY MR. TOOMEY:

Q And you're following your counsel's instruction?

A I am.

Q So just to confirm, what portions of the contents of Internet transactions are scanned for selectors since April 2017?

MR. PATTON: I was waiting for you to finish.

Objection to the extent that it mischaracterizes the prior testimony. The witness can answer the question to the extent it's unclassified. Any classified answer, I instruct her not to provide.

THE WITNESS: You're asking me what portion of the Internet transaction we're scanning, just so I'm clarifying?

BY MR. TOOMEY:

Q Correct, after April 2017.

A After April 2017?

I am not able to answer that question. The answer to that question is classified.

Q Since April 2017, does the NSA review the entire contents of communication of Internet -- let me strike that. I'll restate the question.

Since April 2017, does the NSA scan the entire contents of Internet transactions for selectors?

MR. PATTON: Objection, calls for classified information, information protected by the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q Since April 2017, does the NSA scan any portion of the application layer data of Internet transactions for selectors?

MR. PATTON: Same objection, same instructions.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q And if I were to ask what portions of Internet transaction the NSA scans for selectors, would your answer be the same?

MR. PATTON: Are we talking about post April 2017?

MR. TOOMEY: Yes, post April 2017.

MR. PATTON: Same objection, same instruction.

THE WITNESS: Yes, my answer would be the same.

BY MR. TOOMEY:

Q And since April 2017, does the NSA scan the entire application layer of Internet

transactions for selectors?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Are there any barriers to the NSA restarting "about" collection today?

MR. PATTON: Objection, beyond the scope of 30(b)(6) notice, calls for a legal conclusion.

THE WITNESS: NSA --

MR. PATTON: Just a second. There may be an additional objection.

(Counsel conferring.)

MR. PATTON: I would just add that to the extent that the question calls for a classified answer, I object to that based on the state secrets privilege and the statutory privileges. If there's an unclassified answer, the witness can provide.

And my colleague let's me know that

there's also a vagueness objection.

BY MR. TOOMEY:

Q You can answer to the extent --

A Sure. With the passage of the 702 FAA Reauthorization, there is a requirement for once the FISC has approved us going back to "abouts," that we have to give a 30-day notice to Congress before we can move forward with any type of collection.

MR. PATTON: Any type of "abouts" collection.

THE WITNESS: Any type of "abouts" collection. Apologies for not being clear.

BY MR. TOOMEY:

Q Do you consider that statutory requirement a barrier to the NSA restarting "about" collection?

MR. PATTON: Objection, beyond the scope of 30(b)(6), vague as to what a barrier is, calls for a legal conclusion.

The witness can answer in her own capacity.

THE WITNESS: Can you explain what you mean by barrier? I mean, to the extent -- yeah.

BY MR. TOOMEY:

Q I mean by barrier any obstacle, impediment to restarting "about" collection.

MR. PATTON: Same set of objections, and add in the one that to the extent there's any classified response to that, the witness should not answer as to classified information. You can otherwise provide an unclassified answer in your personal capacity.

THE WITNESS: Certainly getting FISC approval and notifying Congress are additional barriers beyond just being able to turn it on tomorrow.

BY MR. TOOMEY:

Q And could you please state whether there is any -- first of all, are there any other barriers besides the two that you just described?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Go off the record.

(Off the record at 8:25 p.m.)

(Resume at 8:36 p.m.)

MR. TOOMEY: All right, let's go back on the record.

THE WITNESS: Can you read it back?

(The reporter read back the question.)

THE WITNESS: Are you answering first or am I?

MR. PATTON: Sorry, putting this away.

Object to the question to the extent it calls for classified information and information protected by the statutory privileges.

The witness can answer the question to the extent unclassified.

THE WITNESS: So as noted, the FISC would have to approve us going back to doing "abouts," so we would have to address any of the underlying issues as it relates to getting the FISC approval, as were described in the 2017 Memorandum Opinion.

BY MR. TOOMEY:

Q What are those underlying issues?

MR. PATTON: Object to the question to the extent it calls for classified information and information protected by the statutory privileges.

The witness can answer the question to the extent unclassified.

THE WITNESS: So the two unclassified descriptions that were provided in the 2017 Memorandum Opinion indicated there were both technological issues, as well as human error issues.

BY MR. TOOMEY:

Q And what were those issues?

MR. PATTON: Objection to the extent it calls for classified information and information protected by the statutory privileges.

The witness can answer to the extent unclassified.

THE WITNESS: Could I have the 2017 so I can point you to those sections? Do you want to introduce that in? Is that what's coming next?

MR. TOOMEY: Could you please mark that?

(Deposition Exhibit 51 was marked for identification.)

BY MR. TOOMEY:

Q Please take a look at Exhibit 51 which the court reporter has just handed you.

Could you tell me, are you familiar with this document and what it is?

A Yes. This is the Memorandum Opinion and Order of the Foreign Intelligence Surveillance Court dated April 26, 2017.

So I will start with page 14 to 15 --

MR. GILLIGAN: Sorry, did we mark this?

THE WITNESS: Yes, it's 51.

So the first indication of this discussion is starting at the bottom of page 14. The sentence begins, "The October 26, 2016 Notice disclosed that an NSA Inspector General review and report and NSA Office of Compliance for Operation verification activities indicated that, with greater frequency than previously disclosed to the Court, NSA analysts had used U.S.-person

identifiers to query the results of Internet 'upstream' collection, even though NSA's Section 702 minimization procedures prohibited such queries."

BY MR. TOOMEY:

Q So if I could stop you there.

A Sure.

Q Is it accurate to say that the technical and human error issues that the FISC identified related to queries of the results of Internet upstream collection?

(Counsel conferring.)

MR. PATTON: If the answer is yes or no, the witness can answer the question.

THE WITNESS: Yes.

BY MR. TOOMEY:

Q Besides the barriers you already identified and what's described in Exhibit 51, are there any other barriers to the NSA restarting "about" collection?

MR. PATTON: Objection to the extent that it calls for classified information and

information protected by the statutory privileges.

If there's an unclassified answer the witness can provide, she can provide it.

THE WITNESS: I'm sorry, can we go off the record?

(Off the record at 8:42 p.m.)

(Resume at 8:43 p.m.)

THE WITNESS: To the extent that NSA considers budget, time, intelligence needs, risk to the agency, privacy and civil liberties impact, all of those will also be considered as NSA decides whether or not to spend its next intelligence needs to go into "abouts."

Whether that's a particular barrier or not, those are all considerations that NSA will take into consideration as it thinks about whether or not it should go forward with "abouts."

BY MR. TOOMEY:

Q Okay. Is there any other barrier you haven't already described?

A No.

Q Has the NSA disavowed any intention of

resuming "about" collection in the future?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Just object to beyond the scope of 30(b)(6). The witness can answer if she knows.

THE WITNESS: No.

BY MR. TOOMEY:

Q Has the NSA indicated to any member of Congress any interest in resuming "about" collection in the future?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Same objection as beyond the scope of 30(b)(6). The witness can answer if she's aware.

THE WITNESS: Admiral Rogers testified that he would consider going back up on "abouts" collection if he could make it through all the -- you know, if it met the needs -- met intelligence needs, and they were in a position to meet all the needs of the FISC and notification to Congress.

BY MR. TOOMEY:

Q Do you know when Admiral Rogers provided that testimony?

A I want to say roughly October time frame 2018 -- I'm sorry, sorry 2017 -- in the future. Somewhere in the September/October 2017. It might have been part of one of the threat briefings.

Q Do you know to whom he provided that testimony? Which congressional committee or --

A I believe it was SSCI, Senate Select Committee on Intelligence. I'm pretty certain that's who it was.

Q Thank you.

A It could have been part of an appropriations hearing, but ...

Q And was that testimony public testimony?

A Yes, it was.

Q Has the NSA indicated to the FISC any interest in resuming "about" collection in the future?

MR. PATTON: Objection.

(Counsel conferring.)

MR. PATTON: The objection is twofold. One, beyond the scope of 30(b)(6) and, two, object to the extent it calls for a classified answer, and also one subject to statutory privileges. But if the witness is personally aware of that fact and it's unclassified, she can answer.

THE WITNESS: The answer is classified, and I'm following the instructions of my lawyer.

BY MR. TOOMEY:

Q Has the NSA indicated to the FISC that it intends to resume "about" collection in the future?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Same answer.

MR. TOOMEY: Can we mark as the next exhibit, please, this document?

(Deposition Exhibit 52 was marked for identification.)

BY MR. TOOMEY:

Q Could you please take a look at Exhibit 52 and tell me if you recognize this document and what it is?

A I recognize this document. It is the NSA press release dated April 28, 2017, stating, "NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702."

Q Thank you. Let me move to a different -- can we please mark this document as Exhibit 53?

(Deposition Exhibit 53 was marked for identification.)

BY MR. TOOMEY:

Q Could you please take a look at this document, state whether you're familiar with it, and describe it.

A Yes, I am familiar with it. It is the statement from April 28th, 2017, stating, "NSA Stops Certain Section 702 'Upstream' Activities."

Q And I'm going to read a short passage from the first paragraph at the end, which says,

"After a comprehensive review of mission needs, current technological constraints, United States person privacy interests, and certain difficulties in implementation, NSA has decided to stop some of its activities conducted under Section 702."

Is that sentence accurate?

A Yes.

Q Did any court order the NSA to stop "about" collection?

MR. PATTON: One second.

(Counsel conferring.)

MR. PATTON: My only objection is to vagueness as to the term "stop" in the context of a court order.

MR. GILLIGAN: Beyond the scope.

MR. PATTON: It's also beyond the scope then.

MR. TOOMEY: You can answer.

THE WITNESS: Actually, I would just like more specificity. What are you -- I'm not sure I entirely understand.

If you read -- maybe I'll give a

little bit more answer. If you read on the second page of Exhibit 53, it states, "After considerable evaluation of the program and available technology, NSA has decided that its Section 702 foreign intelligence surveillance activities will no longer include any upstream internet communications that are solely 'about' a foreign intelligence target."

So could you be clearer of the particular court?

BY MR. TOOMEY:

Q Could you read me the title of Exhibit 53?

A Sure. NSA statement, "NSA Stops Certain Section 702 'Upstream' Activities," dated April 28th, 2017.

Q And my question is did any court order the NSA to stop "about" collection?

MR. PATTON: Same objections.

THE WITNESS: Can you describe what court you're talking about?

BY MR. TOOMEY:

Q I'm asking about any court.

A Any court?

Q But any court would include the FISC.

MR. PATTON: Same objections. Also, this particular one calls for a legal conclusion too. You can answer.

THE WITNESS: Okay.

So the Attorney General and the DNI put forward a set of targeting procedures to the FISC, and the FISC agreed with those procedures. There was no FISC ordering us to stop.

BY MR. TOOMEY:

Q Did Congress prohibit the NSA from conducting "about" collection in April of 2017?

MR. PATTON: Objection, vague as to April 2017. Same set of objections as before, beyond the scope of 30(b)(6), calls for a legal conclusion, vague.

THE WITNESS: No.

BY MR. TOOMEY:

Q Congress hasn't since prohibited the

NSA from restarting "about" collection, correct?

MR. PATTON: Objection, beyond the scope, calls for a legal conclusion.

THE WITNESS: With the passage of the 702 FAA Reauthorization, it puts in place a requirement for notification 30 days between when the FISC approves it and when we could start, unless there's extenuating circumstances.

BY MR. TOOMEY:

Q So that statute doesn't contain a prohibition on restarting "about" collection?

A Correct.

MR. PATTON: Same set of objections.

THE WITNESS: Correct.

BY MR. TOOMEY:

Q Today, does upstream surveillance involve the scanning of all international text-based communications on individual circuit or circuits the NSA is monitoring?

MR. PATTON: Objection, calls for classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow instructions.

MR. GILLIGAN: Could I hear the question again, please?

(The reporter read back the question.)

MR. GILLIGAN: Can we go talk, please? Off the record.

(Off the record at 8:57 p.m.)

(Resume at 9:22 p.m.)

BY MR. TOOMEY:

Q Let's go back on the record.

Ms. Jaques, could you please read back the last question?

(The reporter read back the question.)

MR. PATTON: Objection to the question, that calls for a classified answer, and also an answer that seeks information protected by the statutory provisions.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

MR. TOOMEY: So going forward, can we shorten that to assert state secrets and statutory privileges?

MR. PATTON: I will shorten it as fast as I can.

BY MR. TOOMEY:

Q In June 2015, did upstream surveillance involve the scanning of all international text-based communications on the individual circuit or circuits the NSA was monitoring?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Today, if some international text-based communications on a given circuit are not scanned, please explain in as much detail as necessary to completely answer why those communications are not scanned.

MR. PATTON: Please repeat the

question.

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for classified information and information protected by the statutory privileges.

The witness can answer the question to the extent that she is aware of an unclassified answer to that question.

THE WITNESS: Can you read the question one more time to make sure I have it entirely accurate?

(The reporter read back the question.)

THE WITNESS: As we were discussing in the existing Civil Liberties and Privacy Report, the process is that there's filtering, and then there's scanning. So to the extent that we have filtered wholly domestic communications out as part of that, those would not be scanned.

BY MR. TOOMEY:

Q Beyond that response and beyond the unclassified information you've already provided today, can you please fully explain in as much

detail as necessary why some communications are not scanned?

MR. PATTON: Object to the question, calls for classified information, information protected by the statutory privileges.

Instruct not to answer.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Same question as of June 2015. If you need me to restate the question, I can.

A Can you restate the question?

Q Apart from the unclassified information you've already provided today, as of June 2015, if some international text-based communications on a given circuit were not scanned, please explain in as much detail as necessary to fully answer why those communications are not scanned.

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Object to the question,

calls for classified information and information protected by the statutory privileges.

If there's any information that the witness is aware of that has not already been provided either in the interrogatory responses or in the prior testimony that would answer that question, she can go ahead and give it.

If not, I would instruct her not to answer the question based on those privileges.

THE WITNESS: There's no additional information, so I'll follow counsel's directions.

BY MR. TOOMEY:

Q There's no additional unclassified information?

A There's no additional unclassified information that I can provide you beyond what we've already provided you.

Q And there is classified information which you're not providing based on your counsel's instruction?

MR. PATTON: To the extent that the answer to that question is yes or no, you can

answer the question.

THE WITNESS: Yes, that's correct.

MR. TOOMEY: Thank you. Let's go off record.

(Off the record at 9:29 p.m.)

(Resume at 9:39 p.m.)

EXAMINATION BY COUNSEL FOR PLAINTIFFS

BY MS. HANLEY COOK:

Q Hi, I'm Devon Hanley Cook. We spent the day together, but nice to meet you. I want to thank you for your patience and for putting up with all our questions and going so late today. I also want to thank you, Dawn. I know it's been a really long day for everybody.

Does NSA now scan Wikimedia's communications in the course of upstream surveillance?

MR. PATTON: Objection, calls for classified information, subject to state secrets privilege and to statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the

instructions.

BY MS. HANLEY COOK:

Q In 2015, did NSA scan Wikimedia communications in the course of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Does NSA now copy Wikimedia communications in the course of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q In June 2015, did NSA copy Wikimedia communications in the course of upstream surveillance?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Has NSA acquired Wikimedia communications as a result of upstream surveillance now?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q As of June 2015, had NSA acquired Wikimedia communications as a result of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MS. HANLEY COOK:

Q Can I have Tab X, please? Let's save time, let's do X and Y, please.

MR. GILLIGAN: 54 and 55 then?

THE REPORTER: Yes, 54 and 55.

(Deposition Exhibits 54 and 55 were marked for identification.)

BY MS. HANLEY COOK:

Q Let's start with Exhibit 54.

Have you seen Exhibit 54 before?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Object to the question as beyond 30(b)(6). The witness can answer yes or no if she has personally seen this Exhibit 54 before.

THE WITNESS: No.

BY MS. HANLEY COOK:

Q If you assumed that Exhibit 54 related to upstream surveillance, it would indicate, wouldn't it, that the NSA had an intelligence interest in Wikimedia's communications, wouldn't it?

MR. PATTON: Object to the question, calls for a classified answer, subject to the state secrets privilege and to the statutory

privileges.

Instruct the witness not to answer the question.

THE WITNESS: Will follow those instructions.

BY MS. HANLEY COOK:

Q Turning to Exhibit 55, have you seen this document before? Actually, let me -- Exhibit 54. Recognizing that you have not seen the document before, what do you think it is?

MR. PATTON: Objection. Same objection as before, same instruction.

THE WITNESS: Which instruction was that? Classified?

MR. PATTON: Classified, subject to the state secrets privilege and to statutory privileges.

The witness is instructed not to answer the question.

THE WITNESS: I will follow those instructions. I just had to make sure I knew what the instructions were.

BY MS. HANLEY COOK:

Q Makes sense.

Exhibit 55, have you seen this document before?

MR. PATTON: Object to the question to the extent it's beyond 30(b)(6). The witness can answer yes or no if she has seen this document in her personal capacity.

THE WITNESS: Yes.

BY MS. HANLEY COOK:

Q What is it?

MR. PATTON: Object to the question, calls for a classified answer, subject to the state secrets and to statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow those instructions.

BY MS. HANLEY COOK:

Q If you assumed that Exhibit 55 related to upstream surveillance, it would indicate, wouldn't it, particularly on the second page in the first bullet point, that the NSA has an

intelligence interest in Wikimedia's HTTP communications, wouldn't it?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow those instructions.

BY MS. HANLEY COOK:

Q Do Exhibits 54 or 55 relate to upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow those instructions.

BY MS. HANLEY COOK:

Q At this time, HTTP communications are scanned for selectors in the course of upstream surveillance, aren't they?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Same objection, same instructions. Do you need a reminder on the --

THE WITNESS: I just need to remind

what --

MR. PATTON: Do you need the question read back?

THE WITNESS: Could you read the question again?

(The reporter read back the question.)

MR. PATTON: Object to the question, calls for classified information, information protected by the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow those instructions.

BY MS. HANLEY COOK:

Q As of June 2015, HTTP communications were scanned for selectors in the course of upstream surveillance, right?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MS. HANLEY COOK:

Q At this time, HTTPS communications are

scanned for selectors in the course of upstream surveillance, aren't they?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Same question as to the June 2015 time frame.

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Are Apache Kafka communications scanned for selectors in the course of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Do you know what Apache Kafka communications are?

MR. PATTON: Object to the question, beyond the scope, calls for expert testimony.

The witness can answer in her personal capacity.

THE WITNESS: Not well enough to describe to you.

BY MS. HANLEY COOK:

Q Open VPN communications are scanned for selectors in the course of upstream surveillance, aren't they?

MR. PATTON: Objection, vague as to time period, calls for classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q As of June 2015, were open VPN communications scanned for selectors in the course

of upstream surveillance?

MR. PATTON: Same objection without the vague as to time.

Same instruction not to answer.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Other than public documents, public documents at large, hearing testimony that is transcribed, public documents you reviewed, documents that have been filed or served in this case, or your testimony today, what can you tell me about the volume of communications subject to upstream surveillance at this time using any unit of measurement you want to discuss volume of communications?

MR. PATTON: Just one moment.

Can we go off the record?

(Off the record at the 9:49 p.m.)

(Resume at 9:49 p.m.)

MR. PATTON: Could you read back the question, please?

(The reporter read back the question.)

MR. PATTON: Other than the officially disclosed government statements, whether they be publicly by ODNI or by NSA or filed in this particular case or filed in the FISC and declassified, any other information that the witness would have would be classified, and so I would instruct her not to answer the question based on the state secrets privilege and statutory privileges.

THE WITNESS: I'll follow the instructions.

BY MS. HANLEY COOK:

Q Okay. How many communications -- and you can use any unit of measurement you want -- did NSA retain as a result of upstream surveillance in each of the last three years?

MR. PATTON: Objection, vague as to the term "communication," and classified, subject to the state secrets privilege and statutory privileges, and instruct not to answer.

THE WITNESS: Will follow the

instruction.

BY MS. HANLEY COOK:

Q Same question as to transactions.

MR. PATTON: Same objections except for vagueness, same instruction.

THE WITNESS: I will follow the instructions.

BY MS. HANLEY COOK:

Q What is the volume of communications copied in the course of upstream surveillance in each of the last three years?

MR. PATTON: Objection, vague. Objection, seeks classified information protected by the state secrets privilege, statutory privileges, instruct not to answer.

THE WITNESS: I will follow the instructions.

BY MS. HANLEY COOK:

Q Same question as to transactions.

MR. PATTON: Same objections with exception of vagueness, same instruction.

THE WITNESS: Following the

instructions.

BY MS. HANLEY COOK:

Q What is the volume of communications or transactions that are subject to filtering in the course of upstream surveillance in the last three years?

MR. PATTON: I'm sorry, did you use the term "Internet transactions"?

MS. HANLEY COOK: No.

MR. PATTON: I'm sorry, could you read the question back?

(The reporter read back the question.)

MR. PATTON: Objection, vague as to communications, and objection to the rest for the same reasons set forth before, instruct not to answer.

THE WITNESS: Will follow the instructions.

BY MS. HANLEY COOK:

Q Would the answer be the same if I used the term "Internet transactions"?

MR. PATTON: The instruction not to

answer would be the same, but there would be no vagueness objection, if that helps, or deemed compound since it was previous communications or transactions, but the instruction not to answer would remain the same, yes.

(Deposition Exhibit 56 was marked for identification.)

BY MS. HANLEY COOK:

Q Please take a look at Exhibit 56. Have you seen this document before?

MR. PATTON: We need to go off the record.

MS. HANLEY COOK: Okay.

(Off the record at 9:53 p.m.)

(Resume at 9:59 p.m.)

BY MS. HANLEY COOK:

Q The question was have you seen this document before?

MR. PATTON: Objection as beyond the scope of 30(b)(6). The witness can answer in her personal capacity if she's seen the document before.

THE WITNESS: I've certainly seen portions of it. I'm not sure I saw it in its entirety when I was working at DHS. I don't know that I saw it all in its entirety.

BY MS. HANLEY COOK:

Q What is it?

MR. PATTON: Same objection.

THE WITNESS: Memorandum Opinion for the Counsel to the President on legal issues relating to the testing, use, and deployment of an intrusion detection system (Einstein 2.0) to protect unclassified computer networks in the Executive Branch, dated January 9, 2009.

BY MS. HANLEY COOK:

Q Thank you. Please turn to page 4 of Exhibit 56, the second paragraph that begins "EINSTEIN 2.0."

A Mm-hmm.

Q I'd like you to read the first two sentences to yourself, and tell me when you're done.

A (Witness reviewing document.) Yeah.

Q Exhibit 56 says that Einstein 2.0 sensors will scan a temporary copy of traffic, right?

MR. PATTON: Same objections.

THE WITNESS: That's what the sentence says, yes.

BY MS. HANLEY COOK:

Q Is that sentence containing "temporary copy" accurate to the best of your knowledge?

MR. PATTON: Same objection, lack of foundation as well.

THE WITNESS: To the extent that I at some point reviewed a Privacy Impact Assessment associated with Einstein 1 or Einstein 2, it was many years ago, so I can't speak to whether the specificity -- I didn't review this document in advance of any of this conversation, so I would want to go back and look at all those materials before I gave you an answer one way or the other.

I have no reason to say it's not, but I have no reason to know whether that was exactly how it was implemented, or whether it remains true

today.

BY MS. HANLEY COOK:

Q But this document at least says that it will create a temporary copy, right?

MR. PATTON: Objection, the document speaks for itself.

THE WITNESS: Yes, that's what the sentence says.

BY MS. HANLEY COOK:

Q The next sentence that I had you read says that, "Einstein 2.0 operations will not disrupt the normal operations of federal systems."

Did I read that right?

A Yes, you did.

Q Do you know why Einstein 2 involves the creation of a temporary copy of the traffic being scanned?

MR. PATTON: Objection, beyond the scope of 30(b)(6), calls for -- it also -- it also indicates I'm getting tired -- beyond the scope and lacks foundation.

THE WITNESS: Well, you can read the

words that are on the page.

BY MS. HANLEY COOK:

Q Do the words on this page indicate to you why Einstein 2 involves the creation of a temporary copy of the traffic being scanned?

MR. PATTON: Same objections.

THE WITNESS: Well, it says it's for the purpose of scanning by the sensors. I guess that's not the why.

BY MS. HANLEY COOK:

Q Doesn't Einstein 2 create a temporary copy of the traffic being scanned so that it will not disrupt the normal operations of federal systems?

MR. PATTON: Same objections, including lack of foundation.

THE WITNESS: I'm not -- again, in my personal capacity, having done work on this in previous positions, without having reviewed all those documents, I'm not willing to expound one way or the other on the particular information provided here beyond what you see on the piece of

paper.

BY MS. HANLEY COOK:

Q In June 2015, did upstream surveillance involve the scanning of a temporary copy of the transactions scanned?

MR. PATTON: Objection, calls for classified information, information subject to the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MS. HANLEY COOK:

Q Going back several hours now --

A Awesome.

Q -- you testified I think, but correct me if I'm wrong, that as of June 2015, the NSA scanned at least some portions of the application layer of Internet transactions as part of upstream collection, right?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PADGETT: Can you read the

question?

(The reporter read back the question.)

THE WITNESS: Can we go off the record?

MS. HANLEY COOK: Yeah, thank you.

(Off the record at 10:06 p.m.)

(Resume at 10:11 p.m.)

THE WITNESS: Can you repeat your sentence one more time to make sure I was accurately -- or can you repeat what you --

MS. HANLEY COOK: Dawn, do you mind reading it? Thanks.

(The reporter read back the question.)

THE WITNESS: Yes, that's correct.

BY MS. HANLEY COOK:

Q You also testified that deep packet inspection refers to the scanning of the application layer of Internet packets, right?

A In the general -- oh.

MR. PATTON: Object to the extent it may mischaracterize the testimony, and beyond the scope, but the witness can answer.

THE WITNESS: In the general sense, as is traditionally understood for what deep packet inspection means, not specific to upstream.

BY MS. HANLEY COOK:

Q But it's accurate then to say that upstream surveillance, as of June 2015, involved deep packet inspection, right?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Objection as to vague, beyond the scope of 30(b)(6), and to the extent there's any classified information, instruct the witness not to answer.

If there's an unclassified answer that she can provide, she can provide that now.

THE WITNESS: I have no further information. I will take the instructions and not provide classified information.

BY MS. HANLEY COOK:

Q Today, how many targets does NSA have for upstream surveillance?

MR. PATTON: Objection, calls for

classified information, and information protected by the statutory privileges, instruct not to answer.

THE WITNESS: Could you ask the question again, please?

BY MS. HANLEY COOK:

Q Sure. Today how many targets does NSA have for upstream surveillance?

MR. PATTON: Same objection. If the witness is aware of any unclassified answer, we should probably talk about that.

THE WITNESS: Okay, why don't we go talk about that.

MR. PATTON: Off the record.

(Off the record at 10:14 p.m.)

(Resume at 10:14 p.m.)

MR. PATTON: Read the question back, please.

(The reporter read back the question.)

MR. PATTON: Same objections, same instructions.

THE WITNESS: I will follow the

instructions.

BY MS. HANLEY COOK:

Q In June 2015, how many targets did NSA have for upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: I'll follow the instructions.

BY MS. HANLEY COOK:

Q Without revealing the -- you good?

MR. PATTON: Yeah.

BY MS. HANLEY COOK:

Q Without revealing the contents of any conversations that you had with your attorneys outside this room today, and with the exception of conversations related to determining whether classified information was responsive to a question, where the line was properly drawn on classified information, state secret classifications, during breaks in the deposition today, did you discuss with anyone the substance of your testimony during the deposition?

MR. PATTON: Subject to those caveats you said, plus the statutory privileges, the witness can answer.

THE WITNESS: No.

MS. HANLEY COOK: I have no further questions.

MR. TOOMEY: Can we take a break?

MS. HANLEY COOK: Strike that I said that. Take a break for five minutes to be sure, just go back through the outline.

(Off the record at 10:16 p.m.)

(Resume at 10:26 p.m.)

FURTHER EXAMINATION

BY MR. TOOMEY:

Q When a communication is encrypted using HTTPS, does some of the communication's metadata remain unencrypted?

MR. PATTON: One second.

(Counsel conferring.)

MR. PATTON: Object to the question as beyond the scope of 30(b)(6), calling for an expert opinion. The witness can answer in her

personal capacity to the extent that she is aware of the answer.

THE WITNESS: In the general sense, it will depend on the type of encryption that's being used, and it will depend on the nature of how it's being transmitted, so there's not one answer that fits all.

BY MR. TOOMEY:

Q So when a communication is encrypted using HTTPS, does some of the communication's metadata remain unencrypted?

MR. PATTON: Object to the term "communication" as vague, and same prior objections and instruction to the witness.

THE WITNESS: To the extent that the question is somewhat vague, I'll say generally speaking, yes, but I think there are different ways you could do things that might change that answer.

BY MR. TOOMEY:

Q When a communication is encrypted using HTTPS, are the senders and recipients'

IP addresses unencrypted?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Generally speaking, they will -- I'm sorry, say the question one more time.

(The reporter read back the question.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: Again, the question is somewhat vague, and so I would answer generally that is true, but there are undoubtedly a number of exceptions that also could make that untrue.

MR. TOOMEY: Could you please mark this document as 57.

(Deposition Exhibit 57 was marked for identification.)

BY MR. TOOMEY:

Q Could you please take a look at the document, describe what it is, and tell me if you're familiar with it.

A This is the Notice of Filing of Government's Responses to FISC Questions Regarding

the Amended 2011 Section 702 Certifications, dated November 15th, 2011.

Q Thank you.

A Yes, I am familiar with these documents.

Q Could you please turn to page 9?

A Sure.

Q I'm going to read from about the third paragraph down in the middle of the personal knowledge, which says, "Metadata that has been extracted from Internet transactions consistent with Section 3(b)(5)(b)(4) is subject to the two-year retention limit set forth in Section 3(c) of the amended NSA minimization procedures."

Was that statement accurate at the time this document was filed with the FISC on November 15th, 2011?

A Yes.

Q So the NSA extracts metadata from communications collected in the course of upstream surveillance, correct?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Objection, vague as to time period, but the witness can answer.

THE WITNESS: Could you ask the question again?

(The reporter read back the question.)

MR. PATTON: Objection, vague as to time.

THE WITNESS: So I would just offer that the answer to your question is metadata has been extracted from the Internet transactions. I believe that the question said communications, in which case that would be consistent with the information that was provided here.

BY MR. TOOMEY:

Q So I'll rephrase.

The NSA extracts metadata from Internet transactions collected in the course of upstream surveillance, correct?

MR. PATTON: Objection, vague as to time.

THE WITNESS: Consistent with 2011,

what's written here at 2011, yes, that is true.

BY MR. TOOMEY:

Q Today, the NSA retains metadata associated with its targets' communications in the course of upstream surveillance, correct?

MR. PATTON: Hold on.

(Counsel conferring.)

MR. PATTON: Sorry, could you read the question back, please?

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for classified information or otherwise privileged pursuant to the aforementioned statutes.

If there is an unclassified answer, the witness can provide it.

THE WITNESS: Could you read the question one more time?

(The reporter read back the question.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: NSA retains -- I would

again go back to, instead of saying "communications," I would say "Internet transaction." I would say generally, yes, this is true.

BY MR. TOOMEY:

Q Sorry, I didn't hear you. Could you say that again?

A Sure. NSA retains metadata -- may retain metadata associated with Internet transactions in the course of upstream.

Q The NSA has an interest in the metadata of its targets' communications or Internet transactions, correct?

MR. PATTON: Objection as vague, beyond the scope of 30(b)(6).

The witness can answer.

THE WITNESS: NSA is interested in the metadata associated with the Internet transactions of a targeted selector -- to or from a targeted selector.

BY MR. TOOMEY:

Q So just to be clear, just to make sure

I understood your answer, the NSA has an interest in the metadata of communications to and from a targeted selector?

MR. PATTON: Objection, beyond the scope. The witness can answer.

THE WITNESS: Could you repeat the question?

(The reporter read back the question.)

THE WITNESS: I would not use the word "communications." I would use the word "Internet transactions."

BY MR. TOOMEY:

Q So just to be clear, the NSA has an interest in the metadata of Internet transactions to and from a targeted selector?

MR. PATTON: Objection, beyond the scope, asked and answered.

THE WITNESS: Yes.

MR. TOOMEY: Thank you. All right, we do not have any further questions right now.

MR. PATTON: Before we get off the record, the government is going to invoke Federal

Rule of Civil Procedure 30(e) to reserve the right to review and signature of the witness.

(Whereupon, at 10:36 p.m., the taking of the deposition was concluded. Reading and signature were reserved.)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,	:	
Plaintiff,	:	Case No.
vs.	:	
NATIONAL SECURITY AGENCY, et al.,	:	1:15-cv-00662-TSE
Defendants.	:	

ACKNOWLEDGMENT OF DEPONENT

I, REBECCA J. RICHARDS, do hereby acknowledge that I have read and examined pages ~~11~~ 9 through ~~239~~ 359 of the transcript of my deposition taken on Monday, April 16, 2018, and that:

(Check appropriate box):

( ) the same is a true, correct and complete transcription of the answers given by me to the questions therein recorded.

(X) except for the changes noted in the attached errata sheet, the same is a true, correct and complete transcription of the answers given by me to the questions therein recorded.

5/15/18
DATE

SIGNATURE

Wikimedia Foundation v. NSA, et al., 15-cv-00662-TSE (D. Md.)

ERRATA SHEET of REBECCA J. RICHARDS

Page	Line	To	From	Justification
9	8	Kathleen	Cathleen	Spelling Error
45	4	Michael S. Rogers	Michael F. Rogers	Spelling Error
161	19	telecom	teleco	Spelling Error
169	19	USA FREEDOM Act	USA Freedom Act	Capitalization
192	6	Protocol	protocol	Capitalization
196	13	(with our targeting procedures)	in parens	Transcription Error
263	17	scanned	scan	Clarification

CERTIFICATE OF NOTARY PUBLIC

I, DAWN A. JAQUES, a Notary Public in and for the District of Columbia, before whom the foregoing deposition was taken, do hereby certify that witness whose testimony appears in the foregoing pages was duly sworn by me; that the testimony of said witness was taken by me in shorthand at the time and place mentioned in the caption hereof and thereafter reduced to typewriting under my supervision; that said deposition is a true record of the testimony given by said witness; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this deposition is taken; and, further, that I am not a relative or employee of any attorney or counsel employed by the parties thereto, nor financially or otherwise interested in the outcome of the actions.

Dawn A. Jaques

Dawn A. Jaques, CSR, CLR
Notary Public in and for
District of Columbia

My commission expires:
January 14, 2020

*** ERRATA SHEET ***
TRANSPERFECT DEPOSITION SERVICES
216 E. 45th Street, Suite #903
NEW YORK, NEW YORK 10017
(212) 400-8845

CASE: WIKIMEDIA FOUNDATION v. NATIONAL SECURITY AGENCY, et al.
DATE: APRIL 16, 2018
WITNESS: REBECCA J. RICHARDS REF: 21368

PAGE	LINE	FROM	TO

_____
REBECCA J. RICHARDS

Subscribed and sworn to before me

this ____ day of _____, 20__.

_____
Notary Public

B

D

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix L

NSA Director of Civil Liberties and Privacy Office Report

NSA's Implementation of Foreign Intelligence Surveillance Act Section 702

April 16, 2014

National Security Agency, Civil Liberties and Privacy Office
Report
NSA's Implementation of Foreign Intelligence Surveillance Act Section 702

April 16, 2014

INTRODUCTION

This report was prepared by the National Security Agency (NSA) Civil Liberties and Privacy Office as part of its responsibilities to enhance communications and transparency with the public and stakeholders. Its Director is the primary advisor to the Director of NSA when it comes to matters of civil liberties and privacy. Created in January 2014, the Office is also charged with ensuring that civil liberties and privacy protection are integrated into NSA activities. The intent of this paper is to help build a common understanding that can serve as a foundation for future discussions about the existing civil liberties and privacy protections.

The mission of NSA is to make the nation safer by providing policy makers and military commanders with timely foreign intelligence and by protecting national security information networks. NSA collects foreign intelligence based on requirements from the President, his national security team, and their staffs through the National Intelligence Priorities Framework. NSA fulfills these national foreign intelligence requirements through the collection, processing, and analysis of communications or other data, passed or accessible by radio, wire or other electronic means.

NSA's authority to conduct signals intelligence collection for foreign intelligence and counterintelligence purposes is provided primarily by Section 1.7(c)(1) of Executive Order 12333, as amended. The execution of NSA's signals intelligence mission must be conducted in conformity with the Fourth Amendment. This includes NSA's acquisition of communications to which a U.S. person is a party under circumstances in which the U.S. person has a reasonable expectation of privacy. The Foreign Intelligence Surveillance Act of 1978 (FISA) further regulates certain types of foreign intelligence collection, including that which occurs with compelled assistance from U.S. communications providers.

This Report describes one way in which NSA meets these responsibilities while using Section 702 of FISA, as amended by the FISA Amendments Act of 2008. Although multiple federal agencies participate in Section 702 collection, this paper describes the process by which NSA obtains, uses, shares, and retains communications of foreign intelligence value pursuant to Section 702. It also describes existing privacy and civil liberties protections built into the process.

The NSA Civil Liberties and Privacy Office (CLPO) used the Fair Information Practice Principles (FIPP)[1] as an initial tool to describe the existing civil liberties and privacy protections in place for collection done under Section 702 authority.[2]

SECTION 702 OF FISA

Section 702 of FISA was widely and publicly debated in Congress both during the initial passage in 2008 and the subsequent re-authorization in 2012. It provides a statutory basis for NSA, with the compelled assistance of electronic communication service providers, to target non-U.S. persons reasonably believed to be located outside the U.S. in order to acquire foreign intelligence information. Given that Section 702 only allows for the targeting of non-U.S. persons outside the U.S., it differs from most other sections of FISA. It does not require an individual determination by the U.S. Foreign Intelligence Surveillance Court (FISC) that there is probable cause to believe the target is a foreign power or an agent of a foreign power. Instead, the FISC reviews annual topical certifications executed by the Attorney General (AG) and the Director of National Intelligence (DNI) to determine if these certifications meet the statutory requirements. The FISC also determines whether the statutorily required targeting and minimization procedures used in connection with the certifications are consistent with the statute and the Fourth Amendment. The targeting procedures are designed to ensure that Section 702 is only used to target non-U.S. persons reasonably believed to be located outside the U.S.

The minimization procedures are designed to minimize the impact on the privacy on U.S. persons by minimizing the acquisition, retention, and dissemination of non-publicly available U.S. person information that was lawfully, but incidentally acquired under Section 702 by the targeting of non-U.S. persons reasonably believed to be located outside the U.S. Under these certifications the AG and the DNI issue directives to electronic communication service providers (service providers) that require these service providers to "immediately provide the Government with all information … or assistance necessary to accomplish the acquisition [of foreign intelligence information] in a manner that will protect the secrecy of the acquisition…." The Government's acquisition of communications under its Section 702 authority thus takes place pursuant to judicial review and with the knowledge of the service providers.

NSA cannot intentionally use Section 702 authority to target any U.S. citizen, any other U.S. person, or anyone known at the time of acquisition to be located within the U.S. The statute also prohibits the use of Section 702 to intentionally acquire any communication as to which the

[1] The FIPPS are the recognized principles for assessing privacy impacts. They have been incorporated into EO13636, *Improving Critical Infrastructure Cybersecurity* and the National Strategy for Trusted Identities in Cyberspace. These principles are rooted in the U.S. Department of Health, Education and Welfare's seminal 1973 report, "Records, Computers and the Rights of Citizens." The FIPPs have been implemented in the Privacy Act of 1974, with certain exemptions, including ones that apply to certain national security and law enforcement activities.

[2] NSA CLPO will continue to refine its assessment tools to best suit the mission of NSA, as a member of the Intelligence Community, and to protect civil liberties and privacy.

sender and all intended recipients are known at the time of acquisition to be located inside the U.S. Similarly, the statute prohibits the use of Section 702 to conduct "reverse targeting" (i.e., NSA may not intentionally target a person reasonably believed to be located outside of the U.S. if the purpose of such acquisition is to target a person reasonably believed to be located inside the U.S.). All acquisitions conducted pursuant to Section 702 must be conducted in a manner consistent with the Fourth Amendment. NSA's FISC-approved targeting procedures permit NSA to target a non-U.S. person reasonably believed to be located outside the U.S. if the intended target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning one of the certifications executed by the AG and DNI. Although the purpose of Section 702 is to authorize targeting of non-U.S. persons outside the U.S., the statute's requirement for minimization procedures recognizes that such targeted individuals or entities may communicate about U.S. persons or with U.S. persons. For this reason, NSA also must follow FISC-approved minimization procedures that govern the handling of any such communications.

NSA must report to the Office of the Director of National Intelligence (ODNI) and the Department of Justice (DOJ) any and all instances where it has failed to comply with the targeting and/or minimization procedures. In addition, ODNI and DOJ have access to documentation concerning each of NSA's Section 702 targeting decisions and conduct regular reviews in order to provide independent oversight of NSA's use of the authority. The FISC Rules of Procedure require the Government to notify the Court of all incidents of non-compliance with applicable law or with an authorization granted by the Court. The Government reports Section 702 compliance incidents to the Court via individual notices and quarterly reports. In addition, the Government reports all Section 702 compliance incidents to Congress in the Attorney General's Semiannual Report. Depending on the type or severity of compliance incident, NSA may also promptly notify the Congressional Intelligence Committees, as well as the President's Intelligence Oversight Board of an individual compliance matter.

Existing Privacy and Civil Liberties Protections: Each of the three branches of federal government oversees NSA's use of the Section 702 authorities. NSA provides transparency to its oversight bodies (Congress, DOJ, ODNI, DoD, the President's Intelligence Oversight Board and the FISC) through regular briefings, court filings, and incident reporting. In addition, DOJ and ODNI conduct periodic reviews of NSA's use of the authority and report on those reviews. More recently, at the direction of the President, the Government has provided additional transparency to the public regarding the program by declassifying FISC opinions and related documents. Although FISA surveillance is normally kept secret from the targets of the surveillance, there are exceptions. For example, if the Government intends to use the results of FISA surveillance, to include Section 702 surveillance, in a trial or other proceeding against a person whose communications were collected, the Government must notify the person so the person can challenge whether the communications were acquired lawfully. These protections implement the general Fair Information Practice Principle (FIPP) of transparency.

HOW NSA IMPLEMENTS SECTION 702 of FISA

TRAINING

Before an analyst gains access to any NSA signals intelligence data, the analyst must complete specialized training on the legal and policy guidelines that govern the handling and use of the data. Additional training is required for access to Section 702 data. These annual mandatory training requirements include scenario-based training, required reading, and a final competency test. The analyst must pass this test before being granted access. Furthermore, if a compliance incident involves a mistake or misunderstanding of relevant policies, the analyst is re-trained in order to continue to have access to the data acquired pursuant to Section 702.

IDENTIFYING AND TASKING A SELECTOR

Next in the Section 702 process is for an NSA analyst to identify a non-U.S. person located outside the U.S. who has and/or is likely to communicate foreign intelligence information as designated in a certification. For example, such a person might be an individual who belongs to a foreign terrorist organization or facilitates the activities of that organization's members. Non-U.S. persons are not targeted unless NSA has reason to believe that they have and/or are likely to communicate foreign intelligence information as designated in a certification; U.S. persons are never targeted.

Once the NSA analyst has identified a person of foreign intelligence interest who is an appropriate target under one of the FISC-approved Section 702 certifications, that person is considered the target. The NSA analyst attempts to determine how, when, with whom, and where the target communicates. Then the analyst identifies specific communications modes used by the target and obtains a unique identifier associated with the target – for example, a telephone number or an email address. This unique identifier is referred to as a selector. The selector is not a "keyword" or particular term (e.g., "nuclear" or "bomb"), but must be a specific communications identifier (e.g., e-mail address).

Next the NSA analyst must verify that there is a connection between the target and the selector and that the target is reasonably believed to be (a) a non-U.S. person and (b) located outside the U.S. This is not a 51% to 49% "foreignness" test. Rather the NSA analyst will check multiple sources and make a decision based on the totality of the information available. If the analyst discovers any information indicating the targeted person may be located in the U.S. or that the target may be a U.S. person, such information must be considered. In other words, if there is conflicting information about the location of the person or the status of the person as a non-U.S. person, that conflict must be resolved before targeting can occur.

For each selector, the NSA analyst must document the following information: (1) the foreign intelligence information expected to be acquired, as authorized by a certification, (2) the information that would lead a reasonable person to conclude the selector is associated with a

non-U.S. person, and (3) the information that would similarly lead a reasonable person to conclude that this non-U.S. person is located outside the U.S. This documentation must be reviewed and approved or denied by two senior NSA analysts who have satisfied additional training requirements. The senior NSA analysts may ask for more documentation or clarification, but regardless must verify that all requirements have been met in full. NSA tracks the submission, review, and approval process through the documentation and the senior NSA analysts' determinations are retained for further review by NSA's compliance elements, as well as external oversight reviewers from DOJ and ODNI. Upon approval, the selector may be used as the basis for compelling a service provider to forward communications associated with the given selector. This is generally referred to as "tasking" the selector.

Existing Privacy and Civil Liberties Protections: NSA trains its analysts extensively through a variety of means to ensure that analysts fully understand their responsibilities and the specific scope of this authority. If the analyst fails to meet the training standards, the analyst will not have the ability to use the Section 702 authority for collection purposes. If the analyst fails to maintain ongoing training standards, the analyst will lose the ability to use the Section 702 authority for collection purposes and all ability to retrieve any data previously collected under the authority. NSA requires any authorized and trained analyst seeking to task a selector using Section 702 to document the three requirements for use of the authority – that the target is connected sufficiently to the selector for an approved foreign intelligence purpose, that the target is a non-U.S. person, and that the target is reasonably believed to be located outside the U.S. This documentation must be reviewed, validated, and approved by the senior analysts who have received additional training. These protections implement the general FIPPs of purpose specification, accountability and auditing, and minimization.

ACCESSING AND ASSESSING COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

Once senior analysts have approved a selector as compliant, the service providers are legally compelled to assist the government by providing the relevant communications. Therefore, tasking under this authority takes place with the knowledge of the service providers. NSA receives information concerning a tasked selector through two different methods.

In the first, the Government provides selectors to service providers through the FBI. The service providers are compelled to provide NSA with communications to or from these selectors. This has been generally referred to as the PRISM program.

In the second, service providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about tasked selectors. This type of compelled service provider assistance has generally been referred to as Upstream collection. NSA's FISC-approved targeting procedures include additional requirements for such collection designed to prevent acquisitions of wholly domestic communications. For example, in certain circumstances NSA's procedures require that it employ an Internet Protocol filter to ensure that the target is

located overseas. The process for approving the selectors for tasking is the same for both PRISM and Upstream collection.

Once NSA has received communications of the tasked selector, NSA must follow additional FISC-approved procedures known as the minimization procedures. These procedures require NSA analysts to review at least a sample of communications acquired from all selectors tasked under Section 702, which occurs on a regular basis to verify that the reasonable belief determination used for tasking remains valid.

The NSA analyst must review a sample of communications received from the selectors to ensure that they are in fact associated with the foreign intelligence target and that the targeted individual or entity is not a U.S. person and is not currently located in the U.S. If the NSA analyst discovers that NSA is receiving communications that are not in fact associated with the intended target or that the user of a tasked selector is determined to be a U.S. person or is located in the U.S., the selector must be promptly "detasked." As a general rule, in the event that the target is a U.S. person or in the U.S., all other selectors associated with the target also must be detasked.

Existing Privacy and Civil Liberties Protections: In addition to extensive training, the analyst is required to review the collection to determine that it is associated with the targeted selector and is providing the expected foreign intelligence shortly after the tasking starts and at least annually thereafter. This review allows NSA to identify possible problems with the collection and provides an additional layer of accountability. In addition, NSA has technical measures that alert the NSA analysts if it appears a selector is being used from the U.S. These protections implement the general FIPPs of purpose specification, minimization, accountability and auditing, data quality, and security.

NSA PROCESSING AND ANALYSIS OF COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

Communications provided to NSA under Section 702 are processed and retained in multiple NSA systems and data repositories. One data repository, for example, might hold the contents of communications such as the texts of emails and recordings of conversations, while another, may only include metadata, i.e., basic information about the communication, such as the time and duration of a telephone call, or sending and receiving email addresses.

NSA analysts may access communications obtained under Section 702 authority for the purpose of identifying and reporting foreign intelligence. They access the information via "queries," which may be date-bound, and may include alphanumeric strings such as telephone numbers, email addresses, or terms that can be used individually or in combination with one another. FISC-approved minimization procedures govern any queries done on Section 702-derived information. NSA analysts with access to Section 702-derived information are trained in the proper construction of a query so that the query is reasonably likely to return valid foreign

intelligence and minimizes the likelihood of returning non-pertinent U.S. person information. Access by NSA analysts to each repository is controlled, monitored, and audited. There are, for example, automated checks to determine if an analyst has completed all required training prior to returning information responsive to a query. Further, periodic spot checks on queries by NSA analysts are conducted.

Since October 2011 and consistent with other agencies' Section 702 minimization procedures, NSA's Section 702 minimization procedures have permitted NSA personnel to use U.S. person identifiers to query Section 702 collection when such a query is reasonably likely to return foreign intelligence information. NSA distinguishes between queries of communications content and communications metadata. NSA analysts must provide justification and receive additional approval before a content query using a U.S. person identifier can occur. To date, NSA analysts have queried Section 702 content with U.S. person identifiers less frequently than Section 702 metadata. For example, NSA may seek to query a U.S. person identifier when there is an imminent threat to life, such as a hostage situation. NSA is required to maintain records of U.S. person queries and the records are available for review by both DOJ and ODNI as part of the external oversight process for this authority. Additionally, NSA's procedures prohibit NSA from querying Upstream data with U.S. person identifiers.

Existing Privacy and Civil Liberties Protections: In addition to the training and access controls, NSA maintains audit trails for all queries of the Section 702 data. NSA's Signals Intelligence Directorate's compliance staff routinely reviews a portion of all queries that include U.S. person identifiers to ensure that all such queries are only conducted when appropriate. Personnel from DOJ and ODNI provide an additional layer of oversight to ensure that NSA is querying the data appropriately. These protections implement the general FIPPs of security, accountability and auditing, and data quality.

NSA DISSEMINATION OF INTELLIGENCE DERIVED FROM COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

NSA only generates signals intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information. Dissemination of information about U.S. persons in any NSA foreign intelligence report is expressly prohibited unless that information is necessary to understand foreign intelligence information or assess its importance, contains evidence of a crime, or indicates a threat of death or serious bodily injury. Even if one or more of these conditions apply, NSA may include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. For example, NSA typically "masks" the true identities of U.S. persons through use of such phrases as "a U.S. person" and the suppression of details that could lead to him or her being successfully identified by the context. Recipients of NSA reporting can request that NSA provide the true identity of a masked U.S. person referenced in an intelligence report if the recipient has a legitimate need to know the identity. Under NSA policy, NSA is allowed to unmask the identity only under certain

conditions and where specific additional controls are in place to preclude its further dissemination, and additional approval has been provided by one of seven designated positions at NSA. Additionally, together DOJ and ODNI review the vast majority of disseminations of information about U.S. persons obtained pursuant to Section 702 as part of their oversight process.

Existing Privacy and Civil Liberties Protections: As noted above, NSA only generates signals intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information or not. Additionally, NSA's Section 702 minimization procedures require any U.S. person information to be minimized prior to dissemination, thereby reducing the impact on privacy for U.S. persons. The information may only be unmasked in specific instances consistent with the minimization procedures and NSA policy. These protections implement the general FIPPs of minimization and purpose specification.

RETENTION OF UNEVALUATED COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

The maximum time that specific communications' content or metadata may be retained by NSA is established in the FISC-approved minimization procedures. The unevaluated content and metadata for PRISM or telephony data collected under Section 702 is retained for no more than five years. Upstream data collected from Internet activity is retained for no more than two years. NSA complies with these retention limits through an automated process.

NSA's procedures also specify several instances in which NSA must destroy U.S. person collection promptly upon recognition. In general, these include any instance where NSA analysts recognize that such collection is clearly not relevant to the authorized purpose of the acquisition nor includes evidence of a crime. Additionally, absent limited exceptions, NSA must destroy any communications acquired when any user of a tasked account is found to have been located in the U.S. at the time of acquisition.

Existing Privacy and Civil Liberties Protections: NSA has policies, technical controls, and staff in place to ensure the data is retained in accordance with the FISC-approved procedures. The automated process to delete the collection at the end of the retention period applies to both U.S. person and non U.S. person the information. There is an additional manual process for the destroying information related to U.S. Persons where NSA analysts have recognized the collection is clearly not relevant to the authorized purpose of the acquisition nor includes evidence of a crime. These protections implement the general FIPPs of minimization and security.

ORGANIZATIONAL MANAGEMENT, COMPLIANCE, AND OVERSIGHT

NSA is subject to rigorous internal compliance and external oversight. Like many other regulated entities, NSA has an enterprise-wide compliance program, led by NSA's Director of Compliance, a position required by statute. NSA's compliance program is designed to provide precision in NSA's activities to ensure that they are consistently conducted in accordance with law and procedure, including in this case the Section 702 certifications and accompanying Section 702 targeting and minimization procedures and additional FISC requirements. As part of the enterprise-wide compliance structure, NSA has compliance elements throughout its various organizations. NSA also seeks to detect incidents of non-compliance at the earliest point possible. When issues of non-compliance arise regarding the way in which NSA carries out the FISC-approved collection, NSA takes corrective action and, in parallel, NSA must report incidents of non-compliance to ODNI and DOJ for further reporting to the FISC and Congress, as appropriate or required.

These organizations, along with the NSA General Counsel, the NSA Inspector General, and most recently the Director of Civil Liberties and Privacy have critical roles in ensuring all NSA operations proceed in accordance with the laws, policies, and procedures governing intelligence activities. Additionally, each individual NSA analyst has a responsibility for ensuring that his or her personal activities are similarly compliant. Specifically, this responsibility includes recognizing and reporting all situations in which he or she may have exceeded his or her authority to obtain, analyze, or report intelligence information under Section 702 authority.

Compliance: NSA reports all incidents in which, for example, it has or may have inappropriately queried the Section 702 data, or in which an analyst may have made typographical errors or dissemination errors. NSA personnel are obligated to report when they believe NSA is not, or may not be, acting consistently with law, policy, or procedure. If NSA is not acting in accordance with law, policy, or procedure, NSA will report through its internal and external intelligence oversight channels, conduct reviews to understand the root cause, and make appropriate adjustments to its procedures.

If NSA discovers that it has tasked a selector that is used by a person in the U.S. or by a U.S. person, then NSA must cease collection immediately and, in most cases must also delete the relevant collected data and cancel or revise any disseminated reporting based on this data. NSA encourages self-reporting by its personnel and seeks to remedy any errors with additional training or other measures as necessary. Following an incident, a range of remedies may occur: admonishment, written explanation of the offense, request to acknowledge a training point that the analyst might have missed during training, and/or required retesting. In addition to reporting described above, any intentional violation of law would be referred to the NSA Office of Inspector General. To date there have been no such instances, as most recently confirmed by the President's Review Group on Intelligence and Communications Technology.

External Oversight: As required by the Section 702 targeting procedures, both DOJ and ODNI conduct routine oversight reviews. Representatives from both agencies visit NSA on a bi-monthly basis. They examine all tasking datasheets that NSA provides to DOJ and ODNI to determine whether the tasking sheets meet the documentation standards required by NSA's targeting procedures and provide sufficient information for the reviewers to ascertain the basis for NSA's foreignness determinations. For those records that satisfy the standards, no additional documentation is requested. For those records that warrant further review, NSA provides additional information to DOJ and ODNI during or following the onsite review. NSA receives feedback from the DOJ and ODNI team and incorporates this information into formal and informal training to analysts. DOJ and ODNI also review the vast majority of disseminated reporting that includes U.S. person information.

Existing Privacy and Civil Liberties Protections: The compliance and oversight processes allow NSA to identify any concerns or problems early in the process so as to minimize the impact on privacy and civil liberties. These protections implement the general FIPPs of transparency to oversight organizations and accountability and auditing.

CONCLUSION

This Report, prepared by NSA's Office of Civil Liberties and Privacy, provides a comprehensive description of NSA's Section 702 activities. The report also documents current privacy and civil liberties protections.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix M

U.S. Department of Justice

National Security Division

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

Washington, D.C. 20530

May 2, 2011

The Honorable John D. Bates
United States Foreign Intelligence Surveillance Court
333 Constitution Avenue, N.W.
Washington, D.C. 20001

Re: Clarification of National Security Agency's Upstream Collection Pursuant to Section 702 of FISA ~~(S//SI//NF)~~

Dear Judge Bates:

On April 21, 2011, the National Security Agency (NSA) provided the National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) information clarifying the manner in which NSA acquires certain communications through its upstream collection platforms pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA). Although NSA, NSD, and ODNI are still reviewing this matter and assessing its import, we are providing preliminary notice at this time pursuant to Rule 13(a) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, effective November 1, 2010, in order provide the Court with this additional clarifying information. We have worked closely in these efforts with NSA officials, who have assisted in drafting and reviewing this notice to the Court. ~~(TS//SI//NF)~~

As previously described to the Court, in conducting upstream collection using electronic communication accounts/addresses/identifiers (hereinafter "selectors") pursuant to Section 702, NSA acquires Internet communications that are to or from a tasked selector, or which contain a reference to a tasked selector. The term "Internet communications," as described by the Director of NSA in affidavits supporting DNI/AG 702(g) certifications, "is intended to include electronic communications that [redacted] See, e.g., DNI/AG 702(g) Certification [redacted] Affidavit of General Keith B. Alexander, Director, NSA, filed [redacted] 2010, ¶ 6.

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

Classified by: Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: May 2, 2036

OI Tracking No. 104876

[redacted] ~~(TS//SI//NF)~~

In past representations to the Court, the Government used as an example of upstream collection the acquisition of [redacted] that contained a selector that NSA had tasked under Section 702, such that NSA acquired the [redacted] while it was being transmitted to or from a user of the non-tasked account.[1] [redacted] Based on recent discussions among NSA, NSD, and ODNI regarding one specified category of Internet communications acquired through upstream collection—"electronic communications [redacted]"—and in view of the complexity of this issue and the prior representations to the Court, the Government believes that further description of the scope of NSA's upstream collection is warranted. ~~(TS//SI//NF)~~

One type of "electronic communications [redacted][2] ~~(TS//SI//NF)~~

Depending on [redacted], the data transmitted [redacted] may also include [redacted]

[1] [redacted] ~~(TS//SI//NF)~~

[2] [redacted] ~~(TS//SI//NF)~~

[redacted] including e-mail messages that are not to, from, or about a Section 702-targeted individual. For example, [redacted] The content of [redacted] would be acquired through NSA's Section 702 upstream collection if a tasked selector appeared anywhere [redacted] ~~(TS//SI//NF)~~

As this example demonstrates, an individual Internet communication can contain a single piece of information [redacted], or it could contain multiple pieces of information [redacted] ~~(TS//SI//NF)~~

Additionally, as described in the NSA's targeting procedures, "in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will employ either an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or [redacted]" See, e.g., DNI/AG 702(g) Certification [redacted] Exhibit A at 2. It is through these measures that NSA prevents the intentional acquisition of Internet communications that contain a reference to a targeted selector where the sender and all intended recipients are known at the time of acquisition to be located in the United States. See, e.g., In re DNI/AG Certification [redacted] No. 702(i)-08-01, Mem. Op. at 19 (USFISC Sept. 4, 2008). NSA, NSD, and ODNI are continuing to examine what affect, if any, the type of Internet communications collection discussed in this letter has on the efficacy of these measures. ~~(TS//SI//NF)~~

NSA, NSD, and ODNI are continuing to review and assess this matter and will provide additional information to the Court as appropriate. We appreciate the Court's consideration of this matter and welcome additional opportunities to present further information to the Court. ~~(TS//SI//NF)~~

Respectfully submitted,

[redacted]

Office of Intelligence, NSD
U.S. Department of Justice

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix N

~~SECRET//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

2011 AUG 16 PM 2:16

WASHINGTON, D.C.

LEEANN FLYNN HALL

[redacted]

NOTICE OF FILING OF GOVERNMENT'S SUPPLEMENT TO ITS SUBMISSIONS OF JUNE 1st AND JUNE 28TH, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits the attached supplement in further support of the

~~SECRET//ORCON,NOFORN~~

Classified by: Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: 16 August 2036

arguments set forth in submissions of June 1st and June 28th, 2011, concerning the above-referenced matters. This supplement explains the methodology behind and sets forth the results of a manual review by the National Security Agency (NSA) of a statistically representative sample of the nature and scope of the Internet communications acquired through NSA's FISA Amendments Act Section 702 upstream collection during a six-month period. The Government respectfully submits that the data provided herein supplements and supports the Government's Responses to the Court's Briefing Order of May 9th, 2011, and supplemental questions of June 17, 2011, and will further assist the Court in concluding that the certifications and procedures submitted in the above-referenced matters satisfy the requirements of the Act and are consistent with the Fourth Amendment to the Constitution of the United States. ~~(S//OC,NF)~~

Given the complex nature of the information provided in this supplement, the United States is prepared to provide any additional information the Court believes would aid it in reviewing these matters. The Government may also seek to supplement and/or clarify the information provided herein as appropriate during any hearing that the Court may hold in the above-captioned matters. ~~(S//OC,NF)~~

Respectfully submitted,

[redacted]

National Security Division
United States Department of Justice

(U//FOUO) NSA Characterization of Upstream Data: Process and Results

I. (U) Introduction

~~(TS//SI//NF)~~ This report explains the methodology behind and provides the results of a manual review of a statistically representative sample of Internet communications acquired through NSA's FISA Amendments Act (hereinafter "FAA") section 702 upstream collection during a six-month period.[1] The purpose of this review was to assemble data to assist the Court in understanding the nature and scope of the communications acquired through NSA's upstream collection. The data assembled consisted of:

- The volume of transactions containing single, discrete communications to, from, or about a selector used by a person targeted in accordance with NSA's section 702 targeting procedures (hereinafter "tasked selector") versus transactions containing multiple communications (hereinafter "Multi-communication Transactions" or "MCT") not all of which may be to, from, or about a tasked selector;[2]
- The types of discrete communications contained within MCTs [redacted]; and

[1] ~~(TS//SI//NF)~~ Additionally, as described on pages 8-9 of the Government's June 1, 2011 Response to the Court's Briefing Order of May 9, 2011, NSA conducted two tests of FAA 702 upstream collection in May 2011 using information from NSA's technical databases in an attempt to determine the likelihood of collecting an Internet transaction between a user in the United States and [redacted] NSA also attempted to further determine the extent to which those tests might be statistically representative of NSA's 702 upstream collection and repeated these tests in July 2011 using alternative data sets. Because of the technical limitations for automatically identifying transactions containing multiple communications, NSA assesses that the results of these tests are not comparable to each other or with the results of the separate manual analysis discussed herein. Furthermore, for the same reason of technical limitation, the results do not express as high a degree of granularity and accuracy as the manual analysis discussed herein, which took more than one month of careful review by experienced analysts to complete. None of the results discussed herein and in the Government's June 1 Response, however, are inconsistent.

[2] ~~(TS//SI//NF)~~ As described on pages 27-28 of the Government's June 1, 2011 Response to the Court's Briefing Order of May 9, 2011, NSA's inability to separate out individual pieces of information from Internet communications acquired by NSA's upstream collection systems does not extend to all forms of transactions. NSA has developed the capability to [redacted] identify transactions which [redacted] and, in certain other limited instances, transactions where an "active user" (as described more fully below) is a tasked selector. Based on a test of this capability from July 16th-29th 2011, NSA estimates that approximately only [redacted] of NSA's current upstream collection under FAA section 702 could be identified through [redacted] processes as communications to, from or about NSA's tasked selector. As reflected by the results of this manual review, this figure is significantly under-representative of the total proportion of NSA's upstream collection assessed to be communications to, from or about a tasked selector.

- The volume of MCTs that NSA assesses contain a wholly domestic communication not to, from, or about a tasked selector.[3]

II. (U) How the Statistically Representative Sample Was Assembled

~~(TS//SI//NF)~~ NSA assembled the sample of communications acquired through its upstream collection by first identifying all Internet communications acquired under section 702 – i.e., both from NSA upstream collection and collection from Internet service providers either by or with the assistance of the Federal Bureau of Investigation (hereinafter "PRISM collection") -- during a six-month period from January 1st through June 30th, 2011, and present within [redacted] as of July 14, 2011. As of that date, 140,974,921 Internet communications were present within [redacted] Of these, 127,718,854 (or approximately 91%) were acquired from PRISM collection, and 13,256,067 (or approximately 9%) were acquired through NSA's upstream collection.[6]

~~(TS//SI//NF)~~ The approximately 13.25 million Internet communications acquired through NSA's upstream collection (hereinafter "transactions") were then "shuffled" by NSA statisticians to ensure a random sample (i.e., any sample drawn would be statistically representative of the total 13.25 million transactions). NSA statisticians estimated that a manual review of a sample of approximately 50,000 of these randomized transactions would enable characterization of all 13.25 million transactions with a statistically high level of confidence and precision.[7]

III. (U) How the Manual Review Was Conducted and the Results of the Review

~~(TS//SI//NF)~~ Under the leadership of NSA's Deputy Director, an experienced interdisciplinary team consisting of experienced intelligence analysts, attorneys from NSA's Office of General Counsel, representatives from NSA's Office of the Director of Compliance, NSA statisticians, representatives from NSA's Network Analysis Center, and representatives from NSA's Office of Oversight and Compliance was assembled to conduct the review described herein and compile this report. A team of experienced NSA

---

[3] ~~(TS//SI//NF)~~ This aspect of the review required analysts to perform intensive analysis on discrete communications which did not contain the target's selector within MCTs, to determine if the sender and all intended recipients of those discrete communications were located in the United States. Such in-depth analysis is not typically conducted by analysts in their daily foreign intelligence analysis. Instead, an analyst would tend to focus his or her attention on those discrete communications within the MCT that are to, from, or about their assigned target, and would only perform a deeper inspection of those communications to confirm they were not wholly domestic if they were in-fact pertinent to the analyst's evaluation of foreign intelligence information and therefore worth further analysis for potential use.

[4] ~~(TS//SI//NF)~~ [redacted]

[5] ~~(TS//SI//NF)~~ This figure does not include Internet communications that were acquired during this six-month period but were purged prior to July 14, 2011.

[6] ~~(TS//SI//NF)~~ *See* Figure A of Appendix A, attached hereto.

[7] ~~(TS//SI//NF)~~ Details for the basis for NSA's statistical assertions are set forth in Appendix B, attached hereto.

intelligence analysts was assigned to conduct a manual review of the transactions. Ultimately, that team of NSA intelligence analysts collectively reviewed a total of 50,440 individual transactions.

~~(TS//SI//NF)~~ In order to ensure consistency among the analysts in their review, before beginning the manual review, the team members were trained to recognize MCTs and how to characterize the discrete communications contained within them. The team members were given training materials created specifically for this effort, which included screenshots depicting typical examples of the types of transactions acquired through NSA's upstream collection. NSA's Office of General Counsel, Office of Oversight and Compliance, and Office of the Director for Compliance reviewed all training materials and provided guidance throughout the manual review.

~~(TS//SI//NF)~~ For quality assurance, some transactions (approximately 10 out of every 5,000) underwent independent reviews by more than one analyst. In addition, the team lead performed spot reviews of transactions that had already undergone review (approximately 1 out of every 100). The team lead also personally reviewed any transaction that team members were unable to immediately characterize as clearly being a discrete communication or an MCT; as well as any MCT identified as potentially concerning a person located in the United States. Both the quality assurance overlap and the reviews performed by the team lead revealed no discrepancies among how analysts characterized any of the transactions subjected to these overlapping reviews.

~~(TS//SI//NF)~~ In conducting the manual review, NSA analysts took the following steps and made the following findings:

1. **Determined if the transaction was a single, discrete communication or an MCT.**[8] If the transaction was determined to be a single, discrete communication, no further analysis was done. Transactions determined to be MCTs were further analyzed, as described below.

   - Of the 50,440 transactions reviewed, 45,359 (approximately 90%) were determined to be single, discrete communications. The remaining 5,081 transactions (approximately 10%) were determined to be MCTs.[9]

2. **Characterized the discrete communications within the 5,081 MCTs as being** [redacted]

   - Of the 5,081 MCTs reviewed, [redacted]

[8] ~~(TS//SI//NF)~~ For any objects that the initial reviewer was uncertain about how to characterize (e.g., if the transaction contained data requiring further processing to render it intelligible to the analyst), the team lead performed a second review. As a result, each of 50,440 transactions reviewed were able to be characterized as being either a single, discrete communication or an MCT.

[9] ~~(TS//SI//NF)~~ *See* Figure B of Appendix A.

[10] ~~(TS//SI//NF)~~ [redacted]

[redacted][12]

3. **Determined whether the 5,081 MCTs contained any discrete communications as to which the sender and all intended recipients were located in the United States.** As discussed in more detail below, in many cases NSA analysts were able to make these determinations based on the location of the "active user" of the MCT.[13] In other cases, NSA had to rely on content analysis because the MCT did not contain technical information sufficient to identify the active user or to determine the active user's location. There were, however, instances where the MCT did not contain sufficient technical information or content for NSA to assess whether the MCT contained any wholly domestic communications.

   - Of the 5,081 MCTs, 713 (approximately 14%) had a tasked selector as the active user [redacted]. No further analysis of these MCTs was done to determine whether they contained wholly domestic communications. That is because the user of the tasked selector, who by operation of the NSA targeting procedures is a person reasonably believed to be located outside the United States, would be either the sender or an intended recipient of each of the discrete communications contained within the MCT.[14] Accordingly, all of the discrete communications within those MCTs would have at least one communicant reasonably believed to be located outside the United States (i.e., the target) and thus would not be wholly domestic.
   - Of the 5,081 MCTs, 2,668 (approximately 52%) had an active user that was not a tasked selector but was nonetheless an electronic communications account/address/identifier

[11] ~~(TS//SI//NF)~~ *See* Figure C of Appendix A.

[12] ~~(TS//SI//NF)~~ [redacted]

[13] ~~(TS//SI//NF)~~ When NSA acquires an Internet transaction between an individual using an electronic communications account/address/identifier and his/her service provider, that individual is the "active user" for that transaction. Such transactions can have, at most, one "active user."

[14] ~~(TS//SI//NF)~~ In this context, a communication to or from the target includes communications to or from the tasked selector itself (e.g., an e-mail sent to a tasked e-mail account), as well as communications where the tasked selector appears in other communications attributable to the target [redacted] *See In re DNI/AG Certificatio* [redacted] Docket No. 702(i)-08-01, Mem. Op. at 17 n.14 (USFISC Sept. 4, 2008).

reasonably believed to be used by a person located outside the United States.[15] No further analysis of these MCTs was done to determine whether they contained wholly domestic communications. That is because the foreign-based active user would be either a sender or intended recipient of each of the discrete communications within the transaction. Accordingly, all of the discrete communications within those MCTs would have at least one communicant reasonably believed to be located outside the United States (i.e., the foreign-based active user) and thus would not be wholly domestic.

- Of the 5,081 MCTs, 8 (approximately 0.16%) contained an electronic communication account/address/identifier of a non-targeted active user who appeared to be located in the United States, but none of the discrete communications within the MCT were determined to be wholly domestic because at least one of the communicants to each discrete communication was reasonably believed to be located outside the United States. Specifically, the 8 MCTs were determined to concern six non-targeted active users (i.e., two of the MCTs were duplicates):
  - Four MCTs (including both duplicates) [redacted] contained at least one e-mail message from a tasked selector as well as other e-mail messages from accounts/addresses/identifiers reasonably believed to be used by a person located outside the United States.[16] [redacted].
  - Three MCTs [redacted] with the users of accounts/addresses/identifiers who were reasonably believed to be located outside the United States.[17]
  - One MCT [redacted] where further technical analysis revealed that the active user was reasonably believed to be located outside the United States.
- Of the 5,081 MCTs, 10 (approximately 0.2%) contained an electronic communication account/address/identifier of a non-targeted active user who was located in the United States, and the MCTs contained at least one discrete communication that was wholly

[15] ~~(TS//SI//NF)~~ To determine the location of the non-targeted active user, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

[16] ~~(TS//SI//NF)~~ To determine the location of the senders of each of these discrete e-mail messages, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

[17] ~~(TS//SI//NF)~~ To determine the location of [redacted] NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

domestic. Specifically, all 10 of these MCTs were [redacted] and all 10 involved U.S.-based persons using [redacted].[18] For all 10 of these MCTs, only [redacted] was present. The [redacted] did not include [redacted].

- 9 of the 10 [redacted] were attributed to a single U.S.-based user. Each of these 9 [redacted] 10 total e-mail messages. The 9 [redacted] were not completely duplicative, but many of the 10 e-mail messages [redacted] were duplicative.
  - Two of the messages [redacted] in each of the 9 [redacted] contained a tasked selector and thus were not assessed to be wholly domestic.
  - Three of the messages [redacted] in each of the 9 [redacted] were [redacted] which is located in the United States) and thus were assessed to be wholly domestic.
  - The remaining e-mail messages [redacted] were between the U.S.-based user and persons reasonably believed to be located outside the United States (and thus not assessed to be wholly domestic) or whose location was unknown.[19]
- The other [redacted] was attributed to a different U.S.-based user. This [redacted] 15 total e-mail messages:
  - One of the [redacted] e-mail messages was from a tasked selector and thus was not assessed to be wholly domestic.
  - One of the [redacted] e-mail messages appeared to be a message that the U.S.-based user sent to himself [redacted] and thus was assessed to be wholly domestic.
  - One of the [redacted] e-mail messages appeared to be a message sent by an associate [redacted] account and thus was assessed to be wholly domestic.
  - The remaining e-mail messages [redacted] were between the U.S.-based user and persons reasonably believed to be

[18] ~~(TS//SI//NF)~~ [redacted]

[19] ~~(TS//SI//NF)~~ To determine the location of the other communicants, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

located outside the United States and thus were not assessed to be wholly domestic.[20]

- Of the 5,081 MCTs, 1,682 (approximately 33%) required further, in-depth [redacted] analysis because they lacked information sufficient for NSA to readily identify the active user or determine the active user's location. In most of these cases, the transactions did not contain enough information for NSA to readily determine which electronic communication account/address/identifier appearing in the transaction was that of the active user. In other cases, NSA was able to determine which electronic communication account/address/identifier appearing in the transaction was that of the "active user," but NSA was unable to determine the active user's location. NSA's further [redacted] analysis of these 1,682 MCTs revealed:
  - For 1,220 of these 1,682 MCTs, NSA analysis of [redacted] data indicated that they were characteristic of a foreign use [redacted]
  - For 152 of these 1,682 MCTs, NSA analysis of [redacted] data indicated that they were [redacted]
  - For 86 of these 1,682 MCTs, NSA analysis of a combination of technical data and content revealed that they appeared to contain communications of persons located outside the United States (e.g., through further content analysis, NSA analysts were able to identify the active users of some MCTs and information indicative of those users' locations).
- Of the 5,081 MCTs, NSA cannot determine whether 224 MCTs contained wholly domestic communications, because these MCTs lack information sufficient for NSA to identify the active user or determine the active user's location. Nevertheless, NSA has no basis to believe any of these MCTs contain wholly domestic communications.
  - For 182 of these 224 MCTs, NSA technical analysis indicates that they were characteristic of [redacted]
  - For 1 of these 224 MCTs, NSA initially determined that it contained an electronic communication account/address/identifier of a non-targeted active user who appeared to be located in the United States, but whose location could not be determined upon further technical analysis. Specifically, [redacted]

[20] ~~(TS//SI//NF)~~ To determine the location of the other communicants, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

[redacted].

- 23 of these 224 MCTs were not further analyzed because, although they were present in [redacted] as of the date the sample was assembled, they were subsequently purged and/or placed on NSA's Master Purge List.
- 18 of these 224 MCTs could not be further characterized by NSA analysts.

IV. (U) Conclusions Drawn from the Random Sample

~~(TS//SI//NF)~~ Based on a random sample of the approximately 13.25 million total Internet communications acquired by NSA through "upstream" techniques pursuant to FAA section 702 for the six-month period discussed, NSA assesses that the volume of transactions containing multiple communications not all of which may be to, from, or about a tasked selector is approximately between 1.29 and 1.39 million (9.70%-10.45%).[21] With respect to the types of discrete communications contained within multi-communication transactions manually reviewed by NSA analysts, [redacted]

~~(TS//SI//NF)~~ As described in Appendix B, which details NSA's Statistical Methodology for this review, the data compiled during the above-discussed manual review of a random sample of Internet communications acquired during a six-month period can be used to characterize with a statistically high degree of confidence (i.e., a simultaneous confidence level of 95% for these intervals collectively) the nature and scope of the entirety of the approximately 13.25 million Internet communications from

[21] ~~(TS//SI//NF)~~ As calculated in the attached Appendix detailing NSA's Statistical Methodology for this review, these figures are based on the 45,359 of the 50,440 transactions (89.93%) manually reviewed by NSA analysts as containing single, discrete communications and the 5,081 transactions (10.07%) manually reviewed by NSA analysts as containing multiple communications. *See also* Step 1, *supra* page 3.

[22] ~~(TS//SI//NF)~~ [redacted]

[23] ~~(TS//SI//NF)~~ [redacted]

[24] ~~(TS//SI//NF)~~ [redacted]

which the random sample was drawn. Specifically, NSA assesses that of these approximately 13.25 million Internet communications acquired through NSA upstream collection:

- between approximately 11.87 and 11.97 million (89.55%-90.30%) are transactions that contain only single, discrete communications to, from, or about a tasked selector;
- between 168,853 and 206,922 (1.27%-1.56%)[25] are transactions that contain multiple communications, all of which are either to or from a tasked selector;
- between 1,042,838 and 1,113,947 (7.87%-8.53%)[26] are transactions that contain multiple communications, at least one of which is to, from, or about NSA's tasked selector, but all of which are believed to either be to or from non-targeted persons reasonably believed to be located outside the United States;
- between 48,609 and 70,168 (0.37%-0.53%)[27] are transactions that contain multiple communications, at least one of which is to, from, or about NSA's tasked selector, and at least one of which is a communication between non-targeted persons (i.e., not to, from or about a tasked selector) that lacks sufficient information for NSA to identify the location of the sender and all intended recipients of that communication; and
- between 996 and 4,965 (0.0075%-0.0375%) contain a wholly domestic communication not to, from, or about a tasked selector.

~~(TS//SI//NF)~~ In sum, while there was insufficient information present for 224 multi-communication transactions for NSA analysts to characterize the likelihood that they may contain wholly domestic communications (the majority of which were attributable to [redacted], for the reasons explained in detail

[25] ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 713 of the 5,081 MCTs (14.03%) and 50,440 total transactions (1.41%) reviewed by NSA analysts as containing a tasked selector as the active user [redacted]. See also Step 3, *supra* page 4.

[26] ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 4,134 of the 5,081 MCTs (81.36%) and 50,440 total transactions (8.19%) reviewed by NSA analysts as containing discrete communications believed to be to or from non-targeted persons located outside the United States. More specifically, this total includes the following MCTs manually reviewed by NSA analysts: 2,668 that had an active user reasonably believed to be a person located outside the United States; 8 that included at least one communicant reasonably believed to be located outside the United States for each communication therein; 1,220 that are characteristic o[redacted] 152 that are indicative of [redacted] and 86 that all communications contained therein were to or from persons located outside the United States. *See* Step 3, *supra* pages 4-6.

[27] ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 224 of the 5,081 MCTs (4.41%) and 50,440 total transactions (0.44%%) reviewed by NSA analysts that lacked sufficient information to identify the active user or the active user's location. *See* Step 3, *supra* page 6.

above, NSA has no basis to believe any of the remaining Internet communications reviewed in the 50,440 sample are wholly domestic beyond those 10 discussed above.[28] Moreover, each of those 10 Internet communications has been placed on NSA's Master Purge List.

----- *The remainder of this page intentionally left blank.* -----

[28] ~~(TS//SI//NF)~~ *See* Figure D of Appendix A.

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

(U) VERIFICATION

(U) I declare under penalty of perjury that the facts set forth in the foregoing "NSA Characterization of Upstream Data: Process and Results" are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 16th day of August, 2011.

[redacted]

Signals Intelligence Directorate Compliance Architect
National Security Agency

Appendix A

Fig. A Total FAA 702

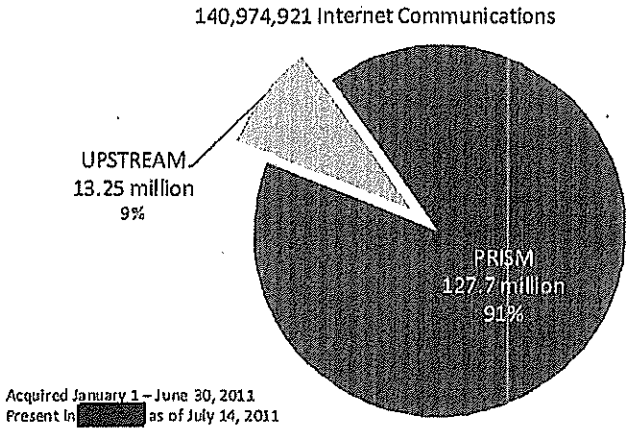


Fig. B Total Upstream Sample

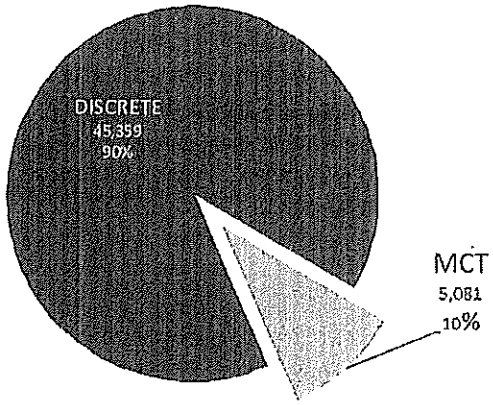


Fig. C MCT Type

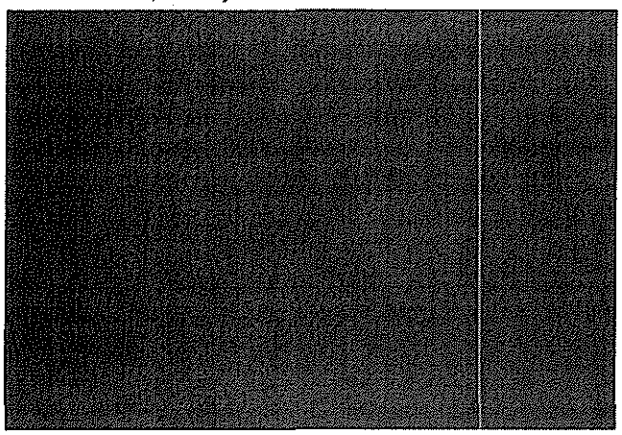
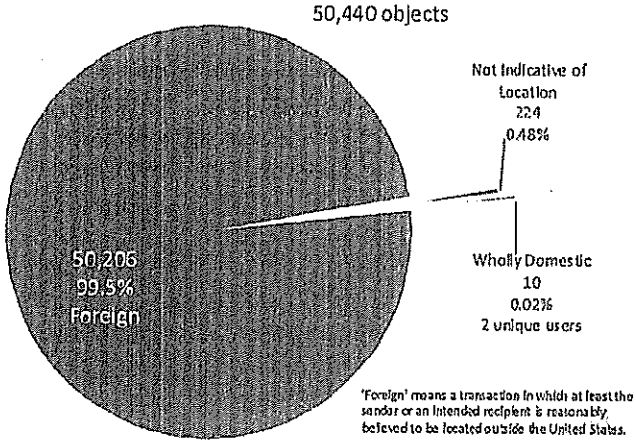


Fig. D Summary



Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360801

Appendix B: Statistical Methodology – FAA Section 702 Upstream Manual Review

~~(TS//SI//NF)~~ Using statistical analysis NSA determined the proportions of transactions satisfying certain criteria (e.g., proportion of FAA Section 702 upstream Internet transactions that are Multi-communication Transactions (MCT) versus transactions containing single, discrete communications). As further described below, transactions were categorized in various ways. The categorization process can be complex; to minimize categorization error, NSA used a statistical approach involving actual examination of an appropriate sample of transactions by experienced intelligence analysts. (The use of only a sample is a concession to the large volume of transactions and the labor-intensive nature of the categorization process.) That is, NSA traded "categorization error" for "statistical error"; the latter refers to the fact that by considering only a randomly sampled portion of the universe of transactions, NSA estimated the true proportions (as they exist in the universe) -- with error bounds and levels of confidence that can be stated justifiably.

~~(TS//SI//NF)~~ **THE SAMPLE.** As discussed more fully in the "NSA Characterization of Upstream Data: Process and Results," NSA identified 13,256,067 transactions acquired through NSA's FAA 702 upstream collection during a six-month period from January 1st through June 30th, 2011. Of those approximately 13.25 million transactions, a team of experienced intelligence analysts carefully examined 50,440 over a nearly one-month time period. The transactions were presented to the analysts in a randomized order, ensuring that a simple random sample would serve as the basis for conclusions -- supported by statistical theory – about the true proportions of the 13.25 million-transaction universe.

~~(TS//SI//NF)~~ **ESTIMATES AND CONFIDENCE INTERVALS.** The proportions formed from the sampled transactions serve as unbiased estimates of the corresponding proportions of the 13,256,067-transaction universe. Further, for (six) selected proportions, NSA states a confidence interval for each. Collectively, these intervals have a simultaneous confidence level of 95%. This means that the intervals were produced by a procedure calibrated to produce, for at least 95% of the sample sets NSA could have drawn, intervals which all cover the corresponding true (i.e., universal) proportions. Individually, each interval has a higher level of confidence associated with it; component confidence levels are quoted below.

~~(TS//SI//NF)~~ For each of the six categories, NSA also states a confidence interval for the actual number of that category's transactions within the 13,256,067-transaction (January-June, 2011 upstream) universe. Such an interval is simply an equivalent representation of the corresponding proportion-interval (it is obtained by multiplying the endpoints of the proportion-interval by 13,256,067), and so the inclusion of such intervals does not affect the (95%) level of simultaneous confidence.

~~(TS//SI//NF)~~ Specifically: By sampling a subset of the universe (or *population*) of upstream transactions, NSA estimated the following six proportions. (Hereinafter, N denotes 13,256,067 – the size of that universe; M denotes the (unknown) actual number of MCTs in that universe).

- M / N: the proportion of the population comprising MCTs;

Derived From: NSA/CSSM 1-52
Dated: ~~20070108~~
Declassify On: 20360801

- 1-(M/N): the proportion of the population comprising discrete transactions;
- the proportion of the population comprising MCTs in which all communications are either to or from NSA's tasked selector (hereinafter labeled "Target" MCTs);
- the proportion of the population comprising MCTs in which all communications are believed to either be to or from non-targeted persons located outside the United States (hereinafter labeled "Foreign" MCTs);
- the proportion of the population comprising MCTs in which the nature of one or more communications between non-targeted persons lacked sufficient information for NSA analysts to identify the location of the sender and all intended recipients (hereinafter labeled "Unknownable" MCTs);
- the proportion of the population comprising MCTs that NSA analysts assessed contain a wholly domestic not to, from, or about a tasked selector (hereinafter labeled "Confirmed Wholly Domestic").

~~(TS//SI//NF)~~ (The first of these proportions equals the total of the last four.) In the following, lower-case letters denote transaction counts as realized in the sample, in categories corresponding to their upper-case counterparts. That is, n is the number of transactions sampled (this turned out to be 50,440), and m is the number of MCTs in the sample.

~~(TS//SI//NF)~~ **OUTLINE OF PROCEDURE.** NSA designed a procedure that accepts a size-n *simple random sample*[1] of the population, and produced from it estimates and confidence intervals for the six "true"[2] proportions NSA sought. The estimates NSA produced are simply the corresponding proportions as found in the sample – e.g., the sample proportion m/n was NSA's estimate of the population proportion M/N; such a sample proportion is unbiased[3] for its population counterpart, meaning that were a sample proportion to be computed for each of the possible size-n samples that could be drawn, the average of these sample proportions would equal the "true" (population) proportion.

---

[1] ~~(TS//SI//NF)~~ A simple random sample is one that is drawn in a way that ensures that all possible size-n subsets of the (size-N) population have an equal chance of being selected; this sampling technique enables statistically justifiable claims by avoiding potential (known or unknown) sources of bias in the population (e.g., a periodic trend in the population over time).

[2] ~~(TS//SI//NF)~~ "True" refers to proportions that relate to the entire population, which cannot be determined for certain, as n is smaller than N.

[3] ~~(TS//SI//NF)~~ Unbiasedness means that the estimate is aiming for the right "target"; however, it indicates nothing about the precision of the estimate. An estimation procedure can be unbiased whether it is based on a small or large sample size n.

~~(TS//SI//NF)~~ To express precision appropriately, NSA designed its procedure to produce confidence intervals – one for each of the (six) population proportions of interest – having a simultaneous confidence level of 95%. This means that:

- Based on a sample, the procedure will produce a collection of intervals, each asserted to contain the true (population) proportion it targets.

- Because the procedure operates on a random sample, the interval endpoints are *random variables*; the particular collection of intervals a particular sample yields may fail to cover one or more of the population proportions it targets. But the procedure is designed so that this failure probability – *whatever* the true proportions are – is no more than 5%; that is, for at least 95% of the (size-n) simple random samples it might process, the procedure will produce intervals which *all* cover their targeted population proportions.

- In order to achieve this level of confidence about a collection of intervals simultaneously, the procedure is designed so that the respective failure probabilities associated with the component intervals total no more than 5%. In particular, this 5% was allocated as follows:

  - 2.5% to the proportion of "Confirmed Wholly Domestic";
  - 0.67% to each of the "Target," "Foreign," "Unknown" proportions;
  - 0.5% to the proportion of MCT (i.e., M/N). As the proportions of discrete and MCT transactions are complementary (i.e., they total 1), the confidence interval for the proportion of discrete transactions is obtained by subtracting each of the endpoints for the MCT-interval from 1 – and it is the case that one of these intervals will cover its population target if and only if the other does. Therefore, there is no need to separately allocate "failure probability" to the proportion-of-discrete.

~~(TS//SI//NF)~~ The probability of drawing a sample resulting in one or more "failing" intervals is no more than the sum of the failure probabilities of the respective component intervals, hence the claim of 95% confidence for the procedure outlined here. The "no more" qualification makes this technique conservative: relationships (complicated and left unanalyzed) between the random variables involved may make the practical confidence level higher; 95% represents a worst-case claim. To achieve simultaneous 95% confidence, the 5% failure probability could have been allocated in any way. (Broadly: the lower the confidence level (i.e., the higher the failure probability), the narrower the intervals the procedure will produce. An extreme example: a procedure for 100% confidence intervals would produce uselessly wide intervals, as it would have to be able to claim that its intervals cover truth for *every* possible size-n sample it could have received.) This procedure for simultaneous intervals is conservative in a further way: Just as the sum of the discrete and MCT proportions equals 1, so does the sum of the discrete, "Target," "Foreign," "Unknown," and "Confirmed Wholly Domestic" proportions. It is difficult to exploit this latter constraint properly; NSA utilized the conservative method described here to ensure that its assertions about the procedure's performance are valid.

~~(TS//SI//NF)~~ **CONFIDENCE-INTERVAL PROCEDURE FOR A SINGLE PROPORTION.** As outlined above, the procedure for (95%) simultaneous confidence intervals was achieved by producing component confidence intervals based on (individually higher) levels of confidence (e.g., 99.5% for M/N). The construction of component confidence intervals can be understood via the following example, using the M/N target. For the sample of size n to be observed, m represents the (random) number of MCTs to be realized in the sample. Formally, m has a *hypergeometric* distribution (arising from sampling transactions "without replacement"); to make the mathematical computations tractable, NSA approximated this distribution by a *binomial* distribution corresponding to sampling *with* replacement (in which each sampled transaction would be replaced after it is drawn, and hence would be eligible to be drawn multiple times). This approximation is uniformly conservative; i.e., it will result in wider intervals. The proportion to be estimated, M/N, appears as the (unknown) parameter (now denoted p) of this binomial distribution. Treating m as a binomial random variable based on n *trials*, NSA used an accepted method (the *Clopper-Pearson* method) as the basis to devise its confidence-interval procedure for p. (Below, the notation $B(n,q)$ refers to an n-trial binomial random variable having parameter q.) Upon observing m, NSA:

- Determines, for each of various proportions x between 0 and 0.5%, parameters q and r such that
  - x is the probability that a $B(n,q)$ random variable takes a value of at least m (but if m=0, take q to be 0);
  - (0.5% - x) is the probability that a $B(n,r)$ random variable takes a value no larger than m (but if m=n, take r to be 1).

  r exceeds q; the pair $[q,r]$ determines an interval.

- Determines the narrowest of all such intervals $[q,r]$ and reports it as the (99.5%) confidence interval for $p = M/N$.

~~(TS//SI//NF)~~ Practically, the q's and r's can be computed using *inverse Beta functions*, and computer software can find the narrowest interval efficiently.

Remainder of this page intentionally left blank.

RESULTS:

	# of transactions in sample	Sample proportion (of 702 upstream)	Confidence interval for corresponding universal proportion	Confidence interval for the actual number (of the 13.25 million)
Discrete	45,359	0.8993	0.8955 – 0.9030	11,870,284 – 11,970,275
MCT	5,081	0.1007	0.0970 – 0.1045	1,285,792 – 1,385,783

	# of transactions in sample	Sample proportion (of MCT)	Confidence interval for corresponding universal (MCT) proportion	Confidence interval for the actual number (of the 13.25 million)
TARGET	713	0.01414	0.01274 – 0.01561	168,853 – 206,922
FOREIGN	4,134	0.08196	0.07867 – 0.08532	1,042,838 – 1,130,947
UNKNOWABLE	224	0.004441	0.003667 – 0.005293	48,609 – 70,168
CONFIRMED WHOLLY DOMESTIC	10	0.0001983	0.00007508 – 0.0003746	996 – 4,965

[redacted]

Remainder of this page intentionally left blank.

VERIFICATION

I declare under penalty of perjury that the facts set forth in this Appendix are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, Section 1746, on this 11th day of August, 2011.

[Statistician]
National Security Agency

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix O

~~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

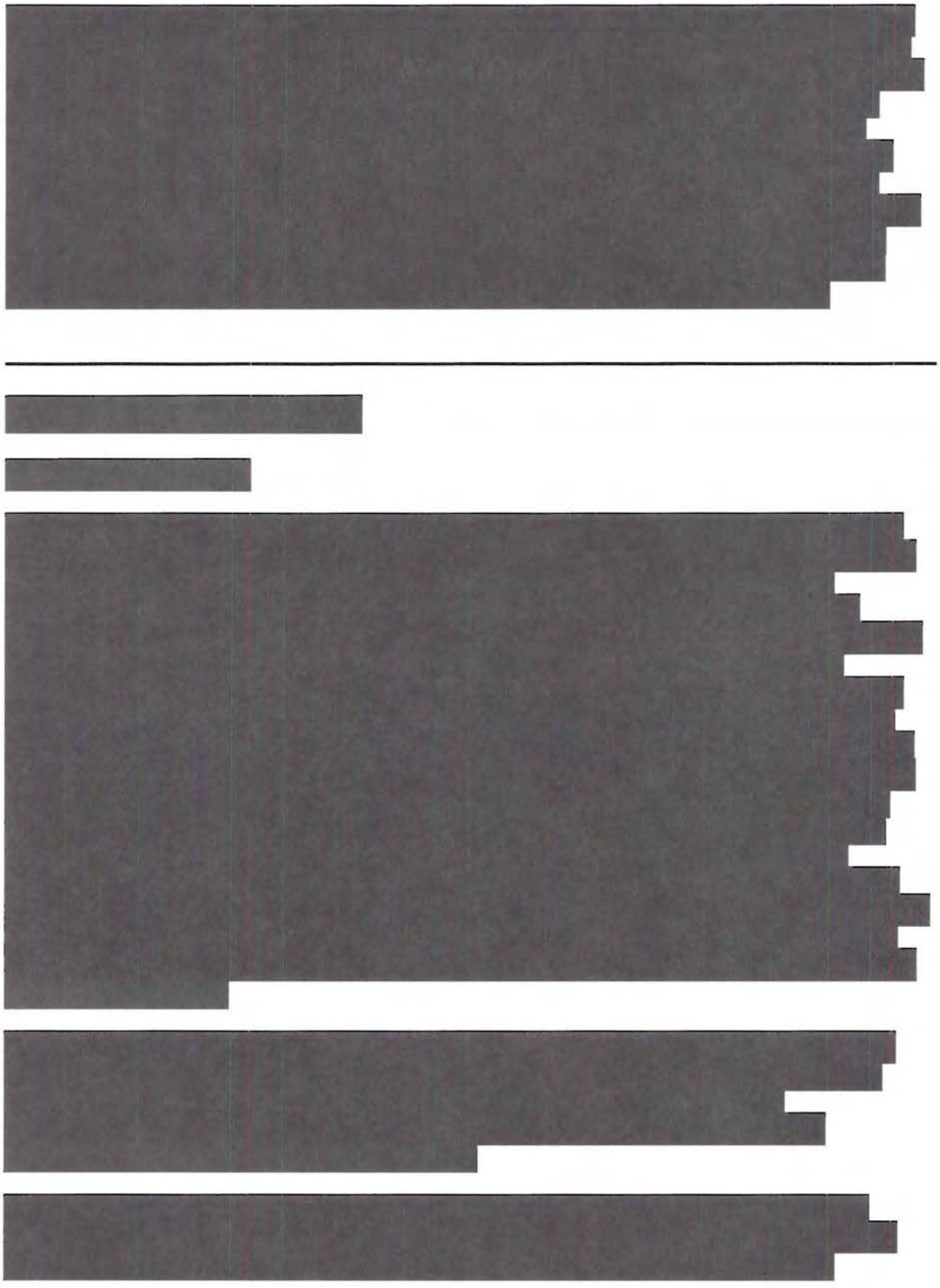
Robert S. Litt
General Counsel
Office of Director of National Intelligence

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

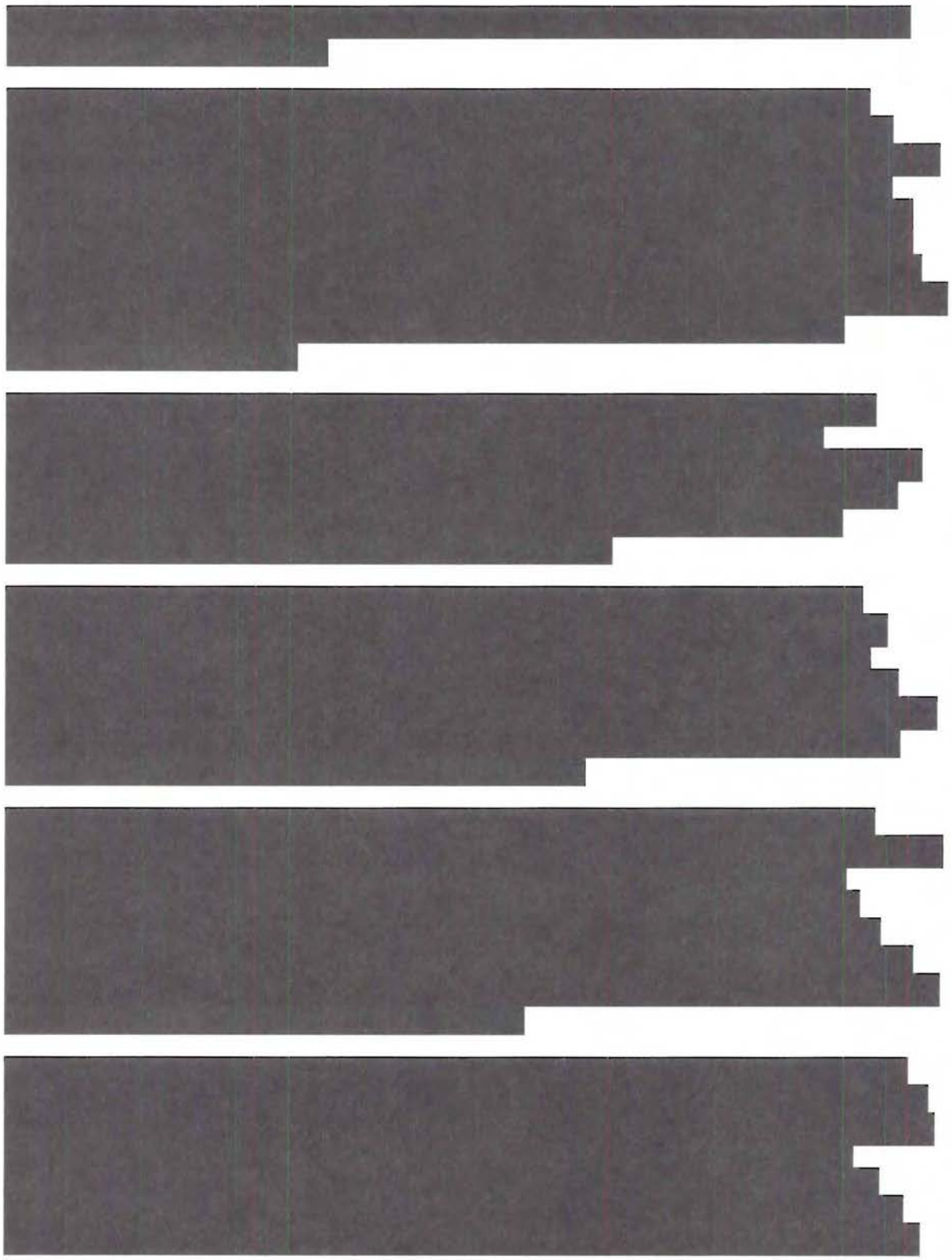
At a Hearing Concerning
"FISA Amendments Act Reauthorization"

Presented on
December 8, 2011

[redacted]

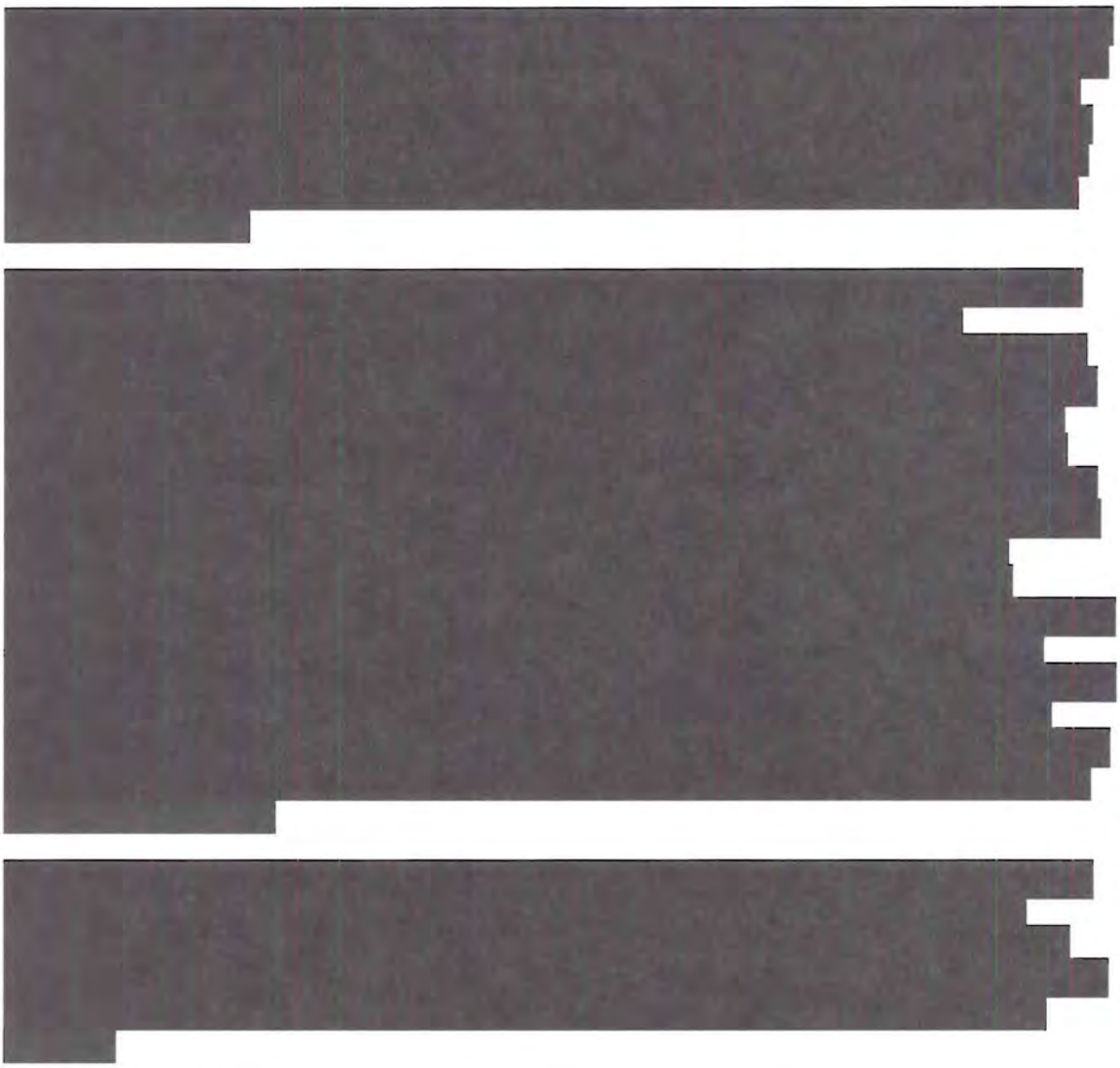


[redacted]



(b) (1) (A)

[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.,* , 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.

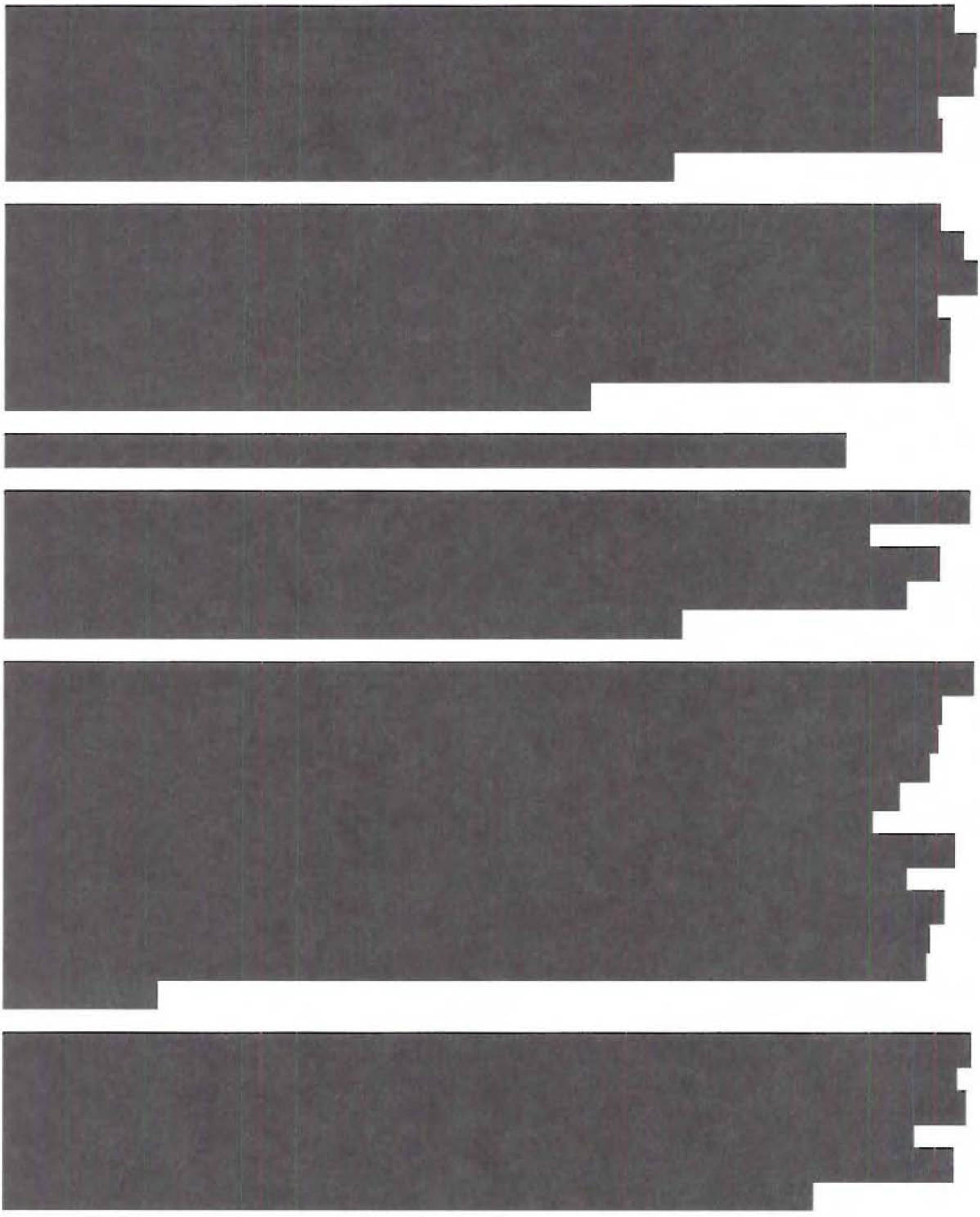
~~(TS//SI//NF)~~ As described above, upstream collection allows NSA to acquire, among other things, communications about a target where the target is not itself a communicant. In doing so, NSA uses [redacted] that are reasonably designed to screen out communications that are wholly domestic in nature, 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.

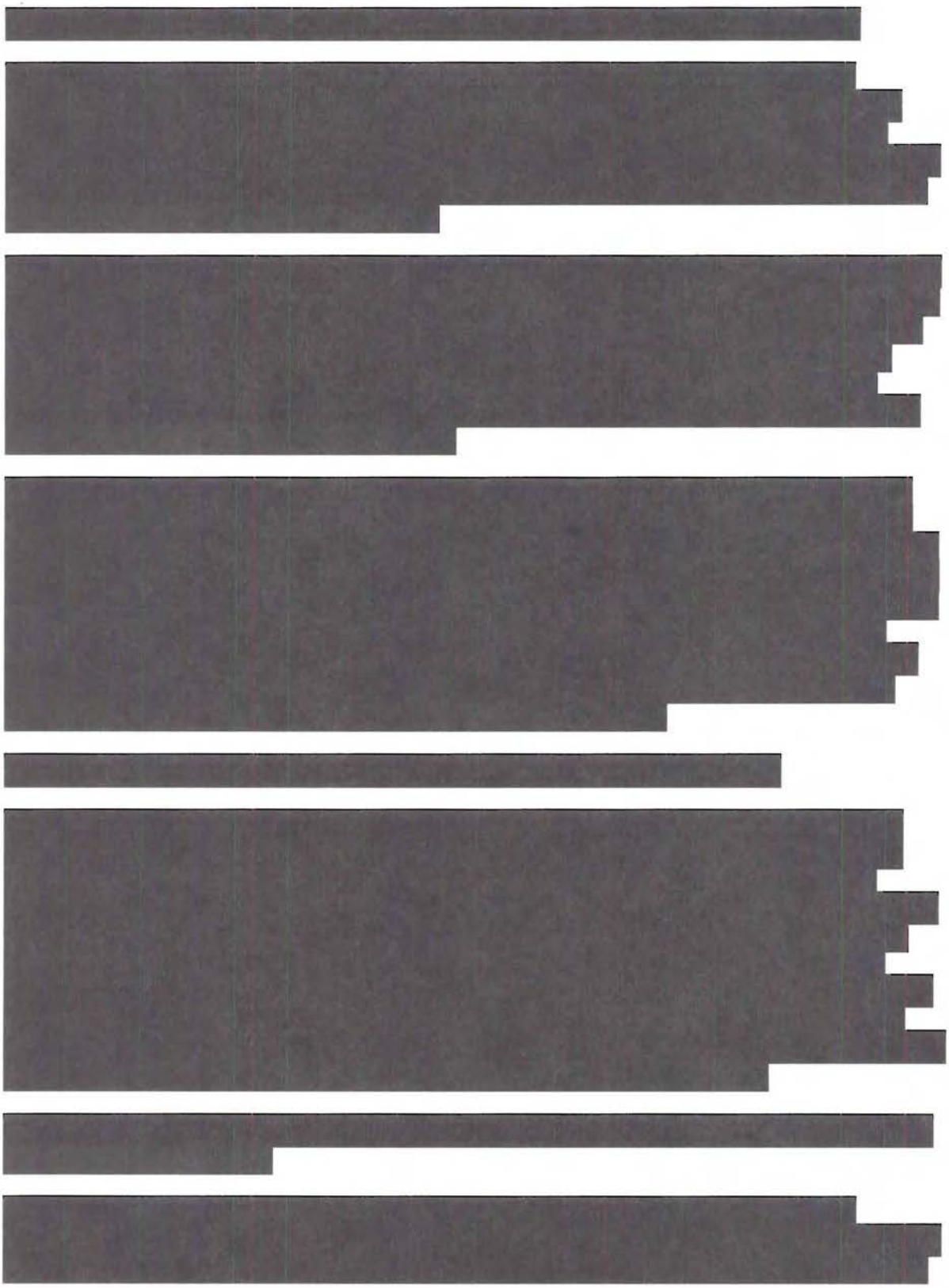
~~(TS//SI//NF)~~ The FISC upheld NSA's continued upstream acquisition of Internet communications under section 702 even though it includes the unintentional acquisition of wholly domestic communications and the incidental acquisition of MCTs that may contain one or more individual communications that 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.

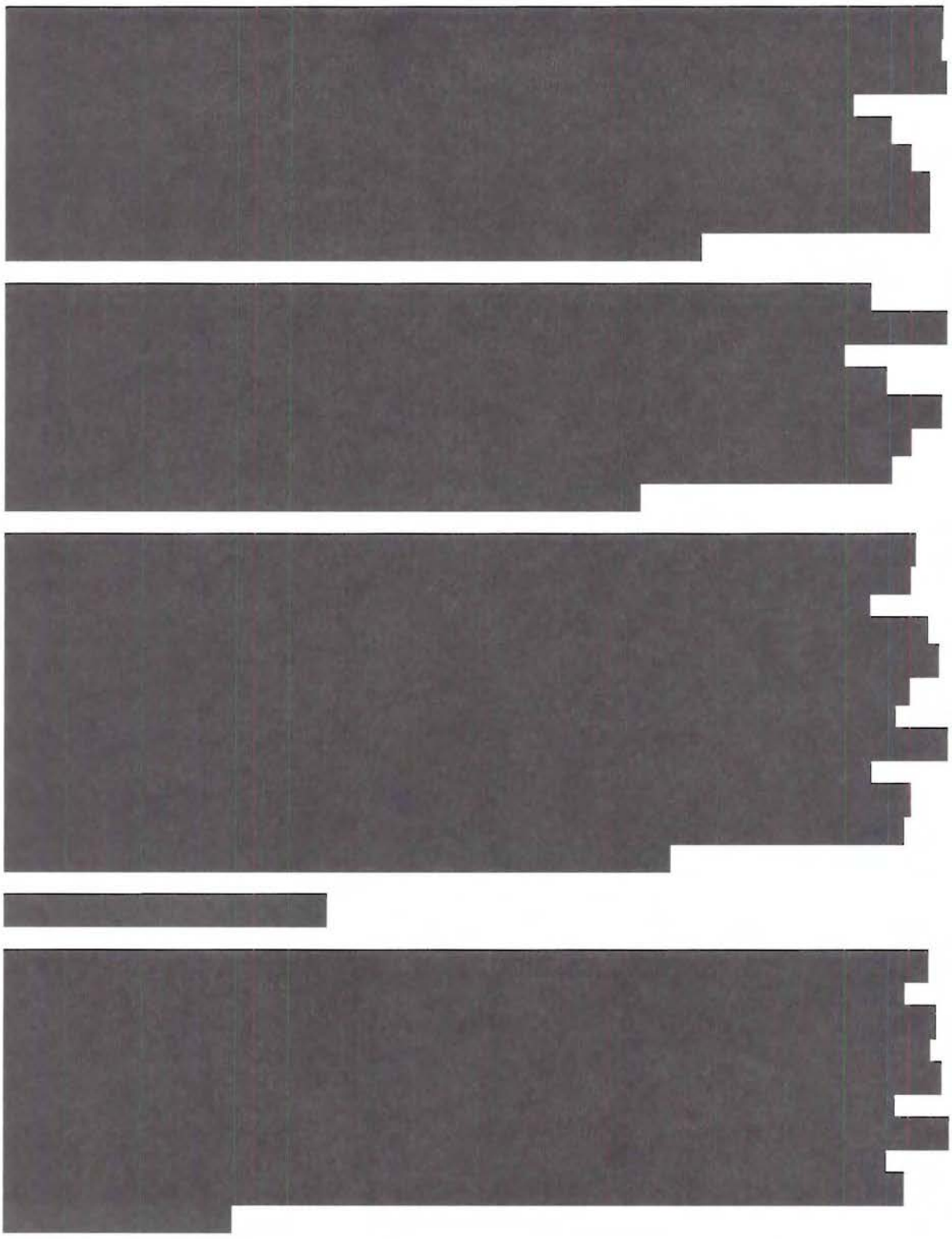
~~(TS//SI//NF)~~ The FISC determined, however, that the minimization procedures governing *retention* of MCTs were inconsistent with the requirements of section 702. The FISC found that the Government had not fully explored options regarding data retention that would be more protective of U.S. persons, 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.

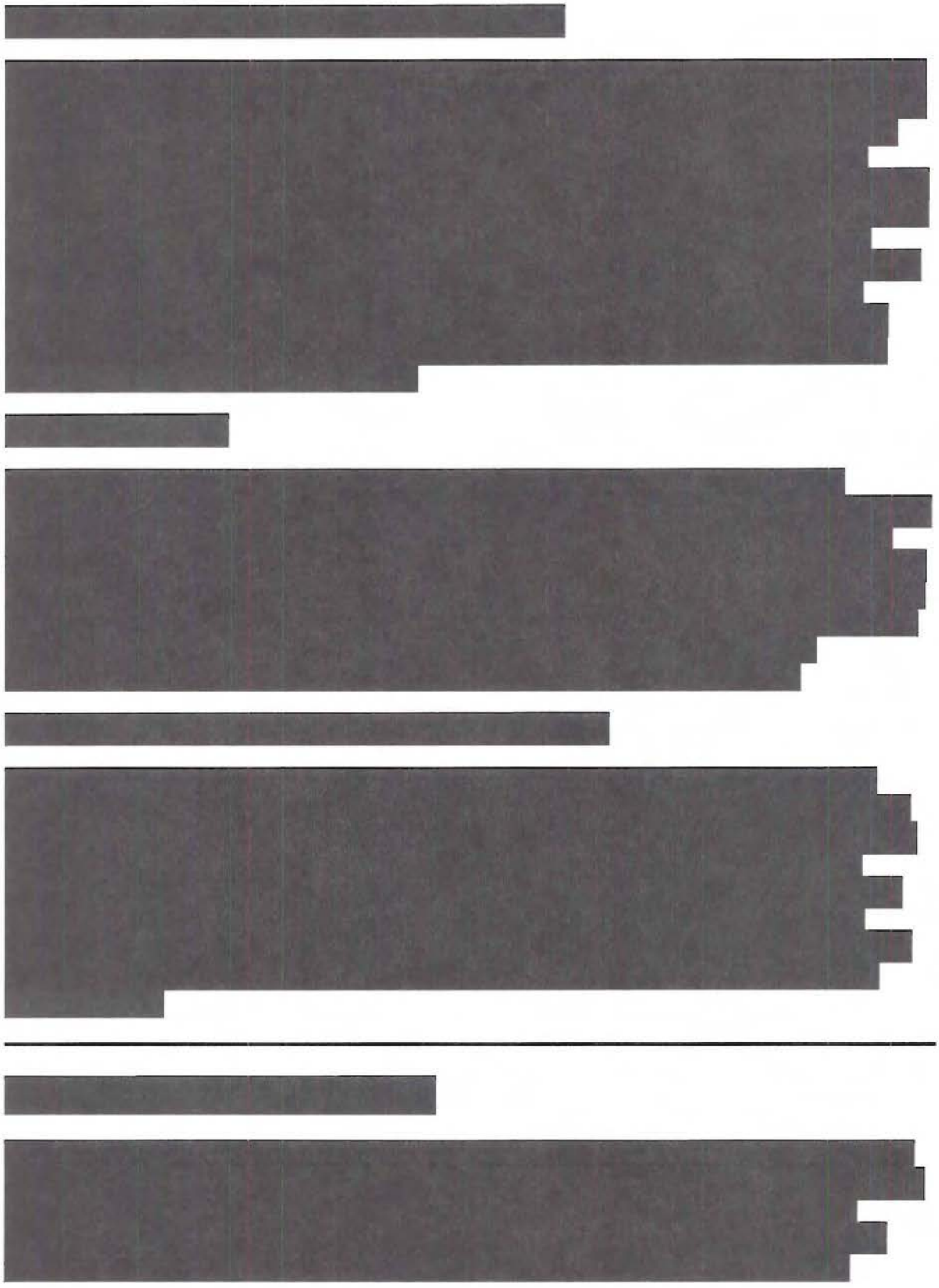
~~(TS//SI//NF)~~ On October 31, 2011, after extensive consultations among the Department, ODNI, and NSA, the Attorney General submitted amended minimization procedures to the FISC addressing the deficiencies noted by the court. These amended procedures continue to allow for the upstream collection of 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.

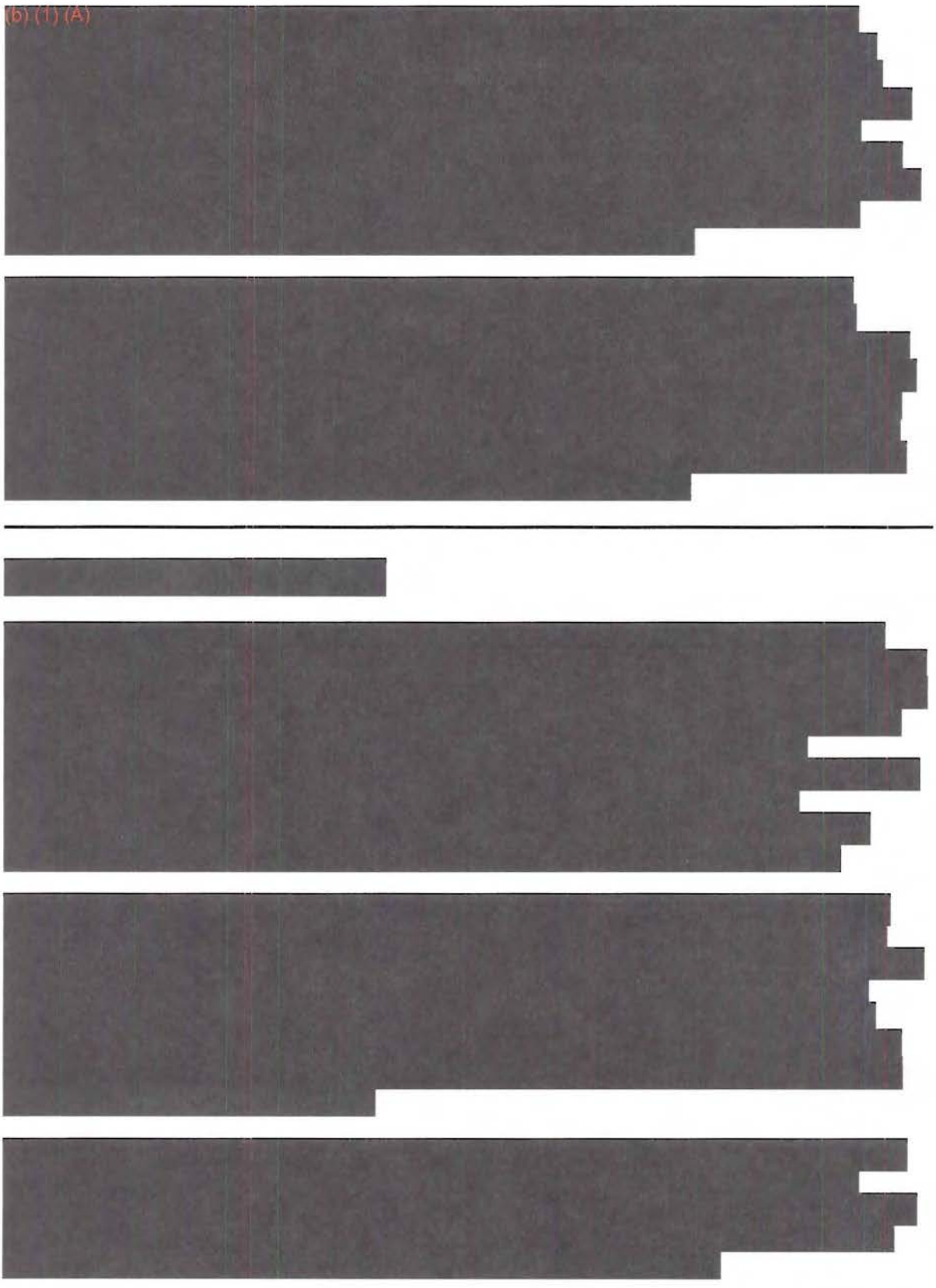


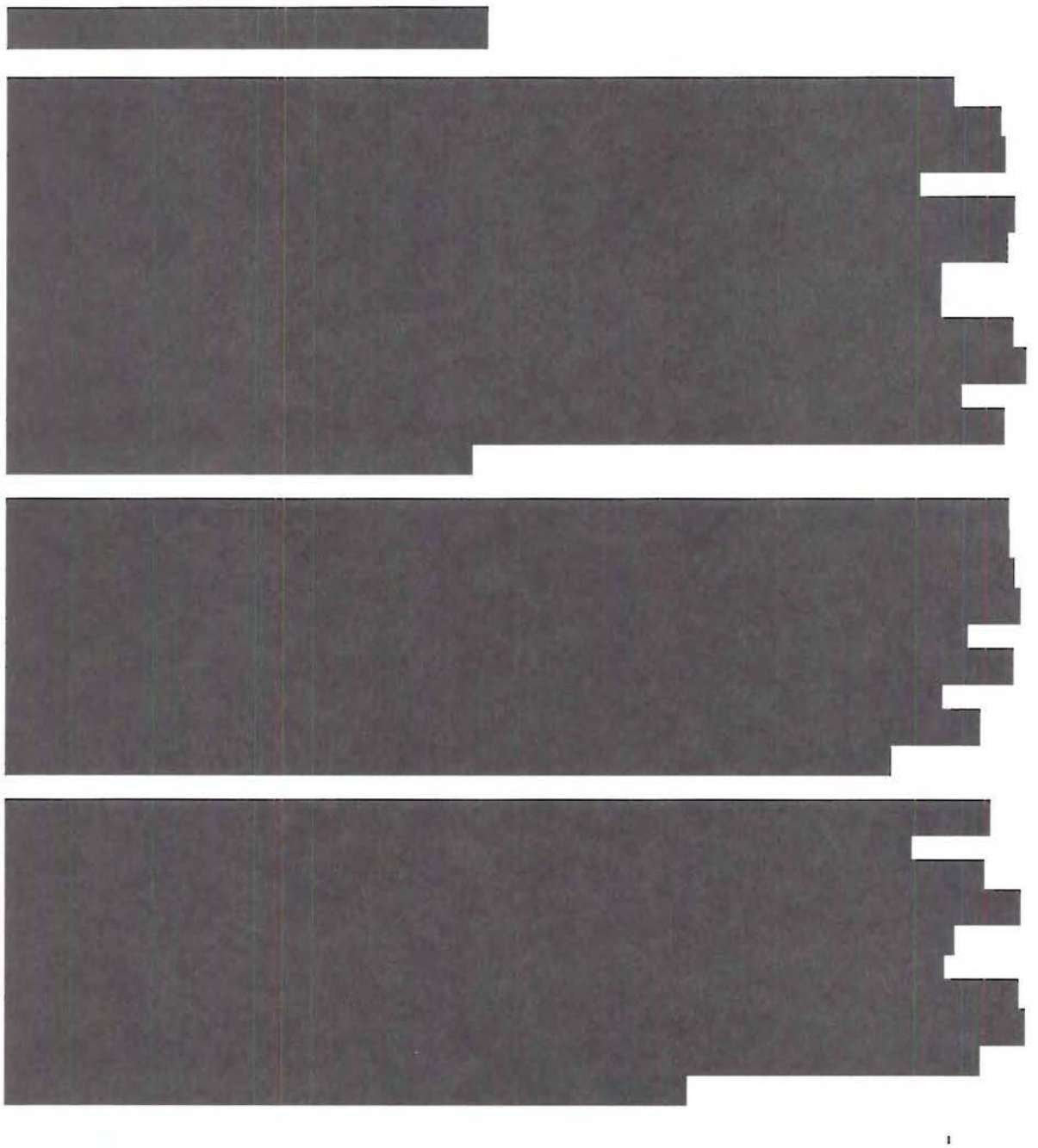






(b) (1) (A)





DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix P

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

MEMORANDUM OPINION

These matters are before the Foreign Intelligence Surveillance Court ("FISC" or "Court") on: (1) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications

[redacted], which was filed on April 20, 2011; (2) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [redacted], which was filed on April 22, 2011; and (3) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [redacted], which was also filed on April 22, 2011.[1]

Through these submissions, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA" or the "Act"), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth below, the government's requests for approval are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the "upstream collection" of Internet transactions containing multiple communications – is, in some respects, deficient on statutory and constitutional grounds.

[1] For ease of reference, the Court will refer to these three filings collectively as the "April 2011 Submissions."

I. BACKGROUND

A. The Certifications and Amendments

The April 2011 Submissions include DNI/AG 702(g) Certification [redacted], all of which were executed by the Attorney General and the Director of National Intelligence ("DNI") pursuant to Section 702. [redacted] previous certifications have been submitted by the government and approved by the Court pursuant to Section 702. [redacted] (collectively, the "Prior 702 Dockets"). Each of the April 2011 Submissions also includes supporting affidavits by the Director or Acting Director of the National Security Agency ("NSA"), the Director of the Federal Bureau of Investigation ("FBI"), and the Director of the Central Intelligence Agency ("CIA"); two sets of targeting procedures, for use by NSA and FBI respectively; and three sets of minimization procedures, for use by NSA, FBI, and CIA, respectively.[2]

Like the acquisitions approved by the Court in the eight Prior 702 Dockets, collection

[2] The targeting and minimization procedures accompanying Certification [redacted] are identical to those accompanying [redacted] As discussed below, the NSA targeting procedures and FBI minimization procedures accompanying Certifications [redacted] also are identical to the NSA targeting procedures and FBI minimization procedures that were submitted by the government and approved by the Court for use in connection with Certifications [redacted]. The FBI targeting procedures and the NSA and CIA minimization procedures that accompany the April 2011 Submissions differ in several respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications [redacted].

under Certifications [redacted] is limited to "the targeting of non-United States persons reasonably believed to be located outside the United States." Certification [redacted]

[redacted]

The April 2011 Submissions also include amendments to certifications that have been submitted by the government and approved by the Court in the Prior 702 Dockets. The amendments, which have been authorized by the Attorney General and the DNI, provide that information collected under the certifications in the Prior 702 Dockets will, effective upon the Court's approval of Certifications [redacted], be handled subject to the same

revised NSA and CIA minimization procedures that have been submitted for use in connection with Certifications [redacted].

B. The May 2 "Clarification" Letter

On May 2, 2011, the government filed with the Court a letter pursuant to FISC Rule 13(a) titled "Clarification of National Security Agency's Upstream Collection Pursuant to Section 702 of FISA" ("May 2 Letter"). The May 2 Letter disclosed to the Court for the first time that NSA's "upstream collection"[3] of Internet communications includes the acquisition of entire "transaction[s]" [redacted][4] According to the May 2 Letter, such transactions may contain data that is wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection. See id. at 2-3. The letter noted that NSA uses [redacted] to ensure that "the person from whom it seeks to obtain foreign intelligence information is located overseas," but suggested that the government might lack confidence in the effectiveness of such measures as applied to Internet transactions. See id. at 3 (citation omitted).

[3] The term "upstream collection" refers to NSA's interception of Internet communications as they transit [redacted], rather than to acquisitions directly from Internet service providers such as [redacted].

[4] The concept of "Internet transactions" is discussed more fully below. See infra, pages 27-41 and note 23.

C. The Government's First Motion for Extensions of Time

On May 5, 2011, the government filed a motion seeking to extend until July 22, 2011, the 30-day periods in which the Court must otherwise complete its review of Certifications [redacted], and the amendments to the certifications in the Prior 702 Dockets. See Motion for an Order Extending Time Limit Pursuant to 50 U.S.C. § 1881a(j)(2) at 1 ("May Motion"). The period for FISC review of Certification [redacted] was then set to expire on May 20, 2011, and the period for review of the other pending certifications and amendments was set to expire on May 22, 2011. Id. at 6.[5]

The government noted in the May Motion that its efforts to address the issues raised in the May 2 Letter were still ongoing and that it intended to "supplement the record . . . in a manner that will aid the Court in its review" of the certifications and amendments and in making the determinations required under Section 702. Id. at 7. According to the May Motion, however, the government would "not be in a position to supplement the record until after the statutory time limits for such review have expired." Id. The government further asserted that granting the requested extension of time would be consistent with national security, because, by operation of

[5] 50 U.S.C. § 1881a(i)(1)(B) requires the Court to complete its review of the certification and accompanying targeting and minimization procedures and issue an order under subsection 1881a(i)(3) not later than 30 days after the date on which the certification and procedures are submitted. Pursuant to subsection 1881a(i)(1)(C), the same time limit applies to review of an amended certification or amended procedures. However, 50 U.S.C. § 1881a(j)(2) permits the Court, by order for reasons stated, to extend "as necessary for good cause in a manner consistent with national security," the time limit for the Court to complete its review and issue an order under Section 1881a(i)(3).

statute, the government's acquisition of foreign intelligence information under Certifications [redacted] could continue pending completion of the Court's review. See id. at 9-10.

On May 9, 2011, the Court entered orders granting the government's May Motion. Based upon the representations in the motion, the Court found that there was good cause to extend the time limit for its review of the certifications to July 22, 2011, and that the extensions were consistent with national security. May 9, 2011 Orders at 4.

D. The May 9 Briefing Order

Because it appeared to the Court that the acquisitions described in the May 2 Letter exceeded the scope of collection previously disclosed by the government and approved by the Court, and might, in part, fall outside the scope of Section 702, the Court issued a Briefing Order on May 9, 2011 ("Briefing Order"), in which it directed the government to answer a number of questions in writing. Briefing Order at 3-5. On June 1, 2011, the United States filed the "Government's Response to the Court's Briefing Order of May 9, 2011" ("June 1 Submission"). After reviewing the June 1 Submission, the Court, through its staff, directed the government to answer a number of follow-up questions. On June 28, 2011, the government submitted its written responses to the Court's follow-up questions in the "Government's Response to the Court's Follow-Up Questions of June 17, 2011" ("June 28 Submission").

E. The Government's Second Motion for Extensions of Time

The Court met with senior officials of the Department of Justice on July 8, 2011, to

discuss the information provided by the government in the June 1 and June 28 Submissions. During the meeting, the Court informed the government that it still had serious concerns regarding NSA's acquisition of Internet transactions and, in particular, whether the Court could make the findings necessary to approve the acquisition of such transactions pursuant to Section 702. The Court also noted its willingness to entertain any additional filings that the government might choose to make in an effort to address those concerns.

On July 14, 2011, the government filed a motion seeking additional sixty-day extensions of the periods in which the Court must complete its review of DNI/AG 702(g) Certifications [redacted], and the amendments to the certifications in the Prior 702 Dockets. Motion for Orders Extending Time Limits Pursuant to 50 U.S.C. § 1881a(j)(2) ("July Motion").[6]

In its July Motion, the government indicated that it was in the process of compiling additional information regarding the nature and scope of NSA's upstream collection, and that it was "examining whether enhancements to NSA's systems or processes could be made to further ensure that information acquired through NSA's upstream collection is handled in accordance with the requirements of the Act." Id. at 8. Because additional time would be needed to supplement the record, however, the government represented that a 60-day extension would be necessary. Id. at 8, 11. The government argued that granting the request for an additional extension of time would be consistent with national security, because, by operation of statute, the

[6] As discussed above, by operation of the Court's order of May 9, 2011, pursuant to 50 U.S.C. § 1881a(j)(2), the Court was required to complete its review of, and issue orders under 50 U.S.C.§ 1881a(i)(3) concerning, DNI/AG 702(g) Certifications [redacted] and the amendments to the certifications in the Prior 702 Dockets, by July 22, 2011. Id. at 6.

government's acquisition of foreign intelligence information under Certifications [redacted] could continue pending completion of the Court's review. Id. at 9-10.

On July 14, 2011, the Court entered orders granting the government's motion. Based upon the representations in the motion, the Court found that there was good cause to extend the time limit for its review of the certifications to September 20, 2011, and that the extensions were consistent with national security. July 14, 2011 Orders at 4.

F. The August 16 and August 30 Submissions

On August 16, 2011, the government filed a supplement to the June 1 and June 28 Submissions ("August 16 Submission"). In the August 16 Submission, the government described the results of "a manual review by [NSA] of a statistically representative sample of the nature and scope of the Internet communications acquired through NSA's . . . Section 702 upstream collection during a six-month period." Notice of Filing of Aug. 16 Submission at 2. Following a meeting between the Court staff and representatives of the Department of Justice on August 22, 2011, the government submitted a further filing on August 30, 2011 ("August 30 Submission").

G. The Hearing and the Government's Final Written Submission

Following review of the August 30 Submission, the Court held a hearing on September 7, 2011, to ask additional questions of NSA and the Department of Justice regarding the government's statistical analysis and the implications of that analysis. The government made its

final written submissions on September 9, 2011, and September 13, 2011 ("September 9 Submission" and "September 13 Submission," respectively).

H. The Final Extension of Time

On September 14, 2011, the Court entered orders further extending the deadline for its completion of the review of the certifications and amendments filed as part of the April Submissions. The Court explained that "[g]iven the complexity of the issues presented in these matters coupled with the Court's need to fully analyze the supplemental information provided by the government in recent filings, the last of which was submitted to the Court on September 13, 2011, the Court will not be able to complete its review of, and issue orders . . . concerning [the certifications and amendments] by September 20, 2011." [redacted] The Court further explained that although it had originally intended to extend the deadline by only one week, the government had advised the Court that "for technical reasons, such a brief extension would compromise the government's ability to ensure a seamless transition from one Certification to the next." [redacted] Accordingly, the Court extended the deadline to October 10, 2011. [redacted]

II. REVIEW OF CERTIFICATIONS [redacted]

The Court must review a certification submitted pursuant to Section 702 of FISA "to determine whether [it] contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). The Court's examination of Certifications [redacted] confirms that:

(1) the certifications have been made under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see Certification [redacted];

(2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see Certification [redacted];

(3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures[7] and minimization procedures;[8]

(4) each of the certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);[9] and

(5) each of the certifications includes an effective date for the authorization in compliance

---

[7] See April 2011 Submissions, NSA Targeting Procedures and FBI Targeting Procedures (attached to Certifications [redacted]).

[8] See April 2011 Submissions, NSA Minimization Procedures, FBI Minimization Procedures, and CIA Minimization Procedures (attached to Certifications [redacted].

[9] See April 2011 Submissions, Affidavits of John C. Inglis, Acting Director, NSA (attached to Certifications [redacted]); Affidavit of Gen. Keith B. Alexander, U.S. Army, Director, NSA (attached to Certification [redacted]); Affidavits of Robert S. Mueller, III, Director, FBI (attached to Certifications [redacted]); Affidavits of Leon E. Panetta, Director, CIA [redacted]

with 50 U.S.C. § 1881a(g)(2)(D), see Certification [redacted][10]

The Court therefore finds that Certification [redacted] contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

III. REVIEW OF THE AMENDMENTS TO THE CERTIFICATIONS IN THE PRIOR DOCKETS.

Under the judicial review procedures that apply to amendments by virtue of Section 1881a(i)(1)(C), the Court must review each of the amended certifications "to determine whether the certification contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). The Court has previously determined that the certifications in each of the Prior 702 Dockets, as originally submitted to the Court and previously amended, contained all the required elements.[11] Like the prior certifications and amendments, the amendments now before the Court were executed under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), and submitted to the Court within the time allowed under 50 U.S.C. § 1881a(i)(1)(C). See

[10] The statement described in 50 U.S.C. § 1881a(g)(2)(E) is not required in this case because there has been no "exigent circumstances" determination under Section 1881a(c)(2).

[11] [redacted]

Certification [redacted][12] Pursuant to Section 1881a(g)(2)(A)(ii), the latest amendments include the attestations of the Attorney General and the DNI that the accompanying NSA and CIA minimization procedures meet the statutory definition of minimization procedures, are consistent with the requirements of the Fourth Amendment, and will be submitted to the Court for approval. Certification [redacted]. The latest amendments also include effective dates that comply with 50 U.S.C. § 1881a(g)(2)(D) and § 1881a(i)(1). Certification [redacted] All other aspects of the certifications in the Prior 702 Dockets – including the further attestations made therein in accordance with § 1881a(g)(2)(A), the NSA targeting procedures and FBI minimization procedures submitted therewith in accordance with § 1881a(g)(2)(B),[13] and the affidavits executed in support thereof in accordance with § 1881a(g)(2)(C) – are unaltered by the latest amendments.

In light of the foregoing, the Court finds that the certifications in the Prior 702 Dockets, as amended, each contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

---

[12] The amendments to the certifications in the Prior 702 Dockets were approved by the Attorney General on April 11, 2011, and by the DNI on April 13, 2011. See Certification [redacted]

[13] Of course, targeting under the certifications filed in the Prior 702 Dockets will no longer be permitted following the Court's issuance of an order on Certifications [redacted]

IV. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is required to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). See 50 U.S.C. § 1881a(i)(2)(B) and (C); see also 50 U.S.C. § 1881a(i)(1)(C) (providing that amended procedures must be reviewed under the same standard). Section 1881a(d)(1) provides that the targeting procedures must be "reasonably designed" to "ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." Section 1881a(e)(1) requires that the minimization procedures "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4) . . . ." Most notably, that definition requires "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h) & 1821(4). Finally, the Court must determine whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A).

A. The Effect of the Government's Disclosures Regarding NSA's Acquisition of Internet Transactions on the Court's Review of the Targeting and Minimization Procedures

The Court's review of the targeting and minimization procedures submitted with the April 2011 Submissions is complicated by the government's recent revelation that NSA's acquisition of Internet communications through its upstream collection under Section 702 is accomplished by acquiring Internet "transactions," which may contain a single, discrete communication, or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities. June 1 Submission at 1-2. That revelation fundamentally alters the Court's understanding of the scope of the collection conducted pursuant to Section 702 and requires careful reexamination of many of the assessments and presumptions underlying its prior approvals.

In the first Section 702 docket, [redacted], the government disclosed that its Section 702 collection would include both telephone and Internet communications. According to the government, the acquisition of telephonic communications would be limited to "to/from" communications – i.e., communications to or from a tasked facility. The government explained, however, that the Internet communications acquired would include both to/from communications and "about" communications – i.e., communications containing a reference to the name of the tasked account. See [redacted]. Based upon the government's descriptions of the proposed collection, the Court understood that the acquisition of Internet communications under Section 702 would be limited to discrete "to/from" communications between or among individual account users and to "about"

communications falling within [redacted] specific categories that had been first described to the Court in prior proceedings. [redacted] Declaration of Director of NSA at 20-22. The Court's analysis and ultimate approval of the targeting and minimization procedures in Docket No. [redacted], and in the other [redacted] Prior 702 Dockets, depended upon the government's representations regarding the scope of the collection. In conducting its review and granting those approvals, the Court did not take into account NSA's acquisition of Internet transactions, which now materially and fundamentally alters the statutory and constitutional analysis.[14]

---

[14] The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.

In March, 2009, the Court concluded that its authorization of NSA's bulk acquisition of telephone call detail records from [redacted] in the so-called "big business records" matter "ha[d] been premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." Docket No. BR 08-13, March 2, 2009 Order at 10-11. Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying. The Court concluded that this requirement had been "so frequently and systemically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively." Id.

Shortly thereafter, the government made a similar disclosure regarding NSA's bulk acquisition of metadata regarding Internet communications in the so-called "big pen register" matter. In [redacted] the government reported that, from the time of the initial Court authorization in 2004, NSA had been continually collecting various forms of data falling outside the scope of the Court's orders, and that "'[v]irtually every PR/TT record' generated by this program included some data that had not been authorized for collection." Docket No. PR/TT [redacted] Mem. Op. at 20-21. This long-running and systemic overcollection had

(continued...)

The government's submissions make clear not only that NSA has been acquiring Internet transactions since before the Court's approval of the first Section 702 certification in 2008,[15] but also that NSA seeks to continue the collection of Internet transactions. Because NSA's acquisition of Internet transactions presents difficult questions, the Court will conduct its review in two stages. Consistent with the approach it has followed in past reviews of Section 702 certifications and amendments, the Court will first consider the targeting and minimization procedures as applied to the acquisition of communications other than Internet transactions – i.e., to the discrete communications between or among the users of telephone and Internet communications facilities that are to or from a facility tasked for collection.[16] The Court will

---

[14](...continued)
occurred despite the government's repeated assurances over the course of nearly [redacted] years that [redacted] authorizations granted by docket number PR/TT [redacted] and previous docket numbers only collect, or collected, authorized metadata." Id. at 20. The overcollection was not detected by NSA until after an "end-to-end review" of the PR/TT metadata program that had been completed by the agency on August 11, 2009. Id.

[15] The government's revelations regarding the scope of NSA's upstream collection implicate 50 U.S.C. § 1809(a), which makes it a crime (1) to "engage[] in electronic surveillance under color of law except as authorized" by statute or (2) to "disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. See [redacted] (concluding that Section 1809(a)(2) precluded the Court from approving the government's proposed use of, among other things, certain data acquired by NSA without statutory authority through its "upstream collection"). The Court will address Section 1809(a) and related issues in a separate order.

[16] As noted, the Court previously authorized the acquisition of [redacted] categories of "about" communications. The Court now understands that all "about" communications are acquired by means of NSA's acquisition of Internet transactions through its upstream collection. See June 1 Submission at 1-2, see also Sept. 7, 2011 Hearing Tr. at 76. Accordingly, the Court considers the (continued...)

then assess the effect of the recent disclosures regarding NSA's collection of Internet transactions on its ability to make the findings necessary to approve the certifications and the NSA targeting and minimization procedures.[17]

B. The Unmodified Procedures

The government represents that the NSA targeting procedures and the FBI minimization procedures filed with the April 2011 Submissions are identical to the corresponding procedures that were submitted to the Court in Docket Nos. [redacted][18] The Court has reviewed each of these sets of procedures and confirmed that is the case. In fact, the NSA targeting procedures and FBI minimization procedures now before the Court are copies

---

[16](...continued)
[redacted]categories of "about" communications to be a subset of the Internet transactions that NSA acquires. The Court's discussion of the manner in which the government proposes to apply its targeting and minimization procedures to Internet transactions generally also applies to the [redacted] categories of "about" communications. See infra, pages 41-79.

[17] The FBI and the CIA do not receive unminimized communications that have been acquired through NSA's upstream collection of Internet communications. Sept. 7, 2011 Hearing Tr. at 61-62. Accordingly, the discussion of Internet transactions that appears below does not affect the Court's conclusions that the FBI targeting procedures, the CIA minimization procedures, and the FBI minimization procedures meet the statutory and constitutional requirements.

[18] See Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [redacted]; Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [redacted]; Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [redacted].

of the procedures that were initially filed on July 29, 2009, in Docket No. [redacted][19] The Court found in those prior dockets that the targeting and minimization procedures were consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment. See Docket No. [redacted] The Court is prepared to renew its past findings that the NSA targeting procedures (as applied to forms of to/from communications that have previously been described to the Court) and the FBI minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.[20]

C. The Amended Procedures

As noted above, the FBI targeting procedures and the NSA and CIA minimization procedures submitted with the April 2011 Submissions differ in a number of respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications [redacted]. For the reasons that follow, the Court finds that, as applied to the previously authorized collection of discrete communications to or from a tasked facility, the amended FBI targeting procedures and the amended NSA and CIA

[19] Copies of those same procedures were also submitted in Docket Nos. [redacted]

[20] The Court notes that the FBI minimization procedures are not "set forth in a clear and self-contained manner, without resort to cross-referencing," as required by FISC Rule 12, which became effective on November 1, 2010. The Court expects that future submissions by the government will comport with this requirement.

minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.

1. The Amended FBI Targeting Procedures

The government has made three changes to the FBI targeting procedures, all of which involve Section I.4. That provision requires the FBI, [redacted]

The new language proposed by the government would allow the FBI to [redacted] The government has advised the Court that this change was prompted by the fact that [redacted] Nevertheless, the current procedures require the FBI to [redacted]. The change is intended to eliminate the requirement of [redacted].

The second change, reflected in subparagraph (a) of Section I.4, would allow the FBI, under certain circumstances, to [redacted]

[redacted]

The above-described changes to the FBI targeting procedures pose no obstacle to a finding by the Court that the FBI targeting procedures are "reasonably designed" to "ensure that any acquisition authorized . . . is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). [redacted]

[redacted]

Furthermore, as the Court has previously noted, before the FBI targeting procedures are applied, NSA will have followed its own targeting procedures in determining that the user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States. See Docket No. [redacted]. The FBI targeting procedures apply in addition to the NSA targeting procedures, [redacted] Id. The Court has previously found that the NSA targeting procedures proposed for use in connection with Certifications [redacted] are reasonably designed to ensure that the users of tasked selectors are non-United States persons reasonably believed to be located outside the United States and also consistent with the Fourth Amendment. See Docket No [redacted]. It therefore follows that the amended FBI targeting procedures, which provide additional assurance that the users of tasked accounts are non-United States persons located outside the United States, also pass muster.

2. The Amended NSA Minimization Procedures

The most significant change to the NSA minimization procedures regards the rules for querying the data that NSA acquires pursuant to Section 702. The procedures previously approved by the Court effectively impose a wholesale bar on queries using United States-Person identifiers. The government has broadened Section 3(b)(5) to allow NSA to query the vast majority of its Section 702 collection using United States-Person identifiers, subject to approval

pursuant to internal NSA procedures and oversight by the Department of Justice.[21] Like all other NSA queries of the Section 702 collection, queries using United States-person identifiers would be limited to those reasonably likely to yield foreign intelligence information. NSA Minimization Procedures § 3(b)(5). The Department of Justice and the Office of the DNI would be required to conduct oversight regarding NSA's use of United States-person identifiers in such queries. See id.

This relaxation of the querying rules does not alter the Court's prior conclusion that NSA minimization procedures meet the statutory definition of minimization procedures. The Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act ("FBI SMPs") contain an analogous provision allowing queries of unminimized FISA-acquired information using identifiers – including United States-person identifiers – when such queries are designed to yield foreign intelligence information. See FBI SMPs § III.D. In granting hundreds of applications for electronic surveillance or physical search since 2008, including applications targeting United States persons and persons in the United States, the Court has found that the FBI SMPs meet the definitions of minimization procedures at 50 U.S.C. §§ 1801(h) and 1821(4). It follows that the substantially-similar

---

[21] The government is still in the process of developing its internal procedures and will not permit NSA analysts to begin using United States-person identifiers as selection terms until those procedures are completed. June 28 Submission at 4 n.3. In addition, the government has clarified that United States-person identifiers will not be used to query the fruits of NSA's upstream collection. Aug. 30 Submission at 11. NSA's upstream collection acquires approximately 9% of the total Internet communications acquired by NSA under Section 702. Aug. 16 Submission at 2.

querying provision found at Section 3(b)(5) of the amended NSA minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons.

A second change to the NSA minimization procedures is the addition of language specifying that the five-year retention period for communications that are not subject to earlier destruction runs from the expiration date of the certification authorizing the collection. See NSA Minimization Procedures, §§ 3(b)(1), 3(c), 5(3)(b), and 6(a)(1)(b). The NSA minimization procedures that were previously approved by the Court included a retention period of five years, but those procedures do not specify when the five-year period begins to run. The change proposed here harmonizes the procedures with the corresponding provision of the FBI minimization procedures for Section 702 that has already been approved by the Court. See FBI Minimization Procedures at 3 (¶ j).

The two remaining changes to the NSA minimization procedures are intended to clarify the scope of the existing procedures. The government has added language to Section 1 to make explicit that the procedures apply not only to NSA employees, but also to any other persons engaged in Section 702-related activities that are conducted under the direction, authority or control of the Director of NSA. NSA Minimization Procedures at 1. According to the government, this new language is intended to clarify that Central Security Service personnel conducting signals intelligence operations authorized by Section 702 are bound by the procedures, even when they are deployed with a military unit and subject to the military chain of

command. The second clarifying amendment is a change to the definition of "identification of a United States person" in Section 2. The new language eliminates a potential ambiguity that might have resulted in the inappropriate treatment of the name, unique title, or address of a United States person as non-identifying information in certain circumstances. Id. at 2. These amendments, which resolve any arguable ambiguity in favor of broader application of the protections found in the procedures, raise no concerns.

3. The Amended CIA Minimization Procedures

The CIA minimization procedures include a new querying provision similar to the provision that the government proposes to add to the NSA minimization procedures and that is discussed above. CIA Minimization Procedures § 4. The new language would allow the CIA to conduct queries of Section 702-acquired information using United States-person identifiers. All CIA queries of the Section 702 collection would be subject to review by the Department of Justice and the Office of the DNI. See id. For the reasons stated above with respect to the relaxed querying provision in the amended NSA minimization procedures, the addition of the new CIA querying provision does not preclude the Court from concluding that the amended CIA minimization procedures satisfy the statutory definition of minimization procedures and comply with the Fourth Amendment.[22]

The amended CIA minimization procedures include a definition of "United States person identity," a term that is not defined in the current version of the procedures. CIA Minimization

[22] The Court understands that NSA does not share its upstream collection in unminimized form with the CIA. [redacted]

Procedures § 1.b. The proposed definition closely tracks the revised definition of "identification of a United States person" that is included in the amended NSA minimization procedures and discussed above. For the same reasons, the addition of this definition, which clarifies the range of protected information, raises no concerns in the context of the CIA minimization procedures.

Another new provision of the CIA minimization procedures prescribes the manner in which the CIA must store unminimized Section 702-acquired communications. See CIA Minimization Procedures § 2. The same provision establishes a default retention period for unminimized communications that do not qualify for longer retention under one of three separate provisions. See id. Absent an extension by the Director of the National Clandestine Service or one of his superiors, that default retention period is five years from the date of the expiration of the certification authorizing the collection. Id. As noted above, this is the same default retention period that appears in the FBI minimization procedures that have previously been approved by the Court. See FBI Minimization Procedures at 3 (¶ j).

The government also has added new language to the CIA minimization procedures to clarify that United States person information deemed to qualify for retention based on its public availability or on the consent of the person to whom it pertains may be kept indefinitely and stored separately from the unminimized information subject to the default storage and retention rules set forth in new Section 2, which is discussed above. CIA Minimization Procedures § 2. Because FISA's minimization requirements are limited to the acquisition, retention, and dissemination of "nonpublicly available information concerning unconsenting United States persons," this provision raises no statutory concern. See 50 U.S.C. §§ 1801(h)(1), 1821(4)(A)

(emphasis added). It likewise raises no Fourth Amendment problem. See Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.").

Finally, a new provision would expressly allow the CIA to retain information acquired pursuant to Section 702 in emergency backup systems that may be used to restore data in the event of a system failure. CIA Minimization Procedures § 6(e). Only non-analyst technical personnel will have access to data stored in data backup systems. Id. Further, in the event that such systems are used to restore lost, destroyed, or inaccessible data, the CIA must apply its minimization procedures to the transferred data. Id. The FBI minimization procedures that have previously been approved by the Court contemplate the storage of Section 702 collection in emergency backup systems that are not accessible to analysts, subject to similar restrictions. See FBI Minimization Procedures at 2 (¶ e.3). The Court likewise sees no problem with the addition of Section 6(e) to the CIA minimization procedures.

D. The Effect of the Government's Disclosures Regarding NSA's Acquisition of Internet Transactions

Based on the government's prior representations, the Court has previously analyzed NSA's targeting and minimization procedures only in the context of NSA acquiring discrete communications. Now, however, in light of the government's revelations as to the manner in which NSA acquires Internet communications, it is clear that NSA acquires "Internet

transactions,"[23] including transactions that contain a single discrete communication ("Single Communication Transactions" or "SCTs"), and transactions that contain multiple discrete communications ("Multi-[C]ommunication Transactions" or "MCTs"), see Aug. 16 Submission at 1.

The Court has repeatedly noted that the government's targeting and minimization procedures must be considered in light of the communications actually acquired. See Docket No. [redacted] ("Substantial 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."), see also Docket No. [redacted] Until now, the Court had a singular understanding of the nature of NSA's acquisitions under Section 702. Accordingly, analysis of the implementation of the procedures focused on whether NSA's procedures were applied effectively in that context and whether the procedures adequately addressed over-collections that occurred. But, for the first time, the government has now advised the Court that the volume and nature of the information it has been collecting is fundamentally different from what the Court had been led to believe. Therefore, the Court must, as a matter of first impression, consider whether, in view of NSA's acquisition of Internet transactions, the targeting and minimization procedures satisfy the statutory standards and comport with the

---

[23] The government describes an Internet "transaction" as "a complement of 'packets' traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device." June 1 Submission at 1.

Fourth Amendment.

For the reasons set forth below, the Court finds that NSA's targeting procedures, as the government proposes to implement them in connection with MCTs, are consistent with the requirements of 50 U.S.C. §1881a(d)(1). However, the Court is unable to find that NSA's minimization procedures, as the government proposes to apply them in connection with MCTs, are "reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1) &1821(4)(A). The Court is also unable to find that NSA's targeting and minimization procedures, as the government proposes to implement them in connection with MCTs, are consistent with the Fourth Amendment.

1. The Scope of NSA's Upstream Collection

NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702, but the vast majority of these communications are obtained from Internet service providers and are not at issue here.[24] Sept. 9 Submission at 1; Aug. 16 Submission at Appendix A. Indeed, NSA's upstream collection constitutes only approximately

[24] In addition to its upstream collection, NSA acquires discrete Internet communications from Internet service providers such as [redacted] Aug. 16 Submission at 2; Aug. 30 Submission at 11; see also Sept. 7, 2011 Hearing Tr. at 75-77. NSA refers to this non-upstream collection as its "PRISM collection." Aug. 30 Submission at 11. The Court understands that NSA does not acquire "Internet transactions" through its PRISM collection. See Aug. 16 Submission at 1.

9% of the total Internet communications being acquired by NSA under Section 702. Sept. 9 Submission at 1; Aug. 16 Submission at 2.

Although small in relative terms, NSA's upstream collection is significant for three reasons. First, NSA's upstream collection is "uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information."[25] Docket No. [redacted].

Second, the Court now understands that, in order to collect those targeted Internet communications, NSA's upstream collection devices acquire Internet transactions, and NSA acquires millions of such transactions each year.[26] Third, the government has acknowledged that, due to the technological challenges associated with acquiring Internet transactions, NSA is unable to exclude certain Internet transactions from its upstream collection. See June 1 Submission at 3-12.

In its June 1 Submission, the government explained that NSA's upstream collection devices have technological limitations that significantly affect the scope of collection. [redacted]

[redacted]

[25] [redacted]

[26] NSA acquired more than 13.25 million Internet transactions through its upstream collection between January 1, 2011, and June 30, 2011. See Aug. 16 Submission at 2; see also Sept. 9 Submission at 1-2.

[redacted]. See id. at 7. Moreover, at the time of acquisition, NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector.[27] Id. at 2.

As a practical matter, this means that NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it, and:

[redacted]

See id. at 6.

The practical implications of NSA's acquisition of Internet transactions through its upstream collection for the Court's statutory and Fourth Amendment analyses are difficult to assess. The sheer volume of transactions acquired by NSA through its upstream collection is such that any meaningful review of the entire body of the transactions is not feasible. As a result, the Court cannot know for certain the exact number of wholly domestic communications acquired through this collection, nor can it know the number of non-target communications

[redacted]

acquired or the extent to which those communications are to or from United States persons or persons in the United States. Instead, NSA and the Court can only look at samples of the data and then draw whatever reasonable conclusions they can from those samples. Even if the Court accepts the validity of conclusions derived from statistical analyses, there are significant hurdles in assessing NSA's upstream collection. Internet service providers are constantly changing their protocols and the services they provide, and often give users the ability to customize how they use a particular service.[28] Id. at 24-25. As a result, it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future.

Recognizing that further revelations concerning what NSA has actually acquired through its 702 collection, together with the constant evolution of the Internet, may alter the Court's analysis at some point in the future, the Court must, nevertheless, consider whether NSA's targeting and minimization procedures are consistent with FISA and the Fourth Amendment based on the record now before it. In view of the revelations about how NSA is actually conducting its upstream collection, two fundamental underpinnings of the Court's prior assessments no longer hold true.

---

28 [redacted]

First, the Court previously understood that NSA's technical measures[29] would prevent the acquisition of any communication as to which the sender and all intended recipients were located in the United States ("wholly domestic communication") except for "theoretically possible" cases [redacted] The Court now understands, however, that NSA has acquired, is acquiring, and, if the certifications and procedures now before the Court are approved, will continue to acquire, tens of thousands of wholly domestic communications. NSA's manual review of a statistically representative sample drawn from its upstream collection[30] reveals that NSA acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication.[31] See Aug. 16 Submission at 9. In addition to these MCTs, NSA

[29] [redacted]

[30] In an effort to address the Court's concerns, NSA conducted a manual review of a random sample consisting of 50,440 Internet transactions taken from the more than 13.25 million Internet transactions acquired through NSA's upstream collection during a six month period. See generally Aug. 16 Submission (describing NSA's manual review and the conclusions NSA drew therefrom). The statistical conclusions reflected in this Memorandum Opinion are drawn from NSA's analysis of that random sample.

[31] Of the approximately 13.25 million Internet transactions acquired by NSA through its upstream collection during the six-month period, between 996 and 4,965 are MCTs that contain a wholly domestic communication not to, from, or about a tasked selector. Aug. 16 Submission at 9.

likely acquires tens of thousands more wholly domestic communications every year,[32] given that NSA's upstream collection devices will acquire a wholly domestic "about" SCT if it is routed internationally.[33] Moreover, the actual number of wholly domestic communications acquired

---

[32] NSA's manual review focused on examining the MCTs acquired through NSA's upstream collection in order to assess whether any contained wholly domestic communications. Sept. 7, 2011 Hearing Tr. at 13-14. As a result, once NSA determined that a transaction contained a single, discrete communication, no further analysis of that transaction was done. See Aug. 16 Submission at 3. After the Court expressed concern that this category of transactions might also contain wholly domestic communications, NSA conducted a further review. See Sept. 9 Submission at 4. NSA ultimately did not provide the Court with an estimate of the number of wholly domestic "about" SCTs that may be acquired through its upstream collection. Instead, NSA has concluded that "the probability of encountering wholly domestic communications in transactions that feature only a single, discrete communication should be smaller – and certainly no greater – than potentially encountering wholly domestic communications within MCTs." Sept. 13 Submission at 2.

The Court understands this to mean that the percentage of wholly domestic communications within the universe of SCTs acquired through NSA's upstream collection should not exceed the percentage of MCTs containing a wholly domestic communication that NSA found when it examined all of the MCTs within its statistical sample. Since NSA found 10 MCTs with wholly domestic communications within the 5,081 MCTs reviewed, the relevant percentage is .197% (10/5,081). Aug. 16 Submission at 5.

NSA's manual review found that approximately 90% of the 50,440 transactions in the sample were SCTs. Id. at 3. Ninety percent of the approximately 13.25 million total Internet transactions acquired by NSA through its upstream collection during the six-month period, works out to be approximately 11,925,000 transactions. Those 11,925,000 transactions would constitute the universe of SCTs acquired during the six-month period, and .197% of that universe would be approximately 23,000 wholly domestic SCTs. Thus, NSA may be acquiring as many as 46,000 wholly domestic "about" SCTs each year, in addition to the 2,000-10,000 MCTs referenced above.

[33] Internet communications are "nearly always transmitted from a sender to a recipient through multiple legs before reaching their final destination." June 1 Submission at 6. For example, an e-mail message sent from the user of [redacted] to the user of [redacted] will at the very least travel from the [redacted] user's own computer, to [redacted], to [redacted], and then to the computer of the [redacted] user. Id. Because the communication's route is made up of multiple legs, the transaction used to transmit the communication across any particular leg of the route need only identify the IP

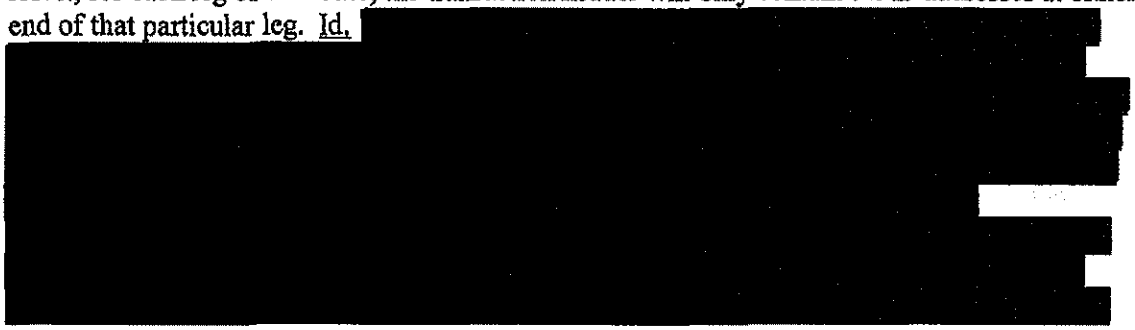
(continued...)

may be still higher in view of NSA's inability conclusively to determine whether a significant portion of the MCTs within its sample contained wholly domestic communications.[34]

Second, the Court previously understood that NSA's upstream collection would only acquire the communication of a United States person or a person in the United States if: 1) that

---

[33](...continued)
addresses at either end of that leg in order to properly route the communication. Id. at 7. As a result, for each leg of the route, the transaction header will only contain the IP addresses at either end of that particular leg. Id.



[34] During its manual review, NSA was unable to determine whether 224 of the 5,081 MCTs reviewed contained any wholly domestic communications, because the transactions lacked sufficient information for NSA to determine the location or identity of the "active user" (i.e., the individual using the electronic communications account/address/identifier to interact with his/her Internet service provider). Aug. 16 Submission at 7. NSA then conducted an intensive review of all available information for each of these MCTs, including examining the contents of each discrete communication contained within it, but was still unable to determine conclusively whether any of these MCTs contained wholly domestic communications. Sept. 9 Submission at 3. NSA asserts that "it is reasonable to presume that [the] 224 MCTs do not contain wholly domestic communications," but concedes that, due to the limitations of the technical means used to prevent the acquisition of wholly domestic communications, NSA may acquire wholly domestic communications. See Aug. 30 Submission at 7-8. The Court is prepared to accept that the number of wholly domestic communications acquired in this category of MCTs is relatively small, for the reasons stated in the government's August 30 Submission. However, when considering NSA's upstream collection as a whole, and the limitations of NSA's technical means, the Court is not prepared to presume that the number of wholly domestic communications contained within this category of communications will be zero. Accordingly, the Court concludes that this category of communications acquired through NSA's upstream collection may drive the total number of wholly domestic communications acquired slightly higher.

person was in direct contact with a targeted selector; 2) the communication referenced the targeted selector, and the communication fell into one of [redacted] specific categories of "about" communications; or 3) despite the operation of the targeting procedures, United States persons or persons inside the United States were mistakenly targeted. See Docket No. [redacted]. But the Court now understands that, in addition to these communications, NSA's upstream collection also acquires: a) the communications of United States persons and persons in the United States that are not to, from, or about a tasked selector and that are acquired solely because the communication is contained within an MCT that somewhere references a tasked selector [redacted] and b) any Internet transaction that references a targeted selector, regardless of whether the transaction falls within one of the [redacted] previously identified categories of "about communications," see June 1 Submission at 24-27. [redacted]

On the current record, it is difficult to assess how many MCTs acquired by NSA actually contain a communication of or concerning a United States person,[35] or a communication to or from a person in the United States. This is because NSA's manual review of its upstream collection focused primarily on wholly domestic communications – i.e., if one party to the

[35] NSA's minimization procedures define "[c]ommunications of a United States person" to include "all communications to which a United States person is a party." NSA Minimization Procedures § 2(c). "Communications concerning a United States person" include "all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person. Id. § 2(b).

communication was determined to be outside the United States, the communication was not further analyzed. Aug. 16 Submission at 1-2. Nevertheless, NSA's manual review did consider the location and identity of the active user for each MCT acquired, and this information – when considered together with certain presumptions -- shows that NSA is likely acquiring tens of thousands of discrete communications of non-target United States persons and persons in the United States, by virtue of the fact that their communications are included in MCTs selected for acquisition by NSA's upstream collection devices.[36]

To illustrate, based upon NSA's analysis of the location and identity of the active user for the MCTs it reviewed, MCTs can be divided into four categories:

1. MCTs as to which the active user is the user of the tasked facility (i.e., the target of the acquisition) and is reasonably believed to be located outside the United States;[37]

2. MCTs as to which the active user is a non-target who is believed to be located inside the United States;

3. MCTs as to which the active user is a non-target who is believed to be located outside the United States; and

---

[36] Although there is some overlap between this category of communications and the tens of thousands of wholly domestic communications discussed above, the overlap is limited to MCTs containing wholly domestic communications. To the extent that the wholly domestic communications acquired are SCTs, they are excluded from the MCTs referenced here. Similarly, to the extent communications of non-target United States persons and persons in the United States that are contained within the tens of thousands of MCTs referenced here are not wholly domestic, they would not be included in the wholly domestic communications referenced above.

[37] Although it is possible for an active user target to be located in the United States, NSA's targeting procedures require NSA to terminate collection if it determines that a target has entered the United States. NSA Targeting Procedures at 7-8. Accordingly, the Court excludes this potential category from its analysis.

4. MCTs as to which the active user's identity or location cannot be determined.

Aug. 16 Submission at 4-8.

With regard to the first category, if the target is the active user, then it is reasonable to presume that all of the discrete communications within an MCT will be to or from the target. Although United States persons and persons in the United States may be party to any of those communications, NSA's acquisition of such communications is of less concern than the communications described in the following categories because the communicants were in direct communication with a tasked facility, and the acquisition presumptively serves the foreign intelligence purpose of the collection. NSA acquires roughly 300-400 thousand such MCTs per year.[38]

For the second category, since the active user is a non-target who is located inside the United States, there is no reason to believe that all of the discrete communications contained within the MCTs will be to, from, or about the targeted selector (although there would need to be at least one such communication in order for NSA's upstream devices to acquire the transaction). Further, because the active user is in the United States, the Court presumes that the majority of that person's communications will be with other persons in the United States, many of whom will be United States persons. NSA acquires approximately 7,000-8,000 such MCTs per year, each of which likely contains one or more non-target discrete communications to or from other

[38] NSA acquired between 168,853 and 206,922 MCTs as to which the active user was the target over the six-month period covered by the sample. Aug. 16 Submission at 9.

persons in the United States.[39]

The third category is similar to the second in that the active user is a non-target. Therefore, there is no reason to believe that all of the communications within the MCTs will be to, from, or about the targeted selector (although there would need to be at least one such communication in order for NSA's upstream devices to acquire the transaction). However, because the active user is believed to be located outside the United States, the Court presumes that most of that persons's communications will be with other persons who are outside the United States, most of whom will be non-United States persons. That said, the Court notes that some of these MCTs are likely to contain non-target communications of or concerning United States persons, or that are to or from a person in the United States.[40] The Court has no way of knowing precisely how many such communications are acquired. Nevertheless, it appears that NSA acquires at least 1.3 million such MCTs each year,[41] so even if only 1% of these MCTs

---

[39] In its manual review, NSA identified ten MCTs as to which the active user was in the United States and that contained at least one wholly domestic communication. See Aug. 16 Submission at 5-7. NSA also identified seven additional MCTs as to which the active user was in the United States. Id. at 5. Although NSA determined that at least one party to each of the communications within the seven MCTs was reasonably believed to be located outside the United States, NSA did not indicate whether any of the communicants were United States persons or persons in the United States. Id. The Court sees no reason to treat these two categories of MCTs differently because the active users for both were in the United States. Seventeen MCTs constitutes .3% of the MCTs reviewed (5,081), and .3% of the 1.29-1.39 million MCTs NSA acquires every six months (see id. at 8) is 3,870- 4,170, or 7,740-8,340 every year.

[40] The government has acknowledged as much in its submissions. See June 28 Submission at 5.

[41] Based on its manual review, NSA assessed that 2668 of the 5,081 MCTs reviewed (continued...)

contain a single non-target communication of or concerning a United States person, or that is to or from a person in the United States, NSA would be acquiring in excess of 10,000 additional discrete communications each year that are of or concerning United States persons, or that are to or from a person in the United States.

The fourth category is the most problematic, because without the identity of the active user – i.e., whether the user is the target or a non-target – or the active user's location, it is difficult to determine what presumptions to make about these MCTs. NSA acquires approximately 97,000-140,000 such MCTs each year.[42] In the context of wholly domestic communications, the government urges the Court to apply a series of presumptions that lead to the conclusion that this category would not contain any wholly domestic communications. Aug. 30 Submission at 4-8. The Court questions the validity of those presumptions, as applied to wholly domestic communications, but certainly is not inclined to apply them to assessing the likelihood that MCTs might contain communications of or concerning United States persons, or communications to or from persons in the United States. The active users for some of these

---

[41](...continued)
(approximately 52%) had a non-target active user who was reasonably believed to be located outside the United States. Aug. 16 Submission at 4-5. Fifty-two percent of the 1.29 to 1.39 million MCTs that NSA assessed were acquired through its upstream collection every six months would work out to 670,800 - 722,800 MCTs, or approximately 1.3-1.4 million MCTs per year that have a non-target active user believed to be located outside the United States.

[42] NSA determined that 224 MCTs of the 5,081 MCTs acquired during a six-month period [redacted] From this, NSA concluded that it acquired between 48,609 and 70,168 such MCTs every six months through its upstream collection (or approximately 97,000-140,000 such MCTs each year). Id. at 9 n.27.

MCTs may be located in the United States, and, even if the active user is located overseas, the MCTs may contain non-target communications of or concerning United States persons or that are to or from persons in the United States. Accordingly, this "unknown" category likely adds substantially to the number of non-target communications of or concerning United States persons or that are to or from persons in the United States being acquired by NSA each year.

In sum, then, NSA's upstream collection is a small, but unique part of the government's overall collection under Section 702 of the FAA. NSA acquires valuable information through its upstream collection, but not without substantial intrusions on Fourth Amendment-protected interests. Indeed, the record before this Court establishes that NSA's acquisition of Internet transactions likely results in NSA acquiring annually tens of thousands of wholly domestic communications, and tens of thousands of non-target communications of persons who have little or no relationship to the target but who are protected under the Fourth Amendment. Both acquisitions raise questions as to whether NSA's targeting and minimization procedures comport with FISA and the Fourth Amendment.

2. NSA's Targeting Procedures

The Court will first consider whether NSA's acquisition of Internet transactions through its upstream collection, as described above, means that NSA's targeting procedures, as implemented, are not "reasonably designed" to: 1) "ensure that any acquisition authorized under [the certifications] is limited to targeting persons reasonably believed to be located outside the United States"; and 2) "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the

United States." 50 U.S.C. § 1881a(d)(1); id. § (i)(2)(B). The Court concludes that the manner in which NSA is currently implementing the targeting procedures does not prevent the Court from making the necessary findings, and hence NSA's targeting procedures do not offend FISA.

a. Targeting Persons Reasonably Believed to be Located Outside the United States

To the extent NSA is acquiring Internet transactions that contain a single discrete communication that is to, from, or about a tasked selector, the Court's previous analysis remains valid. As explained in greater detail in the Court's September 4, 2008 Memorandum Opinion, in this setting the person being targeted is the user of the tasked selector, and NSA's pre-targeting and post-targeting procedures ensure that NSA will only acquire such transactions so long as there is a reasonable belief that the target is located outside the United States. Docket No. [redacted].

But NSA's acquisition of MCTs complicates the Court's analysis somewhat. With regard to "about" communications, the Court previously found that the user of the tasked facility was the "target" of the acquisition, because the government's purpose in acquiring such communications is to obtain information about that user. See id. at 18. Moreover, the communication is not acquired because the government has any interest in the parties to the communication, other than their potential relationship to the user of the tasked facility, and the parties to an "about" communication do not become targets unless and until they are separately vetted under the targeting procedures. See id. at 18-19.

In the case of "about" MCTs – i.e., MCTs that are acquired because a targeted selector is referenced somewhere in the transaction – NSA acquires not only the discrete communication

that references the tasked selector, but also in many cases the contents of other discrete communications that do not reference the tasked selector and to which no target is a party. See May 2 Letter at 2-3 [redacted] By acquiring such MCTs, NSA likely acquires tens of thousands of additional communications of non-targets each year, many of whom have no relationship whatsoever with the user of the tasked selector. While the Court has concerns about NSA's acquisition of these non-target communications, the Court accepts the government's representation that the "sole reason [a non-target's MCT] is selected for acquisition is that it contains the presence of a tasked selector used by a person who has been subjected to NSA's targeting procedures." June 1 Submission at 4. Moreover, at the time of acquisition, NSA's upstream collection devices often lack the capability to determine whether a transaction contains a single communication or multiple communications, or to identify the parties to any particular communication within a transaction. See id. Therefore, the Court has no reason to believe that NSA, by acquiring Internet transactions containing multiple communications, is targeting anyone other than the user of the tasked selector. See United States v. Chemical Found., Inc., 272 U.S. 1, 14-15 (1926) ("The presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties.").

b. Acquisition of Wholly Domestic Communications

NSA's acquisition of Internet transactions complicates the analysis required by Section 1881a(d)(1)(B), since the record shows that the government knowingly acquires tens of thousands of wholly domestic communications each year. At first blush, it might seem obvious

that targeting procedures that permit such acquisitions could not be "reasonably designed . . . to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1)(B). However, a closer examination of the language of the statute leads the Court to a different conclusion.

The government focuses primarily on the "intentional acquisition" language in Section 1881a(d)(1)(B). Specifically, the government argues that NSA is not "intentionally" acquiring wholly domestic communications because the government does not intend to acquire transactions containing communications that are wholly domestic and has implemented technical means to prevent the acquisition of such transactions. See June 28 Submission at 12. This argument fails for several reasons.

NSA targets a person under Section 702 certifications by acquiring communications to, from, or about a selector used by that person. Therefore, to the extent NSA's upstream collection devices acquire an Internet transaction containing a single, discrete communication that is to, from, or about a tasked selector, it can hardly be said that NSA's acquisition is "unintentional." In fact, the government has argued, and the Court has accepted, that the government intentionally acquires communications to and from a target, even when NSA reasonably – albeit mistakenly – believes that the target is located outside the United States. See Docket No. [redacted]

[redacted]

With respect to MCTs, the sole reason NSA acquires such transactions is the presence of a tasked selector within the transaction. Because it is technologically infeasible for NSA's

upstream collection devices to acquire only the discrete communication to, from, or about a tasked selector that may be contained within an MCT, however, the government argues that the only way to obtain the foreign intelligence information found within the discrete communication is to acquire the entire transaction in which it is contained. June 1 Submission at 21. As a result, the government intentionally acquires all discrete communications within an MCT, including those that are not to, from or about a tasked selector. See June 28 Submission at 12, 14; see also Sept. 7, 2011 Hearing Tr. at 33-34.

The fact that NSA's technical measures cannot prevent NSA from acquiring transactions containing wholly domestic communications under certain circumstances does not render NSA's acquisition of those transactions "unintentional." The government repeatedly characterizes such acquisitions as a "failure" of NSA's "technical means." June 28 Submission at 12; see also Sept. 7, 2011 Hearing Tr. at 35-36. However, there is nothing in the record to suggest that NSA's technical means are malfunctioning or otherwise failing to operate as designed. Indeed, the government readily concedes that NSA will acquire a wholly domestic "about" communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server. See June 1 Submission at 29. And in the case of MCTs containing wholly domestic communications that are not to, from, or about a tasked selector, NSA has no way to determine, at the time of acquisition, that a particular communication within an MCT is wholly domestic. See id. Furthermore, now that NSA's manual review of a sample of its upstream collection has confirmed that NSA likely acquires tens of thousands of wholly domestic communications each year, there is no question that the

government is knowingly acquiring Internet transactions that contain wholly domestic communications through its upstream collection.[43]

The government argues that an NSA analyst's post-acquisition discovery that a particular Internet transaction contains a wholly domestic communication should retroactively render NSA's acquisition of that transaction "unintentional." June 28 Submission at 12. That argument is unavailing. NSA's collection devices are set to acquire transactions that contain a reference to the targeted selector. When the collection device acquires such a transaction, it is functioning precisely as it is intended, even when the transaction includes a wholly domestic communication. The language of the statute makes clear that it is the government's intention at the time of acquisition that matters, and the government conceded as much at the hearing in this matter. Sept. 7, 2011 Hearing Tr. at 37-38.

Accordingly, the Court finds that NSA intentionally acquires Internet transactions that reference a tasked selector through its upstream collection with the knowledge that there are tens of thousands of wholly domestic communications contained within those transactions. But this is not the end of the analysis. To return to the language of the statute, NSA's targeting procedures must be reasonably designed to prevent the intentional acquisition of "any communication as to which the sender and all intended recipients are known at the time of

[43] It is generally settled that a person intends to produce a consequence either (a) when he acts with a purpose of producing that consequence or (b) when he acts knowing that the consequence is substantially certain to occur. Restatement (Third) of Torts § 1 (2010); see also United States v. Dyer, 589 F.3d 520, 528 (1st Cir. 2009) (in criminal law, "'intent' ordinarily requires only that the defendant reasonably knew the proscribed result would occur"), cert. denied, 130 S. Ct. 2422 (2010).

acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1)(B) (emphasis added). The underscored language requires an acquisition-by-acquisition inquiry. Thus, the Court must consider whether, at the time NSA intentionally acquires a transaction through its upstream collection, NSA will know that the sender and all intended recipients of any particular communication within that transaction are located in the United States.

Presently, it is not technically possible for NSA to configure its upstream collection devices [redacted] the practical effect of this technological limitation is that NSA cannot know at the time it acquires an Internet transaction whether the sender and all intended recipients of any particular discrete communication contained within the transaction are located inside the United States.

[redacted]

[44] See supra, note 33.

[redacted]

Given that NSA's upstream collection devices lack the capacity to detect wholly domestic communications at the time an Internet transaction is acquired, the Court is inexorably led to the conclusion that the targeting procedures are "reasonably designed" to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. This is true despite the fact that NSA knows with certainty that the upstream collection, viewed as a whole, results in the acquisition of wholly domestic communications.

By expanding its Section 702 acquisitions to include the acquisition of Internet transactions through its upstream collection, NSA has, as a practical matter, circumvented the spirit of Section 1881a(b)(4) and (d)(1) with regard to that collection. NSA's knowing acquisition of tens of thousands of wholly domestic communications through its upstream collection is a cause of concern for the Court. But the meaning of the relevant statutory provision is clear and application to the facts before the Court does not lead to an impossible or absurd result. The Court's review does not end with the targeting procedures, however. The Court must

also consider whether NSA's minimization procedures are consistent with §1881a(e)(1) and whether NSA's targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

3. NSA's Minimization Procedures, As Applied to MCTs in the Manner Proposed by the Government, Do Not Meet FISA's Definition of "Minimization Procedures"

The Court next considers whether NSA's minimization procedures, as the government proposes to apply them to Internet transactions, meet the statutory requirements. As noted above, 50 U.S.C. § 1881a(e)(1) requires that the minimization procedures "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4) . . . ." That definition requires "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A). For the reasons stated below, the Court concludes that NSA's minimization procedures, as applied to MCTs in the manner proposed by the government, do not meet the statutory definition in all respects.

a. The Minimization Framework

NSA's minimization procedures do not expressly contemplate the acquisition of MCTs, and the language of the procedures does not lend itself to straightforward application to MCTs. Most notably, various provisions of the NSA minimization procedures employ the term

"communication" as an operative term. As explained below, for instance, the rules governing retention, handling, and dissemination vary depending whether or not a communication is deemed to constitute a "domestic communication" instead of a "foreign communication," see NSA Minimization Procedures §§ 2(e), 5, 6, 7; a communication "of" or "concerning" a U.S. person, see id. §§ 2(b)-(c), 3(b)(1)-(2), 3(c); a "communication to, from, or about a target," id. § 3(b)(4); or a "communication . . . reasonably believed to contain foreign intelligence information or evidence of a crime," id. But MCTs can be fairly described as communications that contain several smaller communications. Applying the terms of the NSA minimization procedures to MCTs rather than discrete communications can produce very different results.

In a recent submission, the government explained how NSA proposes to apply its minimization procedures to MCTs. See Aug. 30 Submission at 8-11.[45] Before discussing the measures proposed by the government for handling MCTs, it is helpful to begin with a brief overview of the NSA minimization procedures themselves. The procedures require that all acquisitions "will be conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant to the authorized purpose of the collection." NSA

[45] Although NSA has been collecting MCTs since before the Court's approval of the first Section 702 certification in 2008, see June 1 Submission at 2, it has not, to date, applied the measures proposed here to the fruits of its upstream collection. Indeed, until NSA's manual review of a six-month sample of its upstream collection revealed the acquisition of wholly domestic communications, the government asserted that NSA had never found a wholly domestic communication in its upstream collection. See id.

Minimization Procedures § 3(a).[46] Following acquisition, the procedures require that, "[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime." Id. § 3(b)(4). "Foreign communication means a communication that has at least one communicant outside of the United States." Id. § 2(e). "All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications." Id. In addition, domestic communications include "[a]ny communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of the targeting was believed to be a non-United States person but was in fact a United States person . . . ." Id. § 3(d)(2). A domestic communication must be "promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that" the communication contains foreign intelligence

[46] Of course, NSA's separate targeting procedures, discussed above, also govern the manner in which communications are acquired.

information or evidence of a crime, or that it falls into another narrow exception permitting retention. See id. § 5.[47]

Upon determining that a communication is a "foreign communication," NSA must decide whether the communication is "of" or "concerning" a United States person. Id. § 6. "Communications of a United States person include all communications to which a United States person is a party." Id. § 2(c). "Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person." Id. § 2(b).

A foreign communication that is of or concerning a United States person and that is determined to contain neither foreign intelligence information nor evidence of a crime must be destroyed "at the earliest practicable point in the processing cycle," and "may be retained no longer than five years from the expiration date of the certification in any event." Id. § 3(b)(1).[48]

---

[47] Once such a determination is made by the Director, the domestic communications at issue are effectively treated as "foreign communications" for purposes of the rules regarding retention and dissemination.

[48] Although Section 3(b)(1) by its terms applies only to "inadvertently acquired communications of or concerning a United States person," the government has informed the Court that this provision is intended to apply, and in practice is applied, to all foreign communications of or concerning United States persons that contain neither foreign intelligence information nor evidence of a crime. Docket No. 702(i)-08-01, Sept. 2, 2008 Notice of Clarification and Correction at 3-5. Moreover, Section 3(c) of the procedures separately provides that foreign communications that do not qualify for retention and that "are known to contain communications of or concerning United States persons will be destroyed upon recognition," and, like unreviewed communications, "may be retained no longer than five years from the

(continued...)

A foreign communication that is of or concerning a United States person may be retained indefinitely if the "dissemination of such communications with reference to such United States persons would be permitted" under the dissemination provisions that are discussed below, or if it contains evidence of a crime. Id. § 6(a)(2)-(3). If the retention of a foreign communication of or concerning a United States person is "necessary for the maintenance of technical databases," it may be retained for five years to allow for technical exploitation, or for longer than five years if more time is required for decryption or if the NSA Signals Intelligence Director "determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements." Id. § 6(a)(1).

As a general rule, "[a] report based on communications of or concerning a United States person may be disseminated" only "if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person." Id. § 6(b). A report including the identity of the United States person may be provided to a "recipient requiring the identity of such person for the performance of official duties," but only if at least one of eight requirements is also met – for instance, if "the identity of the United States person is necessary to understand foreign intelligence information or assess its importance," or if "information indicates the United States

---

[48](...continued)
expiration date of the certification authorizing the collection in any event."

person may be . . . an agent of a foreign power" or that he is "engaging in international terrorism activities." Id.[49]

b. Proposed Minimization Measures for MCTs

The government proposes that NSA's minimization procedures be applied to MCTs in the following manner. After acquisition, upstream acquisitions, including MCTs, will reside in NSA repositories until they are accessed (e.g., in response to a query) by an NSA analyst performing his or her day-to-day work. NSA proposes adding a "cautionary banner" to the tools its analysts use to view the content of communications acquired through upstream collection under Section 702. See Aug. 30 Submission at 9. The banner, which will be "broadly displayed on [such] tools," will "direct analysts to consult guidance on how to identify MCTs and how to handle them." Id. at 9 & n.6.[50] Analysts will be trained to identify MCTs and to recognize wholly domestic communications contained within MCTs. See id. at 8-9.

When an analyst identifies an upstream acquisition as an MCT, the analyst will decide whether or not he or she "seek[s] to use a discrete communication within [the] MCT,"

---

[49] The procedures also permit NSA to provide unminimized communications to the CIA and FBI (subject to their own minimization procedures), and to foreign governments for the limited purpose of obtaining "technical and linguistic assistance." NSA Minimization Procedures §§ 6(c), 8(b). Neither of these provisions has been used to share upstream acquisitions. Sept. 7, 2011 Hearing Tr. at 61-62.

[50] The banner will not be displayed for communications that "can be first identified through technical means where the active user is NSA's tasked selector or that contain only a single, discrete communication based on particular stable and well-known protocols." Aug. 30 Submission at 9 n.6. See infra, note 27, and supra, note 54.

presumably by reviewing some or all of the MCT's contents. Id. at 8.[51] "NSA analysts seeking to use a discrete communication contained in an MCT (for example, in a FISA application, intelligence report, or Section 702 targeting) will assess whether the discrete communication is to, from, or about a tasked selector." Id. The following framework will then be applied:

- If the discrete communication that the analyst seeks to use is to, from, or about a tasked selector, "any U.S. person information in that communication will be handled in accordance with the NSA minimization procedures." Id. Presumably, this means that the discrete communication will be treated as a "foreign communication" that is "of" or "concerning" a United States person, as described above. The MCT containing that communication remains available to analysts in NSA's repositories without any marking to indicate that it has been identified as an MCT or as a transaction containing United States person information.

- If the discrete communication sought to be used is not to, from, or about a tasked selector, and also not to or from an identifiable United States person, "that communication (including any U.S. person information therein) will be handled in accordance with the NSA minimization procedures." Id. at 8-9.[52] Presumably, this means that the discrete communication will be treated as a "foreign communication" or, if it contains information concerning a United States person, as a "foreign communication" "concerning a United States person," as described above. The MCT itself remains available to analysts in NSA's repositories without any marking to indicate that it has been identified as an MCT or that it contains one or more communications that are not to, from, or about a targeted selector.

---

[51] A transaction that is identified as an SCT rather than an MCT must be handled in accordance with the standard minimization procedures that are discussed above.

[52] The Court understands that absent contrary information, NSA treats the user of an account who appears to be located in the United States as "an identifiable U.S. person." See Aug. 30 Submission at 9 n.7 ("To help determine whether a discrete communication not to, from, or about a tasked selector is to or from a U.S. person, NSA would perform the same sort of technical analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its section 702 targeting procedures.").

• A discrete communication that is not to, from, or about a tasked selector but that is to or from an identifiable United States person "cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations)." Id. at 9. Presumably, this is a reference to Section 1 of the minimization procedures, which allows NSA to deviate from the procedures in such narrow circumstances, subject to the requirement that prompt notice be given to the Office of the Director of National Intelligence, the Department of Justice, and the Court that the deviation has occurred. Regardless of whether or not the discrete communication is used for this limited purpose, the MCT itself remains in NSA's databases without any marking to indicate that it is an MCT, or that it contains at least one communication that is to or from an identifiable United States person. See id.; Sept. 7, 2011 Hearing Tr. at 61.

• If the discrete communication sought to be used by the analyst (or another discrete communication within the MCT) is recognized as being wholly domestic, the entire MCT will be purged from NSA's systems. See Aug. 30 Submission at 3.

c. Statutory Analysis

i. Acquisition

The Court first considers how NSA's proposed handling of MCTs bears on whether NSA's minimization procedures are "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition . . . of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. § 1801(h)(1) (emphasis added). Insofar as NSA likely acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication that is neither to, from, nor about a targeted selector,[53] and tens of thousands of communications of or

[53] As noted above, NSA's upstream collection also likely results in the acquisition of tens (continued...)

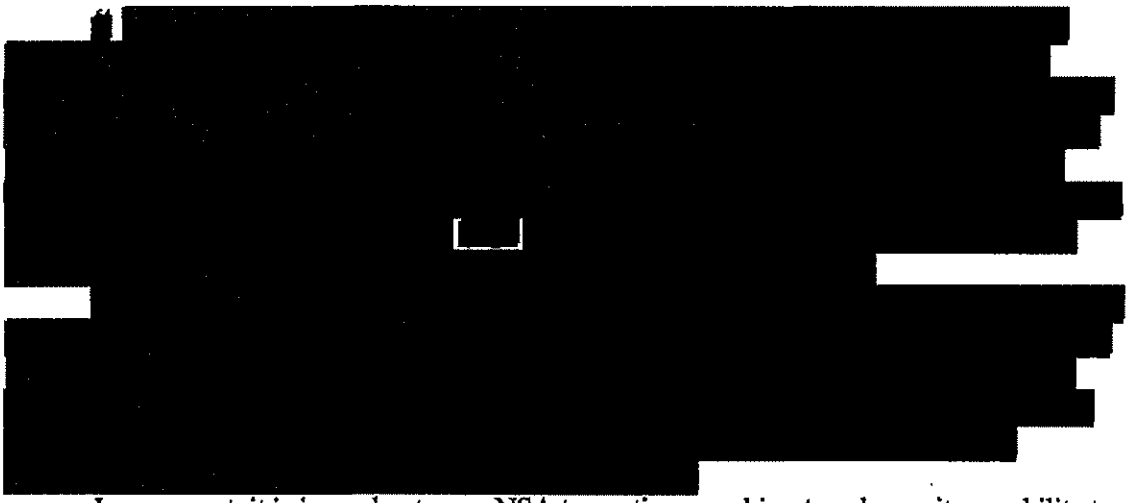
concerning United States persons with no direct connection to any target, the Court has serious concerns. The acquisition of such non-target communications, which are highly unlikely to have foreign intelligence value, obviously does not by itself serve the government's need to "obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. § 1801(h)(1).

The government submits, however, that the portions of MCTs that contain references to targeted selectors are likely to contain foreign intelligence information, and that it is not feasible for NSA to limit its collection only to the relevant portion or portions of each MCT – i.e., the particular discrete communications that are to, from, or about a targeted selector. The Court

---

[53](...continued)
of thousands of wholly domestic SCTs that contain references to targeted selectors. See supra, pages 33-34 & note 33 (discussing the limits [redacted] Although the collection of wholly domestic "about" SCTs is troubling, they do not raise the same minimization-related concerns as discrete, wholly domestic communications that are neither to, from, nor about targeted selectors, or as discrete communications of or concerning United States persons with no direct connection to any target, either of which may be contained within MCTs. The Court has effectively concluded that certain communications containing a reference to a targeted selector are reasonably likely to contain foreign intelligence information, including communications between non-target accounts that contain the name of the targeted facility in the body of the message. See Docket No. 07-449, May 31, 2007 Primary Order at 12 (finding probable cause to believe that certain "about" communications were "themselves being sent and/or received by one of the targeted foreign powers"). Insofar as the discrete, wholly domestic "about" communications at issue here are communications between non-target accounts that contain the name of the targeted facility, the same conclusion applies to them. Accordingly, in the language of FISA's definition of minimization procedures, the acquisition of wholly domestic communications about targeted selectors will generally be "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. 1801(h)(1). Nevertheless, the Court understands that in the event NSA identifies a discrete, wholly domestic "about" communication in its databases, the communication will be destroyed upon recognition. See NSA Minimization Procedures § 5.

accepts the government's assertion that the collection of MCTs yields valuable foreign intelligence information that by its nature cannot be acquired except through upstream collection. See Sept. 7, 2011 Hearing Tr. at 69-70, 74. For purposes of this discussion, the Court further accepts the government's assertion that it is not feasible for NSA to avoid the collection of MCTs as part of its upstream collection or to limit its collection only to the specific portion or portions of each transaction that contains the targeted selector. See id. at 48-50; June 1 Submission at 27.[54] The Court therefore concludes that NSA's minimization procedures are, given the current state of NSA's technical capability, reasonably designed to minimize the acquisition of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.



In any event, it is incumbent upon NSA to continue working to enhance its capability to limit acquisitions only to targeted communications.

ii. Retention

The principal problem with the government's proposed handling of MCTs relates to what will occur, and what will not occur, following acquisition. As noted above, the NSA minimization procedures generally require that, "[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime," see NSA Minimization Procedures § 3(b)(4), so that it can be promptly afforded the appropriate treatment under the procedures. The measures proposed by the government for MCTs, however, largely dispense with the requirement of prompt disposition upon initial review by an analyst. Rather than attempting to identify and segregate information "not relevant to the authorized purpose of the acquisition" or to destroy such information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information, including information of or concerning United States persons with no direct connection to any target. See id. § 3(b)(1).

The proposed measures focus almost exclusively on the discrete communications within MCTs that analysts decide, after review, that they wish to use. See Aug. 30 Submission at 8-10. An analyst is not obligated to do anything with other portions of the MCT, including any wholly domestic discrete communications that are not immediately recognized as such, and communications of or concerning United States persons that have no direct connection to the targeted selector. See id.; Sept. 7, 2011 Hearing Tr. at 61. If, after reviewing the contents of an

entire MCT, the analyst decides that he or she does not wish to use any discrete communication contained therein, the analyst is not obligated to do anything unless it is immediately apparent to him or her that the MCT contains a wholly domestic communication (in which case the entire MCT is deleted).[55] See Aug. 30 Submission at 8-10.

Except in the case of those recognized as containing at least one wholly domestic communication, MCTs that have been reviewed by analysts remain available to other analysts in NSA's repositories without any marking to identify them as MCTs. See id.; Sept. 7, 2011 Hearing Tr. at 61. Nor will MCTs be marked to identify them as containing discrete communications to or from United States persons but not to or from a targeted selector, or to indicate that they contain United States person information. See Aug. 30 Submission at 8-10; Sept. 7, 2011 Hearing Tr. at 61. All MCTs except those identified as containing one or more wholly domestic communications will be retained for a minimum of five years. The net effect is that thousands of wholly domestic communications (those that are never reviewed and those that are not recognized by analysts as being wholly domestic), and thousands of other discrete

[55] The government's submissions make clear that, in many cases, it will be difficult for analysts to determine whether a discrete communication contained within an MCT is a wholly domestic communication. NSA's recent manual review of a six-month representative sample of its upstream collection demonstrates how challenging it can be for NSA to recognize wholly domestic communications, even when the agency's full attention and effort are directed at the task. See generally Aug. 16 and Aug. 30 Submissions. It is doubtful that analysts whose attention and effort are focused on identifying and analyzing foreign intelligence information will be any more successful in identifying wholly domestic communications. Indeed, each year the government notifies the Court of numerous compliance incidents involving good-faith mistakes and omissions by NSA personnel who work with the Section 702 collection.

communications that are not to or from a targeted selector but that are to, from, or concerning a United States person, will be retained by NSA for at least five years, despite the fact that they have no direct connection to a targeted selector and, therefore, are unlikely to contain foreign intelligence information.

It appears that NSA could do substantially more to minimize the retention of information concerning United States persons that is unrelated to the foreign intelligence purpose of its upstream collection. The government has not, for instance, demonstrated why it would not be feasible to limit access to upstream acquisitions to a smaller group of specially-trained analysts who could develop expertise in identifying and scrutinizing MCTs for wholly domestic communications and other discrete communications of or concerning United States persons. Alternatively, it is unclear why an analyst working within the framework proposed by the government should not be required, after identifying an MCT, to apply Section 3(b)(4) of the NSA minimization procedures to each discrete communication within the transaction. As noted above, Section 3(b)(4) states that "[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime." NSA Minimization Procedures § 3(b)(4). If the MCT contains information "of" or "concerning" a United States person within the meaning of Sections (2)(b) and (2)(c) of the NSA minimization procedures, it is unclear why the analyst should not be required to mark it to identify it as such. At a minimum, it seems that the entire MCT could be marked as an MCT. Such markings would

alert other NSA personnel who might encounter the MCT to take care in reviewing it, thus reducing the risk of error that seems to be inherent in the measures proposed by the government, which are applied by each analyst, acting alone and without the benefit of his or her colleagues' prior efforts.[56] Another potentially helpful step might be to adopt a shorter retention period for MCTs and unreviewed upstream communications so that such information "ages off" and is deleted from NSA's repositories in less than five years.

This discussion is not intended to provide a checklist of changes that, if made, would necessarily bring NSA's minimization procedures into compliance with the statute. Indeed, it may be that some of these measures are impracticable, and it may be that there are other plausible (perhaps even better) steps that could be taken that are not mentioned here. But by not fully exploring such options, the government has failed to demonstrate that it has struck a reasonable balance between its foreign intelligence needs and the requirement that information concerning United States persons be protected. Under the circumstances, the Court is unable to find that, as applied to MCTs in the manner proposed by the government, NSA's minimization procedures are "reasonably designed in light of the purpose and technique of the particular surveillance to minimize the . . . retention . . . of nonpublicly available information concerning unconsenting

---

[56] The government recently acknowledged that "it's pretty clear that it would be better" if NSA used such markings but that "[t]he feasibility of doing that [had not yet been] assessed." Sept. 7, 2011 Hearing Tr. at 56.

United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[57] See 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A).

iii. Dissemination

The Court next turns to dissemination. At the outset, it must be noted that FISA imposes a stricter standard for dissemination than for acquisition or retention. While the statute requires procedures that are reasonably designed to "minimize" the acquisition and retention of information concerning United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information, the procedures must be reasonably designed to "prohibit" the dissemination of information concerning United States persons consistent with that need. See 50 U.S.C. § 1801(h)(1) (emphasis added).

---

[57] NSA's minimization procedures contain two provisions that state, in part, that "[t]he communications that may be retained [by NSA] include electronic communications acquired because of limitations [redacted]. The government further represented that it "ha[d] not seen" such a circumstance in collection under the Protect America Act ("PAA"), which was the predecessor to Section 702. Id. at 29, 30. And although NSA apparently was acquiring Internet transactions under the PAA, the government made no mention of such acquisitions in connection with these provisions of the minimization procedures (or otherwise). See id. at 27-31. Accordingly, the Court does not read this language as purporting to justify the procedures proposed by the government for MCTs. In any event, such a reading would, for the reasons stated, be inconsistent with the statutory requirements for minimization.

As the Court understands it, no United States-person-identifying information contained in any MCT will be disseminated except in accordance with the general requirements of NSA's minimization procedures for "foreign communications" "of or concerning United States persons" that are discussed above. Specifically, "[a] report based on communications of or concerning a United States person may be disseminated" only "if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person." NSA Minimization Procedures § 6(b). A report including the identity of the United States person may be provided to a "recipient requiring the identity of such person for the performance of official duties," but only if at least one of eight requirements is also met – for instance, if "the identity of the United States person is necessary to understand foreign intelligence information or assess its importance." Id.[58]

This limitation on the dissemination of United States-person-identifying information is helpful. But the pertinent portion of FISA's definition of minimization procedures applies not merely to information that identifies United States persons, but more broadly to the dissemination of "information concerning unconsenting United States persons." 50 U.S.C. § 1801(h)(1) (emphasis added).[59] The government has proposed several additional restrictions that

---

[58] Although Section 6(b) uses the term "report," the Court understands it to apply to the dissemination of United States-person-identifying information in any form.

[59] Another provision of the definition of minimization procedures bars the dissemination of information (other than certain forms of foreign intelligence information) "in a manner that

(continued...)

will have the effect of limiting the dissemination of "nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to disseminate foreign intelligence information." Id. First, as noted above, the government will destroy MCTs that are recognized by analysts as containing one or more discrete wholly domestic communications. Second, the government has asserted that NSA will not use any discrete communication within an MCT that is determined to be to or from a United States person but not to, from, or about a targeted selector, except when necessary to protect against an immediate threat to human life. See Aug. 30 Submission at 9. The Court understands this to mean, among other things, that no information from such a communication will be disseminated in any form unless NSA determines it is necessary to serve this specific purpose. Third, the government has represented that whenever it is unable to confirm that at least one party to a discrete communication contained in an MCT is located outside the United States, it will not use any information contained in the discrete communication. See Sept. 7, 2011 Hearing Tr. at 52. The Court understands this limitation to mean that no information from such a discrete communication will be disseminated by NSA in any form.

Communications as to which a United States person or a person inside the United States

---

[59](...continued)
identifies any United States person," except when the person's identity is necessary to understand foreign intelligence information or to assess its importance. See 50 U.S.C. §§ 1801(h)(2), 1821(4)(b). Congress's use of the distinct modifying terms "concerning" and "identifying" in two adjacent and closely-related provisions was presumably intended to have meaning. See, e.g., Russello v. United States, 464 U.S. 16, 23 (1983).

is a party are more likely than other communications to contain information concerning United States persons. And when such a communication is neither to, from, nor about a targeted facility, it is highly unlikely that the "need of the United States to disseminate foreign intelligence information" would be served by the dissemination of United States-person information contained therein. Hence, taken together, these measures will tend to prohibit the dissemination of information concerning unconsenting United States persons when there is no foreign-intelligence need to do so.[60] Of course, the risk remains that information concerning United States persons will not be recognized by NSA despite the good-faith application of the measures it proposes. But the Court cannot say that the risk is so great that it undermines the reasonableness of the measures proposed by NSA with respect to the dissemination of information concerning United States persons.[61] Accordingly, the Court concludes that NSA's

---

[60] Another measure that, on balance, is likely to mitigate somewhat the risk that information concerning United States persons will be disseminated in the absence of a foreign-intelligence need is the recently-proposed prohibition on running queries of the Section 702 upstream collection using United States-person identifiers. See Aug. 30 Submission at 10-11. To be sure, any query, including a query based on non-United States-person information, could yield United States-person information. Nevertheless, it stands to reason that queries based on information concerning United States persons are at least somewhat more likely than other queries to yield United States-person information. Insofar as information concerning United States persons is not made available to analysts, it cannot be disseminated. Of course, this querying restriction does not address the retention problem that is discussed above.

[61] In reaching this conclusion regarding the risk that information concerning United States persons might be mistakenly disseminated, the Court is mindful that by taking additional steps to minimize the retention of such information, NSA would also be reducing the likelihood that it might be disseminated when the government has no foreign intelligence need to do so.

minimization procedures are reasonably designed to "prohibit the dissemination[] of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to . . . disseminate foreign intelligence information." See 50 U.S.C. § 1801(h)(1).[62]

4. NSA'S Targeting and Minimization Procedures Do Not, as Applied to Upstream Collection that Includes MCTs, Satisfy the Requirements of the Fourth Amendment

The final question for the Court is whether the targeting and minimization procedures are, as applied to upstream collection that includes MCTs, consistent with the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A)-(B). The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Court has assumed in the prior Section 702 Dockets that at least in some circumstances, account holders have a reasonable expectation of privacy in electronic communications, and hence that the acquisition of such communications can result in a "search" or "seizure" within the meaning of the Fourth Amendment. See, e.g., Docket No. [redacted]. The government accepts the proposition that the acquisition of

[62] The Court further concludes that the NSA minimization procedures, as the government proposes to apply them to MCTs, satisfy the requirements of 50 U.S.C. §§ 1801(h)(2)-(3) and 1821(4)(B)-(C). See supra, note 59 (discussing 50 U.S.C. §§ 1801(h)(2) & 1821(4)(B)). The requirements of 50 U.S.C. §§ 1801(h)(4) and 1821(4)(D) are inapplicable here.

electronic communications can result in a "search" or "seizure" under the Fourth Amendment. See Sept. 7, 2011 Hearing Tr. at 66. Indeed, the government has acknowledged in prior Section 702 matters that the acquisition of communications from facilities used by United States persons located outside the United States "must be in conformity with the Fourth Amendment." Docket Nos. [redacted]. The same is true of the acquisition of communications from facilities used by United States persons and others within the United States. See United States v. Verdugo-Urquidez, 494 U.S. 259, 271 (1990) (recognizing that "aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country").

a. The Warrant Requirement

The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the "foreign intelligence exception" to the warrant requirement of the Fourth Amendment. See Docket No. [redacted]. The government's recent revelations regarding NSA's acquisition of MCTs do not alter that conclusion. To be sure, the Court now understands that, as a result of the transactional nature of the upstream collection, NSA acquires a substantially larger number of communications of or concerning United States persons and persons inside the United States than previously understood. Nevertheless, the collection as a whole is still directed at [redacted] conducted for the purpose of national security – a

purpose going "'well beyond any garden-variety law enforcement objective.'" See id. (quoting In re Directives, Docket No. 08-01, Opinion at 16 (FISA Ct. Rev. Aug. 22, 2008) (hereinafter "In re Directives")).[63] Further, it remains true that the collection is undertaken in circumstances in which there is a "'high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake.'" Id. at 36 (quoting In re Directives at 18). Accordingly, the government's revelation that NSA acquires MCTs as part of its Section 702 upstream collection does not disturb the Court's prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA's targeting and minimization procedures.

b. Reasonableness

The question therefore becomes whether, taking into account NSA's acquisition and proposed handling of MCTs, the agency's targeting and minimization procedures are reasonable under the Fourth Amendment. As the Foreign Intelligence Surveillance Court of Review ("Court of Review") has explained, a court assessing reasonableness in this context must consider "the nature of the government intrusion and how the government intrusion is implemented. The more important the government's interest, the greater the intrusion that may be constitutionally

[63] A redacted, de-classified version of the opinion in In re Directives is published at 551 F.3d 1004. The citations herein are to the unredacted, classified version of the opinion.

tolerated." In re Directives at 19-20 (citations omitted), quoted in Docket No [redacted]. The court must therefore

> balance the interests at stake. If the protections that are in place for individual privacy interests are sufficient in light of the government interest at stake, the constitutional scales will tilt in favor of upholding the government's actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Id. at 20 (citations omitted), quoted in Docket No [redacted]. In conducting this balancing, the Court must consider the "totality of the circumstances." Id. at 19. Given the all-encompassing nature of Fourth Amendment reasonableness review, the targeting and minimization procedures are most appropriately considered collectively. See Docket No. [redacted] (following the same approach).[64]

The Court has previously recognized that the government's national security interest in conducting acquisitions pursuant to Section 702 "'is of the highest order of magnitude.'" Docket No. [redacted] (quoting In re Directives at 20). The Court has further accepted the government's representations that NSA's upstream collection is "'uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information.'" Docket No. [redacted] (quoting

[64] Reasonableness review under the Fourth Amendment is broader than the statutory assessment previously addressed, which is necessarily limited by the terms of the pertinent provisions of FISA.

government filing). There is no reason to believe that the collection of MCTs results in the acquisition of less foreign intelligence information than the Court previously understood.

Nevertheless, it must be noted that NSA's upstream collection makes up only a very small fraction of the agency's total collection pursuant to Section 702. As explained above, the collection of telephone communications under Section 702 is not implicated at all by the government's recent disclosures regarding NSA's acquisition of MCTs. Nor do those disclosures affect NSA's collection of Internet communications directly from Internet service providers [redacted], which accounts for approximately 91% of the Internet communications acquired by NSA each year under Section 702. See Aug. 16 Submission at Appendix A. And the government recently advised that NSA now has the capability, at the time of acquisition, to identify approximately 40% of its upstream collection as constituting discrete communications (non-MCTs) that are to, from, or about a targeted selector. See id. at 1 n.2. Accordingly, only approximately 5.4% (40% of 9%) of NSA's aggregate collection of Internet communications (and an even smaller portion of the total collection) under Section 702 is at issue here. The national security interest at stake must be assessed bearing these numbers in mind.

The government's recent disclosures regarding the acquisition of MCTs most directly affect the privacy side of the Fourth Amendment balance. The Court's prior approvals of the targeting and minimization procedures rested on its conclusion that the procedures "reasonably confine acquisitions to targets who are non-U.S. persons outside the United States," who thus

"are not protected by the Fourth Amendment." Docket No [redacted] The Court's approvals also rested upon the understanding that acquisitions under the procedures "will intrude on interests protected by the Fourth Amendment only to the extent that (1) despite the operation of the targeting procedures, U.S. persons, or persons actually in the United States, are mistakenly targeted; or (2) U.S. persons, or persons located in the United States, are parties to communications to or from tasked selectors (or, in certain circumstances, communications that contain a reference to a tasked selector)." Id. at 38. But NSA's acquisition of MCTs substantially broadens the circumstances in which Fourth Amendment-protected interests are intruded upon by NSA's Section 702 collection. Until now, the Court has not considered these acquisitions in its Fourth Amendment analysis.

Both in terms of its size and its nature, the intrusion resulting from NSA's acquisition of MCTs is substantial. The Court now understands that each year, NSA's upstream collection likely results in the acquisition of roughly two to ten thousand discrete wholly domestic communications that are neither to, from, nor about a targeted selector, as well as tens of thousands of other communications that are to or from a United States person or a person in the United States but that are neither to, from, nor about a targeted selector.[65] In arguing that NSA's

[65] As discussed earlier, NSA also likely acquires tens of thousands of discrete, wholly domestic communications that are "about" a targeted facility. Because these communications are reasonably likely to contain foreign intelligence information and thus, generally speaking, serve the government's foreign intelligence needs, they do not present the same Fourth Amendment concerns as the non-target communications discussed here. See supra, note 53.

targeting and minimization procedures satisfy the Fourth Amendment notwithstanding the acquisition of MCTs, the government stresses that the number of protected communications acquired is relatively small in comparison to the total number of Internet communications obtained by NSA through its upstream collection. That is true enough, given the enormous volume of Internet transactions acquired by NSA through its upstream collection (approximately 26.5 million annually). But the number is small only in that relative sense. The Court recognizes that the ratio of non-target, Fourth Amendment-protected communications to the total number of communications must be considered in the Fourth Amendment balancing. But in conducting a review under the Constitution that requires consideration of the totality of the circumstances, see In re Directives at 19, the Court must also take into account the absolute number of non-target, protected communications that are acquired. In absolute terms, tens of thousands of non-target, protected communications annually is a very large number.

The nature of the intrusion at issue is also an important consideration in the Fourth Amendment balancing. See, e.g., Board of Educ. v. Earls, 536 U.S. 822, 832 (2002); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 659 (1995). At issue here are the personal [redacted] communications of U.S. persons and persons in the United States. A person's "papers" are among the four items that are specifically listed in the Fourth Amendment as subject to protection against unreasonable search and seizure. Whether they are transmitted by letter,

telephone or e-mail, a person's private communications are akin to personal papers. Indeed, the Supreme Court has held that the parties to telephone communications and the senders and recipients of written communications generally have a reasonable expectation of privacy in the contents of those communications. See Katz, 389 U.S. at 352; United States v. United States Dist. Ct. (Keith), 407 U.S. 297, 313 (1972); United States v. Jacobsen, 466 U.S. 109, 114 (1984). The intrusion resulting from the interception of the contents of electronic communications is, generally speaking, no less substantial.[66]

The government stresses that the non-target communications of concern here (discrete wholly domestic communications and other discrete communications to or from a United States person or a person in the United States that are neither to, from, nor about a targeted selector) are acquired incidentally rather than purposefully. See June 28 Submission at 13-14. Insofar as NSA acquires entire MCTs because it lacks the technical means to limit collection only to the discrete portion or portions of each MCT that contain a reference to the targeted selector, the Court is satisfied that is the case. But as the government correctly recognizes, the acquisition of non-target information is not necessarily reasonable under the Fourth Amendment simply

[66] Of course, not every interception by the government of a personal communication results in a "search" or "seizure" within the meaning of the Fourth Amendment. Whether a particular intrusion constitutes a search or seizure depends on the specific facts and circumstances involved.

because its collection is incidental to the purpose of the search or surveillance. See id. at 14. There surely are circumstances in which incidental intrusions can be so substantial as to render a search or seizure unreasonable. To use an extreme example, if the only way for the government to obtain communications to or from a particular targeted [redacted] required also acquiring all communications to or from every other [redacted], such collection would certainly raise very serious Fourth Amendment concerns.

Here, the quantity and nature of the information that is "incidentally" collected distinguishes this matter from the prior instances in which this Court and the Court of Review have considered incidental acquisitions. As explained above, the quantity of incidentally-acquired, non-target, protected communications being acquired by NSA through its upstream collection is, in absolute terms, very large, and the resulting intrusion is, in each instance, likewise very substantial. And with regard to the nature of the acquisition, the government acknowledged in a prior Section 702 docket that the term "incidental interception" is "most commonly understood to refer to an intercepted communication between a target using a facility subject to surveillance and a third party using a facility not subject to surveillance." Docket Nos. [redacted] This is the sort of acquisition that the Court of Review was addressing in In re Directives when it stated that "incidental collections occurring as a result of constitutionally permissible acquisitions do not

render those acquisitions unlawful." In re Directives at 30. But here, by contrast, the incidental acquisitions of concern are not direct communications between a non-target third party and the user of the targeted facility. Nor are they the communications of non-targets that refer directly to a targeted selector. Rather, the communications of concern here are acquired simply because they appear somewhere in the same transaction as a separate communication that is to, from, or about the targeted facility.[67]

The distinction is significant and impacts the Fourth Amendment balancing. A discrete communication as to which the user of the targeted facility is a party or in which the targeted

---

[67] The Court of Review plainly limited its holding regarding incidental collection to the facts before it. See In re Directives at 30 ("On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.") (emphasis added). The dispute in In re Directives involved the acquisition by NSA of discrete to/from communications from an Internet Service Provider, not NSA's upstream collection of Internet transactions. Accordingly, the Court of Review had no occasion to consider NSA's acquisition of MCTs (or even "about" communications, for that matter). Furthermore, the Court of Review noted that "[t]he government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary." Id. Here, however, the government proposes measures that will allow NSA to retain non-target United States person information in its databases for at least five years.

The Title III cases cited by the government (see June 28 Submission at 14-15) are likewise distinguishable. Abraham v. County of Greenville, 237 F.3d 386, 391 (4th Cir. 2001), did not involve incidental overhears at all. The others involved allegedly non-pertinent communications to or from the facilities for which wiretap authorization had been granted, rather than communications to or from non-targeted facilities. See Scott v. United States, 436 U.S. 128, 130-31 (1978), United States v. McKinnon, 721 F.2d 19, 23 (1st Cir. 1983), and United States v. Doolittle, 507 F.2d 1368, 1371, aff'd en banc, 518 F.2d 500 (5th Cir. 1975).

facility is mentioned is much more likely to contain foreign intelligence information than is a separate communication that is acquired simply because it happens to be within the same transaction as a communication involving a targeted facility. Hence, the national security need for acquiring, retaining, and disseminating the former category of communications is greater than the justification for acquiring, retaining, and disseminating the latter form of communication.

The Court of Review and this Court have recognized that the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information. See In re Directives at 29-30; Docket No. [redacted] As explained in the discussion of NSA's minimization procedures above, the measures proposed by NSA for handling MCTs tend to maximize, rather than minimize, the retention of non-target information, including information of or concerning United States persons. Instead of requiring the prompt review and proper disposition of non-target information (to the extent it is feasible to do so), NSA's proposed measures focus almost exclusively on those portions of an MCT that an analyst decides, after review, that he or she wishes to use. An analyst is not required to determine whether other portions of the MCT constitute discrete communications to or from a United States person or a person in the United States, or contain information concerning a United States person or person inside the United States, or, having made such a determination, to do anything about it. Only

those MCTs that are immediately recognized as containing a wholly domestic discrete communication are purged, while other MCTs remain in NSA's repositories for five or more years, without being marked as MCTs. Nor, if an MCT contains a discrete communication of, or other information concerning, a United States person or person in the United States, is the MCT marked as such. Accordingly, each analyst who retrieves an MCT and wishes to use a portion thereof is left to apply the proposed minimization measures alone, from beginning to end, and without the benefit of his colleagues' prior review and analysis. Given the limited review of MCTs that is required, and the difficulty of the task of identifying protected information within an MCT, the government's proposed measures seem to enhance, rather than reduce, the risk of error, overretention, and dissemination of non-target information, including information protected by the Fourth Amendment.

In sum, NSA's collection of MCTs results in the acquisition of a very large number of Fourth Amendment-protected communications that have no direct connection to any targeted facility and thus do not serve the national security needs underlying the Section 702 collection as a whole. Rather than attempting to identify and segregate the non-target, Fourth-Amendment protected information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information and hence to enhance the risk that it will be used and disseminated. Under the totality of the circumstances, then, the Court is unable to find that

the government's proposed application of NSA's targeting and minimization procedures to MCTs is consistent with the requirements of the Fourth Amendment. The Court does not foreclose the possibility that the government might 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.[68]

V. CONCLUSION

For the foregoing reasons, the government's requests for approval of the certifications and procedures contained in the April 2011 Submissions are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the "upstream collection" of Internet transactions containing multiple communications, or MCTs – is, in some respects, deficient on statutory and constitutional grounds. Specifically, the Court finds as follows:

1. Certifications [redacted] and the amendments to the Certifications in the Prior 702 Dockets, contain all the required elements;

---

[68] As the government notes, see June 1 Submission at 18-19, the Supreme Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." City of Ontario v. Quon, — U.S. —, 130 S. Ct. 2619, 2632 (2010) (citations and internal quotation marks omitted). The foregoing discussion should not be understood to suggest otherwise. Rather, the Court holds only that the means actually chosen by the government to accomplish its Section 702 upstream collection are, with respect to MCTs, excessively intrusive in light of the purpose of the collection as a whole.

2. As applied to telephone communications and discrete Internet communications that are to or from a facility tasked for collection, to non-MCT "about" communications falling within the [redacted] categories previously described by the government,[69] and to MCTs as to which the "active user" is known to be a tasked selector, the targeting and minimization procedures adopted in accordance with 50 U.S.C. § 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States;

3. NSA's targeting procedures, as the government proposes to implement them in connection with the acquisition of MCTs, meet the requirements of 50 U.S.C. § 1881a(d);

4. NSA's minimization procedures, as the government proposes to apply them to MCTs as to which the "active user" is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention; and

5. NSA's targeting and minimization procedures, as the government proposes to apply them to MCTs as to which the "active user" is not known to be a tasked selector, are inconsistent with the requirements of the Fourth Amendment.

---

[69] See Docket No. [redacted].

Orders approving the certifications and amendments in part are being entered contemporaneously herewith.

ENTERED this 3rd day of October, 2011.

JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

[redacted], Deputy Clerk, FISC, certify that this document is a true and correct copy of the original. [redacted]

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix Q

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Public Hearing Regarding the
Surveillance Program Operated Pursuant to
Section 702 of the Foreign Intelligence
Surveillance Act

March 19, 2014

The public hearing was held at the Renaissance Mayflower Hotel, 1127 Connecticut Avenue NW, Washington, D.C. 20036 commencing at 9:00 a.m.

Reported by: Lynne Livingston

BOARD MEMBERS

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

PANEL I

Government Perspective on Section 702 Foreign Intelligence Surveillance Act

James A. Baker, General Counsel, Federal Bureau of Investigations
Rajesh De, General Counsel, National Security Agency
Robert Litt, General Counsel, Office of the Director of National Intelligence
Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, Department of Justice

PANEL II

Legal Issues with 702

Foreign Intelligence Surveillance Act

Laura Donohue, Professor of Law, Georgetown University Law School

Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union

Julian Ku, Professor of Law, Hofstra University

Rachel Levinson-Waldman, Counsel, Liberty and National Security Program, Brennan Center for Justice

PANEL III

Transnational and Policy Issues

John Bellinger, Partner, Arnold and Porter

Dean C. Garfield, President and CEO, Information Technology Industry Council

Laura Pitter, Senior National Security Researcher, Human Rights Watch

Ulrich Sieber, Director, Max Planck Institute for Foreign and International Criminal Law, Germany

Christopher Wolf, Partner, Hogan Lovells

PROCEEDINGS

MR. MEDINE: Good morning. Welcome to the Privacy and Civil Liberties Oversight Board's hearing on the 702 Program.

I'm David Medine, PCLOB's chairman. It's 9:05 a.m. on March 19th, 2014 and we are in the grand ballroom of the Mayflower Hotel located at 1127 Connecticut Avenue, NW, Washington, D.C.

This hearing was announced in the Federal Register on March 10th, 2014. As chairman, I will be the presiding officer.

All five Board members are present and there is a quorum. The Board members are Rachel Brand, Elisebeth Collins Cook, James Dempsey, and Patricia Wald.

I will now call the hearing to order. All in favor of opening the hearing please say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous consent to proceed, we will now proceed.

I want to thank the many panelists who

will be participating in today's hearing for agreeing to share their views with the Board.

I also wanted to thank the Board's staff, Sharon Bradford Franklin, Sue Reingold, Peter Winn, Diane Janosek, Brian Frazelle, and Simone Awang for their efforts in making this event possible.

Last year PCLOB agreed to provide the President and Congress a public report on two federal counterterrorism programs, the Section 215 program under the USA PATRIOT Act and the 702 program under the FISA Amendments Act. The report on the 215 program was issued on January 23rd, 2014.

Our focus today will be on the Section 702 program under the FISA Amendments Act. The purpose of this hearing is to foster a public discussion of legal, constitutional, and policy issues relating to this program.

A few ground rules for today, we expect that the discussion will be based on unclassified or declassified information, however some of the

discussion will inevitably touch on leaked classified documents or media reports of classified information.

In order to promote a robust discussion speakers may choose to reference these documents or information, but they should keep in mind that in some cases they remain classified. Therefore, while discussing them, neither the Board members nor speakers in a position to do so will confirm the validity of the documents or information.

There will be three panels today. The first will consist of government officials whose agencies have varying degrees of responsibility for the surveillance programs that will be the subject of our report.

The second panel with consist of academics and advocates who will focus on legal issues, including statutory and constitutional issues. After the first two panels we will be taking a lunch break.

The final panel will consist of a mix of academics, advocates, and private sector

representatives and will focus on transnational and policy issues.

Board members will each pose questions during each panel with questions in rounds for each Board member. Panelists are urged to keep their responses brief and to permit the greatest exchange of views.

The program is being recorded and a transcript will be posted on PCLOB.gov. Written comments from members of the public are welcome and may be submitted online at regulations.gov or by mail until March 28th.

Today's hearing will focus on the government's collection of foreign intelligence information from electronic communication service providers under court supervision pursuant to Section 702 of the Foreign Intelligence Surveillance Act.

Information is obtained with FISA court approval based on written directives from the Attorney General and the Director of National Intelligence to acquire foreign intelligence

information. This law permits the government to target non-U.S. persons, someone who is not a citizen or a permanent resident alien, located outside the United States for foreign intelligence purposes without obtaining a specific warrant for each target.

We will now turn to our first panel, and I understand that Bob Litt will be making an opening statement for the panel.

MR. LITT: Thank you, and thank you for the opportunity to appear on behalf of the whole group here and talk about Section 702.

I would like to give a brief overview of Section 702 to set the stage, and we'll be glad to fill out some of the points I make here in response to questions.

Section 702, as you noted, enables us to collect intelligence against foreign targets who are outside of the United States while robustly protecting privacy rights.

Under Section 702 the FISA court approves annual certifications submitted by the

Attorney General and the Director of National Intelligence that identify categories of foreign intelligence that may be collected. We then target selectors such as telephone numbers or email addresses that will produce foreign intelligence falling within the scope of the certifications.

The FISA court also has to review and approve targeting and minimization procedures. The targeting procedures ensure that we target only non-U.S. persons who are reasonably believed to be outside of the United States, that we do not intentionally intercept totally domestic communications, and that we do not target any person outside of the United States as a subterfuge to actually target someone inside the U.S.

The minimization procedures ensure that consistent with foreign intelligence needs, we minimize the acquisition and retention of non-public information available about U.S. persons and that we prohibit the dissemination of

such information.

I want to make a couple of important overview points about Section 702. First, there is either a misconception or a mischaracterization commonly repeated that Section 702 is a form of bulk collection. It is not bulk collection. It is targeted collection based on selectors such as telephone numbers or email addresses where there's reason to believe that the selector is relevant to a foreign intelligence purpose.

I just want to repeat that Section 702 is not a bulk collection program.

Second, from a legal point of view persons who are not U.S. persons and who are outside of the United States do not have rights under the Fourth Amendment and so the Constitution doesn't require individualized warrants to target them.

In fact, the type of intelligence that is covered by Section 702 targeting foreigners outside of the United States has historically been viewed as part of the President's inherent

constitutional authority and I'm not aware of any other country that brings this kind of collection under this sort of judicial process.

Third, collection under 702 is subject to extensive oversight by all three branches of government. We can explain the oversight in more detail later, but it includes extensive review of collection activities under Section 702 by inspectors general, by the Department of Justice, and the Office of the Director of National Intelligence. It includes reporting of all compliance incidents to the Foreign Intelligence Surveillance Court, and it includes periodic reports both to Congress and to the court.

As the documents that we've declassified and released make clear, the Foreign Intelligence Surveillance Court carefully scrutinizes our activities under this section. And while there have been a number of compliance incidents over the years, the court has never found any intentional efforts to violate the requirements of Section 702.

Fourth, the fact that the communications of U.S. persons may be incidentally intercepted when we target valid foreign intelligence targets is neither unexpected nor unique to Section 702 collection.

Both the statute itself with its required minimization procedures and the legislative history make completely clear that Congress knew full well when it passed Section 702 that incidental collection of communications of U.S. persons would occur when they're in communication with valid foreign targets.

And it's important to note that this kind of incidental collection occurs all the time in other contexts. When we conduct a criminal wiretap or a wiretap pursuant to Title I of FISA we will likely intercept communications of persons who are not targets. When we seize someone's computer we may find communications with persons who are not targets.

The minimization rules under Section 702 which the FISA court approves is consistent

with both the statute and the Fourth Amendment are designed to protect the privacy of persons whose communications are incidentally collected, while still allowing the use of information that is lawfully collected for valid foreign intelligence and law enforcement purposes.

Finally, I want to close by just emphasizing that Section 702 is one of the most valuable collection tools that we have. Many of the specific achievements of Section 702 have to remain classified so that we aren't revealing exactly who we're targeting and what we're collecting. But it is one of our most important sources of information, not only about terrorism but about a wide variety of other threats to our nation.

And unless one of my colleagues has something to add, I think we're ready to address your questions.

MR. MEDINE: Great, thank you very much for that statement.

I wanted to start off and pick up with

your discussion of incidental collection, and again just to make clear that under this program, even though the target may be a non-U.S. person there will be times when the conversations, either by email or telephone, the person on the other end will be a U.S. person.

And so my question to the panel is whether because you're gathering communications of U.S. persons if that implicates Fourth Amendment concerns? And if so, do you believe there's a foreign intelligence exception to the Fourth Amendment? And if not, how is warrantless collection of information of U.S. persons permissible?

And then to follow up on Mr. Litt's comment analogizing this to a traditional wiretap, is there a distinction here where on a traditional wiretap the court has, there's been a judicial determination with particularity of a particular collection, whereas here there's only broad programmatic court approval and not approval of the specific collection?

So I guess broadly speaking, can you address the Fourth Amendment concerns regarding incidental collection?

MR. WIEGMANN: Sure, I'll take that. So this is, as Bob said, collection that is targeting non-U.S. persons overseas who don't enjoy Fourth Amendment rights under controlling Supreme Court precedent. So that affects the Fourth Amendment analysis.

That's not to say that U.S. persons whose information is or whose communications are collected incidentally doesn't trigger a Fourth Amendment review. It does. Those people still have Fourth Amendment rights, but what the courts have said is that, what the FISA court has said is that the minimization procedures that are in place render that collection reasonable from a Fourth Amendment perspective.

We think there's an exception to the warrant requirement. Before FISA was enacted in the 1970s a number of courts held in a number of different circuits that there is a foreign

intelligence exception to the warrant requirement under the Fourth Amendment, in light of the special needs of the government to collect foreign intelligence, weighed against the privacy interests of U.S. persons concluded that you don't need a warrant when you're engaged in foreign intelligence collection.

So then the only remaining question is, is it reasonable under the Fourth Amendment to collect information on U.S. persons incidentally when you're targeting non-U.S. persons. And what the FISA court has held is that it is reasonable in light of the minimization targeting procedures that we have in place. So I don't know if that answers your question, but.

So the way you look at it is the warrant requirements not applicable to foreign intelligence collection still have a reasonableness requirement with respect to incidentally collected U.S. persons, and that in fact, it is reasonable in light of the procedures that we have that are designed to ensure that we

are targeting only non-U.S. persons.

MR. MEDINE: And could you address why the minimization procedures make it a reasonable form of collection under the Fourth Amendment?

MR. WIEGMANN: Yes, so the minimization procedures address, and the targeting procedures address the acquisition, retention, and dissemination of U.S. person information.

And so those procedures all are designed to protect those U.S. persons whose information might be incidentally collected.

So for example, you can only disseminate information about a U.S. person if it is foreign intelligence, or necessary to understand foreign intelligence, or is evidence of a crime.

You have retention rules. I believe in some cases, for NSA for example, you have a five year retention limit on how long the information can be retained. And so these are procedures that the courts have found protect U.S. privacy and make the collection reasonable for Fourth

Amendment purposes.

MR. MEDINE: And under the minimization procedures I understand that the agency, the NSA, FBI, the CIA have their own minimization procedures and they're not the same with each other?

MR. WIEGMANN: That's right.

MR. MEDINE: Can you address why that shouldn't be a concern that this information is not being subjected to the same minimization standards?

MR. WIEGMANN: So each of them have their own minimization procedures based on their unique mission, and the court reviews each of those for CIA, FBI, NSA, and it's found them all reasonable for each different agency. They're slightly different based on the operational needs, but they're similar.

MR. MEDINE: Would it make more sense then if the same set of minimization procedures apply across the board for this kind of information?

MR. WIEGMANN: I don't think. Again, just to contrast, for example, FBI and NSA that are using information in different ways. The FBI has a little more latitude with respect to U.S. person information in terms of criminal activity and evidence of a crime than NSA, which doesn't have that law enforcement mission. So I think it is important to have some differences between the agencies in terms of how they handle the information.

MR. MEDINE: And is it the practice that all information that's collected under 702 is subject to the minimization procedures?

Some questions I think have been raised in some of the comments that were submitted as to whether address books or other information would be considered communications that would be subject to minimization, or is it the approach that all information collected under 702 is subject to minimization?

MR. WIEGMANN: All U.S. person information is subject to minimization procedures.

MR. MEDINE: I think my time is up.

MS. BRAND: First of all, thanks to all of you for being here this morning. We appreciate your taking the time and making yourselves available.

I want to continue on the Fourth Amendment discussion. Could one of you explain the process both inside the executive branch and then with the court of conducting the Fourth Amendment analysis and seeking the court's approval of the Fourth Amendment analysis and what kinds of opinions on the Fourth Amendment you've had from the court, to the extent that you can talk about it. Help us to understand how that works.

MR. WIEGMANN: So, you know, the FISA court operates a little bit differently than a regular court in the sense that it's ex parte, but. So that means only the government is there. There's not a party on the other side.

But other than that, we are briefing the legal issues in much the same way as we would

in a regular proceeding where there is a party on the other side. So we have an obligation to persuade the court that the collection under 702 is lawful, that it complies with the Fourth Amendment, and as I just explained to the chair, that minimization procedures comply with the Fourth Amendment.

So we would brief that issue explaining the Fourth Amendment procedures, and the court issues opinions and has issued opinions going through the Fourth Amendment analysis and finding that 702 collection, including the minimization targeting procedures meets the Fourth Amendment standards. So it's a full-up kind of regular legal briefing on that.

MR. LITT: And if I could just add something to that, it is typical in matters that involve the collection of evidence for these proceedings to be conducted ex parte. Wiretap or search warrant applications are also all done ex parte, even if they happen to present significant legal issues. So this is nothing novel in terms

of the approach that's taken there.

MR. DE: And if I could have one point. So in addition to what Brad was articulating, the court reviews this at least annually, the Fourth Amendment analysis.

As you all know, the 702 process requires annual certification. As part of that certification process every year the minimization and targeting procedures for the various agencies are submitted to the FISC, which by statute has to conduct a Fourth Amendment analysis on those procedures as part of that annual review process.

MS. BRAND: So the Fourth Amendment analysis is once a year of the program overall?

MR. DE: Well, the court has consistent jurisdiction over the program all year. The point I was making is that as part of the annual certification process, by statute the court is required to do a Fourth Amendment analysis of the annual, of the procedures that are submitted annually.

MR. BAKER: It gets evaluated at least

once a year.

MS. BRAND: Can you elaborate on that? What would there be in addition to that once a year analysis?

MR. DE: There could be a variety of factors. There could be a need to change procedures in the year, so that would prompt another analysis. I don't believe we've done that but that could be one circumstance.

There could be a variety of compliance matters that raise particular concerns to the court, in which case the court may want to do a review off-cycle.

So I think we wouldn't presume and say it only had to be once a year, but at a minimum by statute it needs to be once a year.

MS. BRAND: Okay. Bob, you talked about 702 not being bulk collection. I'd like to delve into that a little bit more, it's not bulk collection. You talked about selectors. We need to elaborate on that a little bit, I think. What is it? It's not bulk you say, but what is it?

MR. LITT: Sure. Well, I think it's probably helpful to talk about what bulk collection is first of all.

And if you look at the President's policy directive there's a definition. I don't have it in front of me, but it's essentially bulk collection is collection of communications without relying on some sort of discriminant to ensure that you're targeting particular collection.

It's sort of viewed sort of more informally, it's getting a whole bunch of communications, hanging onto them and then figuring out later what you want.

This is not that. This is a situation where we figure out what we want and we get that specifically. And so that's why it is targeted collection rather than bulk collection. Is that helpful?

MS. BRAND: But I'd like to get a little bit more into what is it that you're getting. So you have a selector, I mean.

MR. LITT: Sure. So Raj probably can

talk to this a little better than I can.

MR. DE: So if I could, I'd step back and just talk about the different types of collection under Section 702, which I think is a necessary predicate to understand how collection occurs.

So there's two types of collection under Section 702. Both are targeted, as Bob was saying, which means they are both selector-based, and I'll get into some more detail about what that means. Selectors are things like phone numbers and email addresses.

Both are affected by compulsory legal process, both types are conducted with the assistance of electronic communication service providers, and both types of collection under 702 are subject to the same statutory standards, so just as a predicate.

The first type is what's now been come to be known as PRISM collection, so just using that shorthand for a moment. And under this type of collection, communications to or from specific

selectors, again, things like phone numbers or emails, are provided with the assistance of ISPs pursuant to directives.

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.

It is also however selector-based, i.e. based on particular phone numbers or emails, things like phone numbers or emails. This is collection to, from, or about selectors, the same selectors that are used in PRISM selection. This is not collection based on key words, for example.

This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.

But given the unique nature of upstream collection there are different minimization procedures that apply, to get to the chair's question earlier.

The reason procedures aren't always the same for different types of collection, as Brad articulated, is that there are both different mission interests and different privacy interests at stake.

MS. BRAND: I see my time is up, so.

MS. COLLINS COOK: Thank you for coming here this morning. We really appreciate your time on this and happy to be a part of this dialogue here.

I wanted to follow up on a couple of points that have already been raised, but first, we've talked about the Fourth Amendment implications of the collection. We've also talked about the fact that, or it is known that the information that's collected can subsequently be queried.

Do you consider that subsequent query a search for the purposes of the Fourth Amendment? And if not, why not?

MR. WIEGMANN: No, I would say that the search occurs at the time that the collection

occurs. So when the information, as Raj just explained, from a particular selector is acquired by NSA, then that's the time at which the search occurs.

Once you've lawfully collected that information, subsequently querying that information isn't a search under the Fourth Amendment, it's information already in the government's custody. And so I don't think there are any other contexts really in general in which a warrant is required to search information already in your custody.

MS. COLLINS COOK: Following up on that, I think some have suggested that whether as a matter of Fourth Amendment necessity or as a policy, as a matter of policy that you should seek court approval before doing a query of a U.S. person identifier.

Can you talk a little bit about what the operational impact of such a requirement might be?

MR. WIEGMANN: Sure, and this is

something I guess some of my colleagues could talk about the operational impact. But as I said, in general with other types of collection, whether it's collection under Title I of FISA, which is your regular collection under which you've gone to the FISA court and already gotten approval to target a particular agent of a foreign power in the United States, or moving over to the criminal side if it's information collected under the Wiretap Act, commonly known as Title III, under which you're conducting surveillance, let's say of an organized crime figure or in a drug case of an individual, in all of these contexts we collect information.

We don't, once we've collected it, we've gotten the necessary court approvals to obtain the information, we don't then have to go back to court to query the same information that we've already collected lawfully a second time to say is it okay to look at it. We've already gotten the conclusion that it's legal to collect it.

And if you have to go back to court every time you look at the information in your custody you can imagine that that would be quite burdensome and difficult, to have to go back every time to look at information that's already in your custody. But I can let the FBI and NSA address it a little bit.

MR. DE: If I could add a couple of points and then I'll turn it to my colleague from the bureau.

Just one basic point, we've been talking about U.S. person queries and I just articulated two types of collection. Just to clarify, U.S. person queries are not allowed under what I described as upstream collection. So as I articulated, there may be different reasons to have tailored procedures, minimization procedures for different types of collections. So such queries are not allowed for upstream.

Adding to Brad's point about lawfully collected information, so once information is collected pursuant to 702, the government can and

often will review what it needs to in that information.

Querying that lawfully collected information, one way to think about that is a way to more efficiently review that which the government already has in its possession and can review all of.

And so to get to your question about policy limits on querying that data, one also needs to understand that that information is at the government's disposal to review in the first instance, and querying it is just a way to organize it.

Secondly -- thirdly, if I could add there are standards in place for querying that information, at least for NSA. Such a query, and we're talking about PRISM collection, must be reasonably likely to return foreign intelligence information.

And then finally, in order to disseminate any U.S. person information that may result from such a query it has to be necessary to

understand the foreign intelligence or evidence of a crime is apparent from our publicly available procedures.

But on the operational element, let me turn that to Jim.

MR. BAKER: So just at a high level I think let me make a couple of comments. So first I think you have to think about the fact that you're creating a new and special category of information, as Brad was saying, right. So this would be information that had already been acquired pursuant to lawful process.

We normally will query that. We'll look through that. When something comes in, we'll look through our collected materials to try to find -- a threat comes in, let's say for example. We look at our collected materials, we try to figure out what we have, and then, you know, move forward as expeditiously as possible.

So you would be creating a new category of information that sort of would be off-limits from the normal type of collection that we do.

And I don't pretend to fully understand all the implications that that would have.

But a couple that come to mind, first of all, obviously would be delay. So you would have some additional process that you would have to go through, and I'm sure there would be some kind of emergency carve out and so on, but you'd have to think about and factor in the reality that you would be introducing delay into the system.

You would also then as a result potentially create a gap. There are several types of gaps, I guess. But you would have, there would be a disinclination for people, because either they don't have the facts, or it's just too hard or whatever, to actually go and pursue that extra pot of information.

So there might be some type of connection between what we can look at normally, this material, and then other types of material. And having that type of gap might, you know, actually create a blind spot for us in terms of intelligence collection.

You'd also have to think about, I think, the technical complexity of what it is that you're suggesting. So this is going to have to be segregated in some way, treated differently. And we'd just have to think about that. That could lead to, you know, training issues, technical costs, things like that.

So it's, you just have to actually do it in a way that would be different than from other types of data that we handle, so that's sort of at a high level some of the things that come to mind.

MR. LITT: Beth, can I add one brief point to this which is that over the last decade, decade and a half, there have been a number of commissions that have been set up to investigate after a variety of terrorism incidents, 9/11, Fort Hood, the underwear bomber and so on. Consistently every one of those commissions has found that we need to eliminate barriers to making use of the information that's lawfully in our possession in order to better protect the nation.

And this, requiring some kind of additional process before we can query this information runs directly contrary to the recommendations of all those commissions.

MS. COLLINS COOK: Thank you. I see that my time is up.

MR. MEDINE: By the way, I should say in the excitement of getting into the questioning I never had actually a chance to introduce the panelists. And so I just wanted for the benefit of the audience, you're familiar to us, but for the benefit of the audience we have Jim Baker, who's the General Counsel of the FBI, Raj De, who's the General Counsel at NSA, Bob Litt is the General Counsel at the Director of National Intelligence, and Brad Wiegmann, who is the Deputy Assistant Attorney General at the National Security Division of the Justice Department.

Again, thank you all for being here.

MR. DEMPSEY: Thanks, and thanks to the witnesses for being here. They are very well-known to us. I think everybody should

realize that we've now spent many, many days with these gentlemen and with many, many of their colleagues at all their agencies going through this information, and delving deeply into this.

And there's been a huge amount of dedication of time on the part of the agencies to make sure that we have everything that we ask for and to make sure that all of our questions are answered. And so, you know, all the Board members really appreciate the amount of time that you've dedicated to talking with us.

And I think it is very important here to be one hundred percent clear, and I think there has been a lot of misunderstanding about the 702 program, and I think I do see issues with the program and things we're talking about, but I think it's very important to narrow the subjects of controversy, or discussion, or concern.

And I'm afraid that Raj may have partly reinserted a problem here when you said that U.S. person selectors were not used for upstream collection, or for upstream searches they're not

used at all, period, at the collection stage.

You were saying that U.S. person identifiers or selectors are not used to search the acquired database of communications that were otherwise acquired on a particularized basis under the upstream program, correct?

MR. DE: Correct. I definitely would prefer not to introduce more ambiguities. Let me be absolutely clear, Section 702 collection of any flavor, upstream or PRISM, is only targeting non-U.S. persons reasonably believed to be located abroad.

The topic I was discussing was, is in the realm of that lawfully collected targets information, once it's in the government's possession a secondary issue arises as to how one can search through that data. And the issue that we were discussing was whether those searches can be conducted using U.S. person identifiers within that lawfully data. And the answer to that question is no with respect to upstream collection.

MR. DEMPSEY: And here when you're talking about search and collect and acquire, all of those terms you're using to mean in a colloquial sense when the government collects, obtains, puts into its database, acquires, you're not parsing those words for 702 purposes. There's not a distinction between the search, the collection, the acquisition, right? It's all, you're using those things all that refer to the same activity.

MR. DE: There's no parsing between acquisition or collection.

So there are some theories out there that when the government receives the data it doesn't count as collection or acquisition. That is incorrect. Acquisition and collection for these purposes are the same thing.

But the term search is a different term. Search, as we were just discussing, means searching information that has already been lawfully acquired or collected.

MR. DEMPSEY: Although the first --

okay, so now we have two meanings of search. It's so hard to be clear on this. Brad was explaining a search occurs when you first collect or acquire. That is the Fourth Amendment search.

MR. DE: I think he was speaking to the use of the term in the Fourth Amendment, not the use of the term for purposes of this.

MR. DEMPSEY: And then querying, then there's a second use of search meaning query. So you query your database?

MR. DE: Correct.

MR. LITT: That's the term that we typically use rather than search in that context.

MR. DEMPSEY: Right. In that case a query is not a search for Fourth Amendment purposes.

MR. LITT: Right.

MR. DEMPSEY: Briefly talk a little bit about this 51 percent theory. So persons reasonably believed to be outside the United States, and there's been some talk about, well, so there may have been some slide somewhere, I don't

know where this came from, but some notion that, oh, if it's a 51 percent likelihood, therefore 49 percent of the time we might be wrong, that the person's not outside the United States and that's permitted under 702. Can you comment on that.

MR. DE: Sure. So I think the bigger picture question that that gets to how a determination is made for purposes of the statute that you are in fact targeting a non-U.S. person reasonably believed to be located abroad.

So as Bob articulated, and I'm sorry for repeating this but just for clarity, the statute does not allow us to target U.S. persons, it does not allow the government to target anybody within the U.S., it does not allow for reverse targeting, it does not allow for the intentional collection of wholly domestic communications.

So as to how we establish a reasonable belief that the target is in fact a non-U.S. person reasonably believed to be located abroad, there is no 51 percent rule that if you are 51 percent sure it is a non-U.S. person located

abroad that is sufficient. That is not the rule, and I don't honestly know where that misconception has come from.

The foreignness determination, which is shorthand for referring to the determination that it is a non-U.S. person reasonably located to be abroad, is based on a totality of the circumstances.

So what does that mean? That means that an analyst must take into account all available information. It means that an analyst cannot ignore any contrary information to suggest that that is not the correct status of the person. And it also means naturally that any such determination is very fact-specific to the particular facts at hand.

I did a little checking and it turns out in our internal training materials, at least at NSA, we actually ask our analysts a question along the lines of, if you have four pieces of information that suggests a person is abroad and two pieces of information that suggests a person

is domestic, given that the score is four to two is that sufficient to establish foreignness?

And the correct answer to that is, no, it is not sufficient because it is not a majority test. It is a totality of the circumstances test. One must take into account the strength, credibility, and import of all relevant information.

But just to add on to that, to your bigger point about confidence in that determination, analysts have an affirmative obligation to periodically revisit the foreignness determination. So it is not a once and done system.

Moreover, targeting determinations must be documented ex ante before any collection occurs. That documentation is reviewed, every determination is reviewed in 60 day increments by the Department of Justice and the Office of the Director of National Intelligence to determine if they agree with that determination.

And then finally, the targeting

procedures, as we mentioned, which account for a lot of this are reviewed annually by the Foreign Intelligence Surveillance Court and approved to be consistent with the Fourth Amendment and the statute obviously.

MR. WIEGMANN: And if I could just add from the DOJ perspective, as Raj said, we reviewed all of those foreignness determinations and we found an error rate of less than .1 percent basically. So that equates to essentially less than one in a thousand cases in which we're finding that NSA is making erroneous foreignness determinations.

MR. MEDINE: Judge Wald.

MS. WALD: Thank you again. I think that the NSA has said that in some of its information that if information about U.S. persons is collected incidentally to a 702 search that was targeted on a non-U.S. person and the incidental information about U.S. persons is found not to have any foreign intelligence value it will be, quote, purged.

Can you explain exactly what purging means? Does that mean that it can subsequently not be used at all, or it can be subsequently used or retained for some purposes? And finally, at what point and by whom would this decision of non-intelligence value be made? There's a lot of sub-questions.

MR. DE: Sure. Well, let me step back for a moment. If the information is determined to not have --

MS. WALD: Could you just speak a tiny bit louder because I'm at the tail-end of this table.

MR. DE: Certainly. If information is determined to not have foreign intelligence value then it is required to be purged.

What purging means is removed from NSA systems in a way that it cannot be used, period.

MS. WALD: For any reason at all?

MR. DE: Correct. There are extensive requirements we have gone through with the Foreign Intelligence Surveillance Court to ensure to the

best extent humanly possible that NSA's technical systems can, in fact, purge data as required by both our minimization procedures and the Foreign Intelligence Surveillance Court.

MS. WALD: But just to pursue that a little bit, in your experience is that to purge or not to purge decision made early in the process or is it kept in there until the analyst or whoever has a chance to do some more hunting around and see whether or not maybe other things would suggest that that does have intelligence value?

In other words, if there's such a concern about U.S., as there is in outside groups, about U.S. incidental information that's in the files and later there's a possibility of it being queried, I wonder how extensive this purging operation really is?

MR. DE: To purge or not to purge, that is the question.

MS. WALD: Yes.

MR. DE: So our procedures require that the determination about foreign intelligence value

be made as early as possible in the, what one in the technical sense calls the processing cycle. So it is not something that by default can be ignored.

That being said --

MS. WALD: And who makes that?

MR. DE: An assessment as to foreign intelligence value is made by foreign intelligence analysts.

MS. WALD: By the analysts who are working on it?

MR. DE: Correct, as they would be the ones who have the most relevant information.

But that also goes to a bigger point as to the nature of intelligence analysis. I think you all would appreciate that it's difficult to determine without context the foreign intelligence value of any particular piece of information. In fact, that's why the intelligence community is often encouraged to connect the dots of various pieces of disparate information.

And so I think we would hope and expect

that analysts make that determination about foreign intelligence value within the context of all available information.

But to your point as to if information is not reviewed, what is the default? This is a large reason why we in fact have default retention periods for data. And for example, for NSA the default for PRISM collection is a five year retention period.

But that's also a reason why that retention period is adjustable, or at least is tailored to the specific nature of the collection.

So for example, for upstream collection the retention period is two years, recognizing the nature of, the unique nature of upstream collection and that it may have a greater implication for privacy interests.

MS. WALD: Okay. The President required, I think he required in his January directive that went to 215 that at least temporarily the selectors in 215 for querying the databank of U.S. telephone calls metadata had to

be approved by the FISA court.

Why wouldn't a similar requirement for 702 be appropriate in the case where U.S. person indicators are used to search the PRISM database? I mean what big difference do you see there?

MR. LITT: Well, I think from a theoretical perspective it's the difference between a bulk collection and a targeted collection, which is that the --

MS. WALD: But I would think that, I'm sorry for interrupting, Bob. I would think that message, since 702 has actually got the content.

MR. LITT: Well, and the second point I was going to make is that I think the operational burden in the context of 702 would be far greater than in the context of 215.

If you recall the number of actual telephone numbers as to which a RAS, reasonable articulable suspicion determination was made under Section 215 was very small.

The number of times that we query the 702 database for information is considerably

larger. I suspect that the Foreign Intelligence Surveillance Court would be extremely unhappy if they were required to approve every such query.

MS. WALD: I suppose the ultimate question for us is whether or not the inconvenience to the agencies, or even the unhappiness of the FISA court would be the ultimate criteria.

MR. LITT: Well, I mean I think it's more than a question of inconvenience. I think it's a question of practicability.

MR. DE: And if I could add one point to that. I think one must also look at the underlying nature of the collection program at issue. And so I think we should be clear not to conflate the 215 program with the 702 program, and as you mentioned, one deals with metadata and one deals with content.

But the important point being the latter is directed at content collection targeting non-U.S. persons located abroad, whereas the 215 program, although it deals with metadata, did not

have such a necessary distinction.

MS. WALD: It did have a selective, I mean the 215 program and the original --

MR. MEDINE: I'm going to, your time, the Judge's time has expired, but we'll have an opportunity in another round to continue that discussion.

I want to shift to a different topic, which is about communication, about searches or about queries, which is, and I'm happy to have you explain it, but my understanding basically is that you are looking for other peoples' discussion of a particular selector or email term.

But I'd like to get back to some of the definitions here, which are there are some terms here that would be helpful to understand your view of, which is what is a target? What is a tasking? What is a selector? What's a directive?

If you could explain those terms, because I did want to shift to how those terms might apply in the about context.

MR. WIEGMANN: Okay, I can take a stab

at that. So a target is the -- maybe I should start with selector since that's the operative term that the others build on.

A selector would typically be an email account or a phone number that you are targeting. So this is the, you get, you know, terrorists at Google.com, you know, whatever. That's the address that you have information about that if you have reason to believe that that person is a terrorist and you would like to collect foreign intelligence information, I might be focusing on that person's account.

So when you go up on that selector, we say go up on or target that selector, that means we're collecting information, we're going to the provider and getting information related to that person's account.

So we're intercepting in real time and then collecting the historic communications of that particular account.

Okay, so that's what we mean by targeting a selector. You're using that selector,

you're providing that to the company, the provider, to get information on that account, or if it's a phone number on that phone number.

So that's when we say selector it's really an arcane term that people wouldn't understand, but it's really phone numbers, email addresses, things like that.

And targeting, it means that's the one you're trying to get. They may be in communication with other email addresses or other phone numbers and so forth. Those are not the targeted numbers or accounts, those are others that are incidentally acquired because they're on the other end of these communications. So target is the one you're going after.

And the statute requires that that target be a non-U.S. person located overseas. And so that's the foreignness determinations that we're talking about as we go through at great lengths to make sure that that target is in fact belongs to a non-U.S. person that is located overseas.

The other two questions?

MR. MEDINE: Tasking or task.

MR. WIEGMANN: Tasking is when you're going and saying, okay, I want to task this account means I want to collect information from that account. So that's the collection.

MR. LITT: You task a selector.

MR. WIEGMANN: You task a selector. So you're identifying, that's when you take that selector to the company and say this one's been approved. You've concluded that it is, does belong to a non-U.S. person overseas, a terrorist, or a proliferator, or a cyber person, right, whoever it is, and then we go to the company and get the information.

MR. MEDINE: And directives.

MR. WIEGMANN: So directives are the orders that go to the companies that say they have to comply with the lawful tasking. So that's the kind of more overarching order that goes to a company provider and says, okay, you have a legal obligation to comply with the taskings that are

given to you and here are the rules and everything. And that's all provided to them.

Is that a fair summary? I'll ask my colleagues to see if that is --

MR. DE: Keeping target as the statutory term. A term like selector is just an operational term to refer to something like an email or phone number, directive being the legal process by which that's effectuated, and tasking being the sort of internal government term for how you start the collection on a particular selector.

MR. MEDINE: Okay. So I guess building on that, what's the statutory rationale for about collections, because if the target is the email account or phone number, what is the justification for gathering communications between two persons, it may even be two U.S. persons who are discussing that phone number or that email address, but they are not themselves, there's no to or from that particular email address or particular phone number, why is that targeting that is permissible under the statute?

MR. WIEGMANN: Right. So the conclusion there again in a typical case, you're right, if you're targeting, you know, bad guy at Google.com you're targeting that person's accounts, their communications.

Why abouts collection is different is it's not necessarily communications to or from that bad guy but instead about that selector.

And so what the court has concluded is that when the statute uses the term targeting of a non-U.S. person overseas, targeting that selector qualifies under the statute for targeting that non-U.S. person overseas.

So it doesn't have to be targeting necessarily to or from, but can also target the communications that are about that particular selector.

MR. MEDINE: So that's a different meaning of target than earlier, which is where you're focusing on an account, now you're discussing targeting means discussions about that account.

MR. WIEGMANN: About that selector, correct.

MR. DE: It is always focused on that account, so I think the key is, the misperception that some may have that about collection is somehow about a key word or about the person that may be behind that account.

But all collections under Section 702, whether it's upstream abouts, which is a subset of upstream, or PRISM is all based on the selectors at issue.

MR. MEDINE: But does it raise -- oh, I see my time has expired so I'll --

MS. BRAND: I'm glad to see you're following your own rules.

Just to follow-up on that because that's a good line of inquiry, just to make sure that everyone understands. So you're saying that if someone is emailing about Rachel Brand or about explosives that would not be a permissible about query under your explanation?

MR. DE: So I would like to --

MS. BRAND: But you could, you could perhaps get it about Rachel Brand at --

MR. DE: Just so that, because I think this is an issue that all of us slip into, clarifying querying for collection.

So we are discussing now the collection of information. Abouts is a type of collection of information.

MS. BRAND: I'm sorry, right. Yes, that's right.

MR. DE: And so all collection of information is based, focused on selectors, not key words, as you just mentioned like terrorist, or like a generic name or things along those lines.

MS. BRAND: Okay.

MR. DE: And it's the same selectors that are used for the PRISM program that are also used for upstream collection. It's just a different way to effectuate the collection.

MS. BRAND: Okay. I think a large part of the function of these hearings is a public

education function and so I thought David's questions were great to explain the meaning of different terms, and I'm glad that you're willing to bear with us asking you some questions that we've already discussed with you in private. But I think it's helpful for everyone to understand what we're talking about.

And along those lines there was some discussion in Pat's questions about purging data that doesn't turn out to be foreign intelligence information.

But can you explain how on the front-end you implement the requirement that, not only that the target be a non-U.S. person reasonably believed to be abroad but that you expect to get foreign intelligence information through the collection, that's a separate statutory requirement. How do you go about ensuring that you're collecting that type of information?

MR. DE: Sure. So in our earlier discussion we skipped right to the foreignness determination, but that's actually a second step.

There has to be a reason one actually wants to collect intelligence from the particular selector in the first place.

And then one has to get to the fact, is this a type of collection permitted under the statute? So there has to be a valid foreign intelligence reason to do that collection.

But beyond that there has to be a valid foreign intelligence reason within the ambit of one of those certifications that the FISC approves annually. Those are certifications on things like counterterrorism, encountering WMDs, for example, weapons of mass destruction.

And so when an analyst needs to make a determination as to the valid foreign intelligence purpose for which they want to effectuate collections, they must also document that.

That is documented in a targeting rationale document in advance, ex ante, and those are always reviewed by the Justice Department and the Director of National Intelligence every 60 days.

MR. WIEGMANN: This is an important point for non-U.S. persons because people think about, okay, well once you've concluded that it's a non-U.S. person overseas then you can collect whatever you want. As Raj said, that's really not the case.

It really is targeted, not only based on the identity of the person and the location of the person, but also that you're trying to get foreign intelligence. And so it's an important protection really in the statute that is designed for non-U.S. persons. It's not blanket collection of any non-U.S. person overseas. It's aimed at only those people who are foreign intelligence targets and you have reason to believe that going up on that account that I mentioned, bad guy at Google.com is going to give you back information, information that is foreign intelligence, like on cyber threats, on terrorists, on proliferation, whatever it might be.

MS. BRAND: What can you tell us in an unclassified setting about the documentation of

foreign intelligence purpose or the oversight to ensure? I mean we've talked a little bit about that in past questions, but can you give us anything more specific?

MR. WIEGMANN: They do have to document that at NSA and every -- it's essentially called a tasking sheet, I think. And on that sheet they are documenting the foreign intelligence purpose that they are trying to pursue in going after a particular target.

And those are all reviewed together with the foreignness determination by the Department of Justice on a regular basis.

MS. BRAND: That's a separate sheet for every selector?

MR. WIEGMANN: For every single one, that's right.

MR. BAKER: And I think, at least with respect to FBI, I think the review that Raj mentioned earlier is done every 30 days on these tasking decisions, I guess you'd say, the foreign intelligence and the foreignness determination.

MR. DE: And if I could put that into the broader context of if the question really is getting at what is the process within which that happens, even before that happens we have training for analysts as to how they should document this material, we have audits of our databases, we have a comprehensive compliance program, we have spot checks, even within NSA prior to the 60 day reviews that are done by the Department of Justice and DNI, for us anyway.

There are also quarterly reports to the FISC on compliance with the program, semiannual reports to the FISC and to Congress, and annual inspectors general assessments, and as I mentioned, the annual certification process by the FISC.

So I think those decisions are, while they're one very granular aspect of the program, are conducted within the context of this broader regime.

MS. BRAND: Okay. And I see that my time just ran out.

MS. COLLINS COOK: I wanted to ask one additional question about abouts. Can you do about collection through PRISM?

MR. DE: No.

MS. COLLINS COOK: So it is limited to upstream collection?

MR. DE: Correct. PRISM is only collection to or from selectors.

MS. COLLINS COOK: I wanted to shift to a separate topic. One of the things that I have found both concerning and frustrating through the process of our evaluation of programs is how to both assess and articulate the efficacy of these programs.

And Mr. Litt, you had begun speaking about this in your prepared remarks. And I'd like to ask a couple of questions. One, how do you assess the efficacy of a particular program? How do you think we should be assessing the efficacy of a particular program?

And three, it's not really a question, it's more of a comment which is, please don't give

me a series of success stories and then say that's how you evaluate the efficacy of the program. Because I think that's an initial response from the government often in response to a question, either from a body like ours or from the media.

But how do you assess the efficacy of the program, how periodically do you do so, and how would you encourage us to assess the efficacy?

MR. LITT: Well, let me start on that, and I want to start by saying that I completely agree with you that sort of individual success stories are not the way to evaluate a collection program and its utility.

The way you evaluate collection programs is going to depend in part on what the particular program is for.

In this case, we have in fact the Office of the Director of National Intelligence has attempted, part of our job is to try to determine that resources are effectively allocated within the intelligence community budget.

And so we have done studies to try to

look at, okay, what are our collection priorities, how much reporting is generated on these priorities, and where do those reports come from, what kind of collection source, to the extent we can identify that. And that's one of the ways that we've determined that Section 702 is relevant.

Another thing is just by looking at the sheer nature of the information that we get and its utility towards a whole variety of national priorities. That's a more impressionistic approach, and yet you can see time and again in important intelligence reports that are provided to policy makers that it's derived from Section 702 collection.

So those are two ways that I would look at estimating the value of a particular collection.

MR. DE: If I could just add on to that. With respect to this program or any program I think intelligence professionals will tell you that any tool must be evaluated in the context of

the other tools in which it is utilized.

All intelligence tools are used in complementary fashion with one another and to isolate one particular tool and evaluate its effectiveness in isolation probably doesn't do us justice as to what's valuable and what's not.

It also depends on the type of tool. Different types of intelligence programs are used for different purposes. A program like Section 702 is used for different purposes, for example, than a program, a metadata program with telephony metadata.

One may be a discovery tool to help pursue more specific collection and others may be used as in fact the specific collection that follows from that.

Third, there may be uses in which the PCLOB has recognized in terms of either directing the government in certain directions or at least helping to shape the focus of the government.

And so I think the absolute wrong question is how many plots did this tool stop.

And you can fill in the blank for what this tool refers to. But that is absolutely the wrong question, and I think it won't do us justice to figure out what we need as a government.

MS. COLLINS COOK: I have time I think for one last question. What is the view of the various agencies as to whether or not 702 is an effective and valuable program for the United States?

MR. BAKER: I think it is an effective and valuable program for the United States.

And if I could just address your last question as well. I mean I think you really, in order to understand whether it's effective and useful you have to think about what your goals are with respect to this particular program.

And the goals for this program, like many other collection programs are to obtain I think timely, accurate, informative foreign intelligence information about the capabilities, plans, intentions of foreign powers, agents, actors, and so on and so forth.

And so I think really what you're talking really is, I think, developing a good metric to understand whether this program is worth all of the costs associated with it. And so I think you'd want to look at the amount of information that you, that we acquire, but also then obviously the quality of it. How good is it? And I think you can slice that a lot of different ways, as my colleagues have suggested.

So I think that's really what I would recommend you be focused on. But you have to, because this is a broad-based foreign intelligence collection program you have to look at not only, I mean you have to look at counterterrorism but you have to look more broadly than that because this program is not limited just to counterterrorism.

MR. DE: I agree it's definitely an effective program. I think the one point I should have added is that the review that Bob mentioned happening within the executive branch is not limited to the executive branch.

Congress also reviews the effectiveness

of this program, as well as the 215 program. And I think that's part of the rationale behind having sunset clauses for various programs is that when those statutory provisions expire, as did the 215 program twice in the last five years and as did 702 in 2012, Congress undertakes, as it should, an evaluation of the effectiveness of the programs.

MR. LITT: So I completely agree that it is an effective and important program and I really want to emphasize the last point that Jim made, which is that this program should not be considered solely as a counterterrorism program. This program has utility, has significant and exceedingly important utility in areas outside of counterterrorism.

MR. DEMPSEY: Trying to clear up another issue in terms of the participation of service providers and the awareness of service providers in the 702 implementation, is 702 implemented, all 702 implementation is done with the full knowledge and assistance of any company that, from which information is obtained, is that

correct?

MR. BAKER: Yes. The answer to that is yes.

MR. DEMPSEY: So early on in the debate there were some statements by companies who may or may not have been involved in the program saying, well, we've never heard of PRISM. But whether they ever heard of PRISM, any company that was, from whom information was being obtained under 702 knew that it was being obtained?

MR. LITT: Correct.

MR. DE: PRISM is just an internal government term that as a result of the leaks became a public term. But collection under this program is done pursuant to compulsory legal process that any recipient company would have received.

MR. DEMPSEY: So they know that their data is being obtained because --

MR. DE: They would have received legal process in order to assist the government, yes.

MR. DEMPSEY: One thing I read in one of the statements is under 702 you could target entire countries or regions, is that correct?

MR. DE: So all collection under 702 is based on specific selectors, things like phone numbers or email addresses. It is not a bulk collection program.

MR. DEMPSEY: And a selector would not be an entire area code, for example?

MR. DE: Correct, correct.

MR. DEMPSEY: Going back to the constitutional -- oh, one other set of questions.

Even I've lost track now of what you've already said here versus what you've said elsewhere. But in terms of where you make a determination that a person is a non-U.S. person outside, reasonably believed to be outside the United States and then you later discover that that was good faith but wrong, the person was in United States, or the person was a U.S. person, do you track that, and what do you do when you discover that, and how often do you discover?

I'm not talking about the roamings, I'm talking just about you thought he was outside the United States and that was just wrong, or you thought he was a non-U.S. person and that was just wrong, how often does that occur?

MR. DE: So I'll defer to Brad on the sort of overarching review, but if I could just make a point about what happens. So yes, we keep track of every time new information comes to our attention to suggest that a prior intelligence evaluation was incorrect, even if it had met the legal standard.

Every such incident is a compliance matter that has to be reported to the FISC and ultimately in semiannual reports reported to the Congress.

And third, that sets in process a purging process by which information that should not have been collected if it had not met the legal standard needs to be purged from NSA systems.

I think Brad can speak to the level of

accuracy of those.

MR. BAKER: Just real quick, it's the same. The item is de-tasked and the information is purged.

MR. WIEGMANN: Right. So just to distinguish again between two different types of compliance issues. One is the roamer example that you mentioned.

So this is, let's say we're up on a cell phone that we believe belongs to a bad guy who's outside the United States, a foreign person, and then that person shows up in Chicago, when that happens we de-task that cell phone. That means we're no longer collecting the communications.

That's a compliance incident that's reported but it's not an erroneous determination. It's based on the movement of the individual.

So putting those cases aside, in cases where we just kind of get it wrong, we think the email account or the phone is located overseas but it turns out that that's wrong, or it turns out

that we think it's a non-U.S. person but it is a U.S. person, we do review every single one to see if that's the case.

And our review at Justice we decided to review, and as I mentioned earlier, we think it's less than one in a thousand cases where they make that determination erroneously.

MR. DE: And this probably bears worth repeating that the initial determination is not a once and done, so there is an affirmative obligation for analysts to reaffirm the foreignness determination on a periodic basis, which contributes to the ability to make sure that determination is in fact fresh and current, which of course contributes to the accuracy of that determination.

MR. DEMPSEY: Going to the constitutional issues, back to those for a second, the FISA court has determined, I mean they must they must determine every year that the program is being implemented consistent with the Fourth Amendment.

The very first time they determined that, there was an opinion that they issued. That one is, am I right, not yet public?

MR. WIEGMANN: I think that's correct.

MR. DEMPSEY: Isn't that a good candidate for declassification?

MR. LITT: We have a lot of good candidates for declassification.

MR. DEMPSEY: Yeah.

MR. LITT: In all seriousness there, we are, there are a lot of documents that we have that we are reviewing for declassification that include not only FISA court opinions but a whole variety of other documents.

MR. DEMPSEY: The FISA court in 2008 when they last considered the constitutionality of a program, the predecessor to 702, the court issued a redacted but largely unclassified opinion conducting a relatively full Fourth Amendment analysis.

And there's been some Fourth Amendment analysis conducted in this situation, and if

you're sort of talking about, you know, the Rosetta Stone kind of Ur document, then the very first court opinion should have been the most fulsome explanation of the constitutionality of the program.

I think that -- I mean I hear Bob saying there's a lot of opinions out there, but to me this one seems to be one that would explicate at least one court's judgement on this because it's been the basis of -- I assume all the rest just said nothing has changed that would merit us to reconsider our very first judgement.

MR. WIEGMANN: So I mean I think it's among the opinions. We're committed to reviewing all the opinions of the FISA court to determine which ones can be declassified in redacted form. So I imagine this will be among those that are reviewed. So absolutely, I don't disagree. It'll be among the opinions that will be reviewed.

MR. DE: I just don't want to leave folks with any mysterious misimpression. I think the Board has access to everything and so one

shouldn't have to assume anything about subsequent opinions. The Board has in fact reviewed everything.

And so I just don't want -- what I think would be an unfortunate consequence would be for folks to take away the impression that there is a mysterious opinion that has some secret analysis, and I don't think that's the case. I don't think you intended to suggest that.

MR. MEDINE: The Board does have access to it but I think the question is whether the public should have access to it as part of the debate. But it's Judge Wald's --

MR. DEMPSEY: The public had access to the 2008 --

MR. MEDINE: It's Judge Wald's turn.

MR. WIEGMANN: So just one other thing I would add on that is that 702 collection has now been challenged by a number of criminal defendants when 702 information is being used against them in their cases. And so we'll be filing public briefs and we can expect some more decisions in that area

as well.

So that's another way that the constitutionality of 702 will now be on the public record, or I mean the opinions on it, and the briefs and everything will now be a matter of public record.

MR. MEDINE: Judge Wald.

MS. WALD: Okay. By whom and under what substantive criteria is the initial decision to use a U.S. person selector for searching the PRISM base made? I mean who decides let's do that? What's the substantive criteria on which they make it?

You don't have to go into the review process. I know the decision will be reviewed up and down. But how does that get made? What's the substantive basis?

MR. DE: So I can speak for NSA in particular.

MS. WALD: So just to clarify, that means if it goes to one of the other agencies, not NSA, CIA or FBI or something, they make their own

substantive decisions for querying?

MR. DE: Yes. The 702 program perhaps as a necessary predicate is one that all agencies operate on their own and have their own minimization procedures which would address topics like searches.

NSA's procedures in this regard, in this element have been made public and so the standard is that such a query needs to be reasonably likely to return foreign intelligence information.

MS. WALD: Be reasonably likely. And who is it made by initially?

MR. DE: It's made by the analyst.

MS. WALD: By the analyst who's working on that particular case, okay.

My other question is that the President did, if I understand his directive correctly, direct that there be some changes in the treatment of non-U.S. persons as to the limits on and retention of the data acquired incidentally to bring them more in line with those of U.S. persons

incidentally where there is no foreign intelligence value apparently.

Can you tell us a little bit more specifically if anything has been done in that regard or is being contemplated vis-a-vis 702?

MR. LITT: So I think first of all it's important to understand the point that somebody made, it may have been Brad made earlier, which is that there are already protections to some degree built into the system there. The protections for non-U.S. persons are not as great as those for U.S. persons because U.S. persons are protected by the Fourth Amendment.

But there is a requirement that we can't target a selector unless we have reason to believe it's of foreign intelligence value. And there's sort of a general principle that the intelligence agencies, their job is to collect, analyze, and disseminate foreign intelligence information, not random information.

I think what the President has directed is that we go back and look at our procedures and

not only with respect to 702, but with respect to signals intelligence in general, assess whether, the extent to which it's possible to provide limitations on collection, retention, and dissemination that more closely track those for U.S. persons.

For example, Executive Order 12333 provides specific categories of personal information about U.S. persons that can appropriately be retained and disseminated.

There's a list of them in Executive Order 12333 and the President has asked that we assess whether we can apply those same sorts of rules to personal identifiable information of non-U.S. persons.

MS. WALD: Right now, just to follow-up, right now if you get incidental information about a foreign person in the course of targeting another foreign person and you look at it, do you use the same criteria and look at the same review and say, well, you know, he was just talking to his grandmother or something, there isn't any

foreign intelligence there, and you purge it?

MR. DE: Any time there is not foreign intelligence value to collection, by definition it would be purged.

But I think an important point to be made as you are articulating, Judge, is incidental collection, just to explain that term a little bit, all communications obviously have two ends. One end is the target and the other is presumably not a target. We don't know. One doesn't know ex ante.

And so by definition there will be incidental collection of non-U.S. persons, as well as U.S. persons. Historically, constitutional protections obviously have only applied to the U.S. person subset.

MS. WALD: I understand.

MR. BAKER: Can I just make a comment about that?

MS. WALD: We don't have time. Okay, quickly on the last time, I found it very provocative when you were answering Beth Cook's

question about if you're going to assess the efficacy of a program you have to look at it in terms of its efficacy and the holistic view of all of the programs.

I guess it's inevitable that I would ask the question, but how can anybody except you people do that, because so many of your programs, I think, are just unknown, even to the FISA court? They're not all FISA supervised, and certainly the outside world doesn't know about many of them. So you know, how in effect can an outside assessment be made?

MR. DE: If I could just address it since it was in response to my comment. Certainly I think I would not suggest that there should be a public evaluation of all intelligence programs. I think, for example, this Board as access to information about counterterrorism programs and so I would expect that any evaluation would be in the context of the other CT programs that you have the jurisdiction to review.

As with Congress, as I mentioned, they

reevaluate programs on a periodic basis. And I think the public record now indicates that there is a fairly robust exchange between the executive branch and the legislative branch on a variety of programs. And so I think that's where traditionally the evaluation has occurred.

MR. LITT: Yeah, I was just going to say that we've managed, we've set the balance between public disclosure and the need for secrecy by empowering the congressional intelligence committees. We're required by statute to keep them fully and currently informed of intelligence activities, and we do. They know about these programs and they have the opportunity to evaluate them, and they do.

In fact, they passed an Intelligence Authorization Act that includes a lengthy classified annex that is very prescriptive with respect both to reports that it requires of us and directions as to what we should, you know, where we should be spending our money.

So that's sort of the external

oversight and the way we've said, okay, well, we need to have oversight of these but they still need to remain classified.

MR. MEDINE: Did you want to finish? I don't know, you wanted to make a point earlier about foreign intelligence.

MR. BAKER: I had several points I wanted to make. But let me just on that real quick, I mean I think the, even the addition of Congress having oversight of it, the courts in certain circumstances, and then also obviously the President and all of the executive branch officials, we have an obligation to make sure that in addition to adherence to the law and taking care that the laws are faithfully executed, to spend our time and spend our money on programs that are effective and not be wasting our time on things that are not.

I mean that flows from the President to the DNI, the Attorney General, Director of the FBI, Director of NSA and so on. We should be focused on things that are useful and collecting

information that produces the kind of intelligence information that I was talking about before.

So the other comment that I just wanted to make was just with respect to FBI, our personnel only have access to the databases when they've received the proper training with appropriate oversight and operating consistent with the court-approved standard minimization procedures when they're doing their query activity.

MR. MEDINE: I wanted to shift to a different subject, which is attorney client privilege. There were some press reports a couple of weeks ago about collection of information that may involve attorney client communications.

But I want to focus particularly on the NSA minimization procedures, which I understand do exclude attorney client communications but only in a very narrow context where the client is under criminal indictment and the United States, basically on a federal criminal indictment.

That seems like a very narrow

interpretation of attorney client privilege. I wanted to see if that is the interpretation you apply in minimizing communications, and if it is what impact there would be if it was expanded to the more normally accepted definition of attorney client privilege, which is basically lawyers and clients consulting with each other?

MR. DE: So we have written a letter to the ABA and commented on it to the Board and to the public, I think it's a public letter now, which explicates in fuller detail than I probably can off the top of my head as to our procedures.

But I think one fundamental premise is that analysts are under an obligation to identify for the Office of General Counsel any time they encounter something that may be potentially privileged.

And I think as all of us who are lawyers, I think that probably encompasses every one up here on the stage, knows just because a communication is with a lawyer does not mean it is in fact a privileged communication. So it's

helpful to have a lawyer involved to determine that.

While I can't speak to any particular incident that may have been written about in the press I think there's a couple of big picture points that are worth making. One is our office has historically provided a range of advice to minimize to the extent possible the collection of attorney privileged material.

MR. MEDINE: That's privilege just where there's a criminal indictment or are you viewing privilege --

MR. DE: Beyond the criminal. So the point I'm trying to make is that while there may be a specific provision in the 702 procedures that addresses the criminal context, there's a reason why we ask analysts to consult counsel, because the advice can often be tailored to the specifics of a circumstance far outside the criminal realm, recognizing the import of attorney client privileged material in context, even outside the criminal context.

MR. MEDINE: I want to talk a little bit about reverse targeting where you target someone overseas potentially with the view of collecting information about a U.S. person in the United States, and that's impermissible.

There seems, again maybe this is a somewhat technical point, but there seems to be somewhat of a quirk in the statute. It says that you can target people reasonably believed to be outside the Unites States, you cannot reverse target someone outside the United States if the purpose is to target a particular known person reasonably believed to be in the United States.

Does that permit targeting a person outside the United States with the intent of gathering information about U.S. persons not in the United States?

MR. WIEGMANN: No.

MR. MEDINE: Why not?

MR. WIEGMANN: There's a separate provision that bars targeting U.S. persons outside the United States and so if you were doing that

and you are trying to target a U.S. person outside the United States, you couldn't do that.

MR. MEDINE: So you wouldn't do the reverse targeting procedure?

MR. WIEGMANN: I don't know if you would call that reverse targeting --

MR. DE: There is another statutory provision that prohibits the targeting of U.S. persons outside the U.S. under 702 --

MR. MEDINE: Even reverse targeting? Again, I'm not talking about -- I agree it's clear that you can't target a U.S. person outside of the United States, but what if I find a non-U.S. person that I know is in communication with a U.S. person who's also outside of the United States, is that permissible?

MR. WIEGMANN: No.

MR. DE: No.

MR. MEDINE: Because?

MR. WIEGMANN: Because you would be targeting, if your real purpose is to target that U.S. person, you're targeting that person.

MR. MEDINE: So reverse targeting in your view is the same as targeting? The prohibition on reverse targeting is co-existent with the prohibition on targeting?

MR. WIEGMANN: Well, I mean again I think of reverse targeting as a geographic issue essentially when you're targeting, let's say you have a legitimate target overseas but you really want the communications of a U.S. person or a non-U.S. person inside the United States, but the statute says you can't do that.

MR. MEDINE: Right, but --

MR. WIEGMANN: But as we were just explaining which is if you have a U.S. person that you're interested in overseas, you can't use 702 to target them either and I don't think --

MR. MEDINE: Or reverse target them?

MR. WIEGMANN: What's that?

MR. MEDINE: If you know that that U.S. person is in communication with a non-U.S. person and both of them are overseas --

MR. WIEGMANN: Right.

MR. MEDINE: Could you target the non-U.S. person to get the U.S. person's communications?

MR. WIEGMANN: You couldn't do it for that purpose but if the non-U.S. person overseas is a valid foreign intelligence target that you're interested in their communications, sure, you can target that person. And the fact that they're incidentally communicating with a U.S. person overseas, that's okay. I wouldn't consider that reverse targeting.

You still have to have that legitimate target. I don't know if that answers your question, but.

MR. MEDINE: It did.

MR. BAKER: I'm not going to read it now and take up your time, but take a look at Section 704 A 2, and that may address the kind of concern that you're focused on perhaps, but perhaps not.

MR. MEDINE: Okay. I wanted to get back to efficacy. As you know, our charge is to

look at the balance between national security and privacy and civil liberties, and I think following up on Ms. Cook's question -- sorry, I'll just hold that until the next round.

MS. BRAND: I wanted to go back to upstream collection a little bit. I've seen some statements in the public domain about the volume of upstream collection vis-a-vis the volume of PRISM collection. What can you tell us in a public setting about that?

MR. DE: I think the best publicly available information is from the October 11th, 2011 opinion that has now been declassified in which there was a rough estimate there, and forgive me for if it's not precise, but that about 10 percent of collection is upstream. On the order of magnitude, I just don't know the exact number.

MS. BRAND: Okay. So you said in an earlier round of questioning that upstream, collection from upstream is retained for a shorter period of time than collection from PRISM and you

said that the reason for that distinction is that there's a potentially greater privacy concern with respect to upstream collection.

Can you elaborate on why, whether the additional privacy concerns that pertain to upstream.

MR. DE: Sure. And a lot of this is laid out in this court opinion that's now public. This is from the fall of 2011. I think because of the nature of abouts collections, which we have discussed, there is potentially a greater likelihood of implicating incidental U.S. person communication or inadvertently collecting wholly domestic communications that therefore must need to be purged.

And for a variety of circumstances the court evaluated the minimization procedures we had in place and as a consequence of that evaluation the government put forth a shorter retention period to be sure that the court could reach comfort with the compliance of those procedures with the Fourth Amendment. And so two years was

one element of the revised procedures that are now public.

MS. BRAND: So from what you just said that if using a legitimately tasked about term a wholly domestic communication is collected, it has to be purged?

MR. DE: If one recognizes it, yes. In fact, there's a --

MS. BRAND: Even if it has foreign intelligence information?

MR. DE: There are specifics. Off the top of my head I can't articulate all the particular exceptions in the minimization procedures but there are an elaborate set of detailed procedures that are now public that discuss how upstream collection must be treated in order to account for this concern.

And it has things like data must be segregated in certain ways where the risk of collecting a wholly domestic communication is higher, there's a shorter retention period.

Wholly domestic communications are not

permitted under the statute, and so therefore as a default rule, yes, it must be purged.

MS. BRAND: Jim, was there something you wanted to add?

Okay. I want to use the word incidental collection there again, and your definition earlier seemed to be that by incidental you mean, by incidental U.S. person collection you mean that the person on the other end of the phone from the non-U.S. person abroad is a U.S. person. That's your definition, right?

Is there another definition that you're aware of? Because you seem to be -- okay.

I think there's been some frustration with the use the term incidental in that context because it's not accidental, it's intentional. It's actually unavoidable. And so I just wanted to make sure that we're all on the same page, that by incidental you mean not accidental, not unintentional, but this is actually what we're doing.

MR. LITT: It is incidental to the

collection on the target. It is not accidental, it is not inadvertent. Incidental is the appropriate term for it.

MS. BRAND: Okay.

MR. DE: And I'd say that term I think has been used far beyond this program and historically, so there's no judgement intended. That is just a term.

MS. BRAND: Okay, okay. I'll hold the other questions for another round.

MS. COLLINS COOK: Just following up on David's question, I think it goes to a broader point which is that there is a perception that this statute is fairly complicated, there's got to be loopholes or idiosyncrasies in there somewhere.

But let me just ask you, would it be the view of the United States government that it is appropriate to use 702 to intentionally target U.S. persons, whether directly or through reverse targeting, whether they are inside the United States or outside the United States?

MR. LITT: No, definitely not.

MR. DE: No.

MR. LITT: That is not permissible.

MS. COLLINS COOK: I wanted to also follow up on a question about the abouts. And I apologize, again just for folks understanding that we spent six and a half hours talking with folks about just the oversight mechanisms in place and were unable to get through that entire conversation. So I apologize if you've said this before today.

The collection methods, procedures that you use with respect to abouts, those procedures, are they approved by the FISA court?

MR. DE: Yes.

MS. COLLINS COOK: Are those transparent to Congress?

MR. DE: Yes.

MS. COLLINS COOK: I think we haven't necessarily, we started to allude to this but can you talk a little bit about your impression of how the intel committees in particular view their obligations with respect to oversight of your

programs and whether you have found in your experience that to be pro forma or in any way lacking?

And let the record reflect a few, not quite eye rolls, but I think the response was, no, they have not found this to be pro forma in any way.

MR. LITT: I've been on this job now for getting on towards five years and I have found nothing about my interactions or our institutional interactions with the intelligence committees to be pro forma.

They have fairly substantial staffs which have a lot of experience. Some of them come from the community. They know, they dig very deeply into what we do. The DNI occasionally uses the term wire-brushing for the interactions that we have with the committees, so it's not a pro forma interaction in any way.

MR. DE: If I could add one point, on programs like 702 that we're talking about today for example, we all lived through the

reauthorization of Section 702 in 2012.

That process was not simply in connection with the intelligence committees, but I can remember numerous briefings where we would go up for a member, for all member briefings that the intelligence committees would host for the Congress.

So I don't want to leave the impression that it's only with the intelligence committees, particularly for a program like 702 that needs to be voted on by all members of Congress on the basis of a sunset clause.

MS. COLLINS COOK: I want to make sure that my colleagues have time for their last round of questions so I'll cede my time.

MR. DEMPSEY: Going back to the minimization procedures question, and specifically the incidental collection question, am I right that the rule is that whether the information is inadvertently collected, that is you were tasking on the wrong selector or some mistake was made and you got something that you didn't intend to get

that's inadvertent, or you were correctly targeting the right account and then you collected communications to or from a U.S. person that's incidental, the procedures say, minimization procedures, rules say that if you never discover that it was inadvertent and never discover that it was incidental, you never realized that it was a U.S. person collection, it's deleted after five years?

The basic rule is you keep it for five years, you keep everything for five years, two years on upstream, five years on PRISM, and then it gets deleted. That's the baseline rule, right?

MR. LITT: Correct.

MR. DEMPSEY: And then you on top of that the rule is that if then you, through analysis, through reviewing it that it was inadvertent or incidental collection on a U.S. person you must immediately purge? Bob's shaking his head.

MR. LITT: There's a difference in the way inadvertent and incidental, as you're using

those terms, are very different concepts.

Inadvertent refers to a collection that was not authorized by law. That is purged.

Incidental --

MR. DEMPSEY: Purged unless?

MR. LITT: Unless, as Raj mentioned, that there are certain exceptions. I'm certainly not able to recite them but they do exist. But they're fairly narrow.

Incidental is collection that is authorized by law. And at that point the rules relating to U.S. persons kick in and if you determine that it has no foreign intelligence value you purge it.

MR. DEMPSEY: Right, but I mean what's your response to the argument, well, fine, that just means that if you think it's valuable you can keep it, if you don't think it's valuable then you purge it?

MR. LITT: But it's lawfully collected.

MR. DEMPSEY: Fair enough. But you do, if it is of interest to you, you do keep it?

MR. LITT: If it's of potential foreign intelligence value --

MR. DEMPSEY: Minimization means --

MR. LITT: If it can be useful to providing the intelligence that policy makers need or to protecting the nation against threats, then yes, we keep it for the required period.

MR. WIEGMANN: So again, to make it more concrete, if it's a terrorist overseas, he is calling a number in the United States that belongs to a U.S. person, we want to keep that information. It is incidental, the fact that we're getting the U.S. person number and we're targeting that non-U.S. person overseas, but he's calling Minneapolis, we want to keep that communication because it's of high interest to us.

MR. DE: One point I would add is just that minimization refers to steps in the process, everything from collection to review to dissemination. And so I think we're talking about one element here, and to retention. And so there are different stages in the process.

To disseminate that information a certain threshold would have to be met and so forth.

MR. DEMPSEY: Yeah, I wish there were some way, I mean I know it's totally now embedded both in law and guideline and practice, but minimization means different things.

Minimization means keep it for five years and then delete it, minimization means don't disseminate identifying information, minimization means delete it unless it's intelligence information. Those are very different.

MR. LITT: Well, they all fall within the statutory definition of minimization essentially. I'm going to mangle it a little bit, but it's procedures that are designed to minimize the acquisition, retention, and dissemination of information about unconsenting United States persons consistent with the need to produce foreign intelligence information.

And so you're going to have different minimization rules based on the particular

missions of the agencies. You're going to have different minimization rules depending on the nature of the activity you're governing. You're going to have different minimization rules depending upon the nature of the information. But minimization is that entire category of rules.

MR. DEMPSEY: But it is a little bit of a circular definition which means different things in different contexts. Sometimes it means you've --

MR. LITT: I'm not sure I'd say circular but I would say it means different things in different contexts.

MR. WIEGMANN: It's a balance.

MR. BAKER: If I could just real quick just to emphasize, you know, as Bob was just alluding to, the FBI does have its own standard minimization procedures with respect to this type of activity. I assume you've had access to those.

So anyway, there's a lot on the table that we just talked about with respect to minimization, but I would direct you to those as

well in terms of understanding the FBI's role.

MR. MEDINE: Judge Wald.

MS. WALD: When a U.S. person information that's been, quote, incidentally acquired and kept for legitimate reasons or whatever in the base is disseminated to foreign governments, as is permitted under certain circumstances, it said that it's usually masked.

I think it would be useful for public consumption to know what the masking process entails, and in what circumstances it isn't masked, and whether or not the different agencies can use different criterias for masking or it's all centralized by Justice or the Attorney General's provision.

MR. DE: Well, I can speak just for masking generally at NSA, and abstracting from the second party issue for a moment, is substituting a generic phrase like U.S. person for the name of the U.S. person that is actually collected.

And that U.S. person is a legal term. Obviously that means an individual or it could

mean a U.S. company or firm.

I don't think there's a centralized process. That's how we do it at NSA. I think that's how other agencies do it as well.

MS. WALD: But different agencies decide how to interpret their own criteria as to what should be masked and what shouldn't?

MR. LITT: It's part of the, in the 702 context it's part of their minimization procedures.

MS. WALD: Well, so what does that tell me? No, I mean specifically as to whether or not in what circumstances it's not masked, that's up to each agency, or not?

MR. LITT: Yeah, it's done on an agency by agency basis.

MR. WIEGMANN: But generally speaking, I think the minimization rules of each agency generally would not permit you to disseminate U.S. person information where that is not either foreign intelligence or necessary to understand that foreign intelligence. So in other words --

MR. DE: Or evidence of a crime.

MR. WIEGMANN: Or evidence of a crime for FBI.

So in other words, if I need to, if it's Joe Smith and his name is necessary if I'm passing it to that foreign government and it's key that they understand that it's Joe Smith because that's relevant to understanding what the threat is, or what the information is, let's say he's a cyber, malicious cyber hacker or whatever, and it was key to know the information, then you might pass Joe Smith's name.

If it was not, if it was incidentally in the communication but was not pertinent to the information you're trying to convey, then that would be deleted. It would just say U.S. person. It would be blocked out.

So they were in communication with, and it would just say U.S. person. So that's essentially how it works I think more or less in all the agencies. Is that a fair description, Raj?

MR. DE: Yeah, the basic parameters for FISA collection are articulated in the statute, the big principles of necessary to understand foreign intelligence or evidence of a crime. And then that's effectuated through the minimization procedures that each agency has. That's for 12333 collection. It's articulated, as Bob mentioned, in 12333.

MS. WALD: With those last subpart, would those, just take NSA as an example, would those mask criteria also include foreigners, non-U.S. person's information?

I mean suppose the government of Romania asks some question which might require a Rumanian non-targeted person who's in your PRISM base, would these masking procedures, etcetera, apply there too or are they just for U.S. persons?

MR. DE: In today's rule, masking procedures are for U.S. persons because they are derivative of the constitutional requirement, the minimization procedures that need to conform with the constitutional parameters for U.S. persons.

MS. WALD: So it would be up to the agency to decide whether they thought it was right or wrong to give that information to a foreign government?

MR. DE: I think there's two points to mention. One is no information would ever be disseminated unless it had foreign intelligence value.

MS. WALD: No, I know.

MR. DE: That's the entire point of disseminating that information.

MS. WALD: But having made that decision in terms --

MR. DE: If I may continue. The second point is that I think what the President has directed the DNI to examine in the PPD is what protections could be extended to non-U.S. persons. That's the study.

MS. WALD: And that's what you're working on?

MR. DE: That's the issue we're evaluating now.

MR. BAKER: One quick comment though. If I'm not mistaken, if you look in 50 USC 1806, which is Title I of FISA but I think also applies to Section 702, it says, and I don't think it restricts it with respect to U.S. person or non-U.S. person, that no federal officer or employee can disclose, can use or disclose information at all except for a lawful purpose.

So the information could only be disclosed for a lawful purpose. And I believe that's across the board.

MS. WALD: I don't have anything more.

MS. COLLINS COOK: I wanted to make sure I understood though both Judge Wald's question and the response.

I understood her to be asking under what circumstances dissemination could be made to a foreign government.

Are there separate agreements and procedures that might govern in that instance or are analysts able to simply decide they would like to provide foreign intelligence information to

foreign governments?

MR. DE: At least our procedures, our publicly available procedures have provisions that address sharing with second party partners. I don't have at my fingertips the details, but I can certainly get back to you on that. But they are now public and articulate the circumstances under which information can be shared with second party partners. Those procedures are approved by the FISC annually.

MR. LITT: I think that the critical point is that these are part of the minimization procedures that have to be approved by the FISA court to the extent we're talking again about Section 702.

MS. WALD: The minimization procedures are only for U.S. persons, aren't they?

MR. LITT: Yes, that's right.

MS. WALD: But I was talking --

MR. LITT: But there are general rules about when we can share FISA information.

MR. MEDINE: All right. Well, I want

to thank the panel very much for spending a fair amount of time with us today and discussing these issues in a public setting and we appreciate it.

And we'll take a short break and then we'll resume at eleven o'clock with our second panel. Thank you.

(Off the record)

MR. MEDINE: We're now ready to begin our second panel, and we are very pleased to be joined by Laura Donohue, who's a Professor of Law at Georgetown University Law School, Jameel Jaffer, for a return engagement, Deputy Legal Director at the ACLU, Julian Ku, who's a Professor of Law at Hofstra University, and Rachel Levinson-Waldman, who is Counsel for Liberty and National Security Program at the Brennan Center for Justice, and each will make a brief set of remarks, if you want to start.

MS. DONOHUE: Sure. Thank you very much for the opportunity to be here today. I'm looking forward to the discussion on 702.

I'd like to confine my remarks to four

central areas, just my initial remarks, and raise statutory and constitutional concerns.

First is with regard to targeting. I'm particularly concerned about four areas here. First is the inclusion of information about targets, and not just to or from targets.

Second is the burden of proof regarding whether somebody is a U.S. person or not.

Third is with regard to the burden of proof regarding the location of the individual. That is, if the NSA in either instance does not confirm, does not actually know where they are, the assumption that is built into the minimization and targeting is that it is neither a U.S. person, nor are they domestically located. And there is no affirmative duty for due diligence on the NSA to actually check their databases to find out if that individual is or is not a U.S. person and is or is not in the United States. And then the implications for the right to privacy.

In the second area on the post-targeting analysis, I'm particularly concerned

about the role of FISC, that it's severely circumscribed and that we're having warrantless searches.

So in the last panel we heard about that moment at which the information is obtained is not a search because it's foreign intelligence and there's an exception for the gathering of the intelligence.

But when information is then used for criminal prosecution, then at that point when the data is searched, if it were a case where if I were, say, speaking with a mobster in the United States and they happened to overhear incidental to my communications that I was engaged in other criminal activity, they would have to go to a court to obtain a warrant to then put a wiretap on my phone and listen to the content of my communications.

In this situation they don't do that and then they find that individuals are implicated in criminal activity and refer it for criminal prosecution.

And I would be happy to address the 2002 Foreign Intelligence Surveillance Court of review opinion that addressed this aspect, but it was with regard to Title I where there was probable cause that had already been established that the target in that case was a foreign power, an agent of a foreign power.

In this particular case, the individual is not themselves the target of any investigation and so the prerequisite Fourth Amendment threshold has not been met.

The third area is the retention and the --

MS. COLLINS COOK: Can you slow down just a bit? I can't keep up. Thank you.

MR. MEDINE: And we also have a court reporter who's probably her fingers are slowing down.

MS. DONOHUE: Sorry, I beg your pardon. I realize we only have a few minutes, and I also have written remarks which I'll be submitting.

MS. COLLINS COOK: I have reviewed

them. Thank you. I've reviewed what you've submitted thus far.

MS. DONOHUE: Right. So I will be submitting on these particular points following the hearing.

On the third area, the retention and the dissemination of data, and this came up with Judge Wald's question on the previous panel, there are a number of exceptions in terms of when the information itself has to be expunged.

The foreign intelligence information exception I would direct your attention to. It's not defined in either Section 702 specifically, or in the minimization or targeting procedures.

It is, however, defined in FISA to include any information that would be helpful for foreign affairs, which would include economic information, it would include political information, it would include a whole range of data.

The retention, dissemination for criminal prosecution, I've raised the Fourth

Amendment concerns. We're starting to see now in courts what's called parallel construction where individuals where information has come from intelligence agencies' programs, is then passed on to law enforcement, who then must create a parallel trail for probable cause, but the actual tip or initial indication of criminal activity came from intelligence.

And it essentially covers the traces that this initially arose within FISA or within Section 702, and I have increasing concerns, certainly as a scholarly matter, about the growth of parallel construction.

The client attorney privilege you had already mentioned in the last panel. That continues to be, I think, an area of some concern, not just because it's, not just in the post-indictment stage but in terms of all communications with attorneys prior to and in the context of the interception of content.

The retention of encrypted communications was not mentioned in the last

panel. All encrypted communications are retained according to NSA documents, as well as the technical barriers. If there are technical barriers they also will simply keep the information.

The other aspects of this have to do with multiple databases and CIA access, which I was surprised you didn't have the General Counsel of the CIA on the last panel. We now understand from NSA documents that the CIA has a separate set of minimization procedures and also uses Section 702. And I think that's important to take a look at what those procedures are, both the targeting and the minimization.

Finally, the fourth area that I'd just like to raise is the First Amendment concerns that I have. As has been well-recognized in the judicial system, First and Fourth Amendments often travel hand in hand, especially in national security when political matters are on the line.

And in this particular instance not only do we have a general First Amendment concern

but we know that if individuals visit IP addresses, for instance, that have been associated with particular targets, then their correspondence, communication, emails, etcetera, and other information is also retained.

What if that IP address is Al Jazeera, let's say? What if that IP address happens to be a media or a news site that's been associated with a particular area of concern? Then I think there are also First Amendment implications that follow from that.

So in conclusion I'd be happy to talk in more detail about each of these areas, the targeting, the post-targeting analysis, the retention and dissemination of data, and the final First Amendment concerns.

MR. MEDINE: Thank you very much. Mr. Jaffer.

MS. DONOHUE: Thanks.

MR. JAFFER: Thanks for the opportunity to appear before the Board.

The ACLU's view, as you already know,

is that Section 702 is unconstitutional. The statute violates the Fourth Amendment because it permits the government to conduct large scale, warrantless surveillance of Americans' international communications, communications in which Americans have a reasonable expectation of privacy.

In our view, the statute would be unconstitutional even if the warrant requirement didn't apply because the surveillance it authorizes is unreasonable.

As I discuss in more length in my written testimony, the statute lacks any of the indicia of reasonableness that the courts have looked to in upholding other surveillance statutes, including Title III and FISA.

But the point that I would like to emphasize today is that even leaving the constitutionality of the statute to the side, the government is claiming and exercising more authority than the statute actually gives it.

I say that for three reasons. First,

while the statute was intended to augment the government's authority to acquire international communications, the NSA's minimization and targeting procedures give the government broad authority to acquire purely domestic communications as well.

That's because the NSA's procedures allow the agency to presume that its targets are foreign, absent specific evidence to the contrary, and because the procedures don't require the government to destroy purely domestic communications obtained inadvertently.

Instead, they permit the agency to retain those communications when they're believed to contain foreign intelligence information, a phrase that is defined very broadly.

Second, while the statute was intended to give the government authority to acquire communications to and from the government's targets, the NSA's procedures also permit the government to obtain communications that are merely about those targets.

And that practice, in my view, finds no support in the language of the statute or in the statute's legislative history. But it's a practice that has profound implications for individual privacy.

In order to identify the communications that are about its targets, the government has to inspect every communication. To endorse the practice of about surveillance is to say that the government can surveil literally everyone, or at the very least that it can surveil every communication in and out of the country.

Finally, while Section 702 prohibits reverse targeting, the NSA's procedures authorize the government to conduct so-called back door searches, searches of communications already acquired under the FAA using selectors associated with particular known Americans.

Given the absence of any meaningful limitation on the NSA's authority to acquire international communications under Section 702, it's likely that the NSA's databases already

include the communications of millions of Americans.

The NSA's procedures allow the NSA to search through those communications and to conduct the kind of targeted investigations that in other contexts would be permitted only after a judicial finding of probable cause.

And if I have thirty more seconds I would like to make just one final point. Today we're focused on Section 702, but it's important to understand that Section 702 is merely one expression of a broader philosophy.

Yesterday the Washington Post reported that the NSA has built a surveillance system called MYSTIC capable of recording all of a country's phone calls, allowing the NSA to rewind and review conversations as long as a month after they take place.

MYSTIC is the logical endpoint of the arguments that the government is making here today. So the stakes and the conversation that we're having today are very high. It's very

difficult to believe that democratic freedom would survive for long in a system in which the government has a permanent record of every citizen's associations, movements, and communications. Thank you.

MR. MEDINE: Thank you. Professor Ku.

MR. KU: Thank you, and thanks also for the opportunity to appear before the Board today.

I just want to remind -- I have a different view I think from most of the panelists, and I apologize for not getting my remarks ahead of time.

I just want to remind the Board of two under-emphasized points of constitutional law that I think should frame our understanding of the U.S. government's surveillance practices under Section 702.

I mean first, it is important to remember that Section 702 and FISA itself need to be interpreted and understood against the history, and tradition, and the background of the President's broad, inherent executive power under

the Constitution to conduct electronic surveillance of foreign governments and foreign agents, especially overseas.

Second, although we often speak loosely of the Fourth Amendment's limitations on this presidential foreign surveillance power, it's worth noting that courts have repeatedly upheld wide-ranging, warrantless U.S. government surveillance overseas, even of U.S. citizens.

So these two constitutional observations should frame any legal assessment of Section 702 and FISA in general.

If you keep in mind the background and where we're coming from rather than where we are, 702 is not an ineffectual attempt to regulate lawless executive conduct, as the critics would have it.

In actuality, Section 702 almost certainly requires more limitations than are actually required by the Constitution and may even, although I'm not taking that position, but could in some circumstances encroach on the

President's foreign affairs powers to conduct foreign intelligence activities.

So let me just briefly elaborate on these two claims about constitutional law, which I'm sure some folks might disagree with, but this is not a dispute that U.S. presidents have long exercised the power under the Constitution to conduct foreign intelligence, and this uncontroversially flows from the President's role as the chief of foreign affairs under the Constitution. And almost every court considering the question has concluded that the President, has agreed that the President possesses an inherent constitutional authority to conduct foreign surveillance. And this is undisputed by any court.

In other words, there does not need to be statutory authorization for the President to engage in foreign surveillance.

Prior to the enactment of FISA in 1978, the executive branch claimed, and the courts did not dispute that it possessed a broad

constitutional power to conduct surveillance for foreign intelligence purposes, even inside the United States and usually without a warrant.

So prior to the enactment of Section 702 and its predecessors, the executive branch claimed a constitutional power to conduct warrantless surveillance in foreign countries for foreign intelligence purposes, whether or not that surveillance included a U.S. citizen who was physically overseas.

So given this history I'd ask the Board to keep in mind that Section 702 and its predecessors placed more constraints on the executive branch's conduct of overseas foreign intelligence gathering than has ever been imposed in prior, in the past.

You might conclude that we need even more constraints, but we should not kid ourselves that existing constraints or even more constraints as proposed by some other folks, are consistent with historical practice and tradition and moves us further toward constraints.

As to my second point, I do not believe the Fourth Amendment imposes limitations on foreign intelligence as strict as those employed, imposed by Section 702. And let me just briefly explain the two reasons why.

First, it is very clear the Fourth Amendment does not apply to non-U.S. citizens and when they are outside the territory of the United States. And the Supreme Court confirmed this in the 1990 decision of The United State versus Verdugo-Urquidez.

So foreign citizens or the surveillance of foreign citizens outside of the United States is completely unconstrained by the Fourth Amendment.

Second, the courts have confirmed that it's highly unlikely the Fourth Amendment's warrant requirement applies to surveillance of U.S. citizens when they're outside of the United States, especially when the surveillance is conducted for foreign intelligence purposes.

No court in the United States has held

that a warrant is required for a search of a U.S. citizen when they are overseas if that search was conducted for foreign intelligence purposes.

Some courts like the second circuit have even held that no warrant is ever required for an overseas search, while others have relied on a broader foreign intelligence exception.

So there is further details here about the reasonableness, and courts have generally interpreted the Fourth Amendment's reasonableness requirement very generously in favor of the government when conducting overseas searches.

Again, in light of this long history and tradition of the United States conducting essentially unsupervised foreign intelligence gathering without any statutory authority, this is actually the tradition in the U.S. system prior to the enactment of FISA, then more recently Section 702.

So just to conclude, if you look at Section 702, the government faces a complete ban on the intentional targeting of any United States

person reasonably believed to be outside of the United States. And there are other procedural mechanisms, as you know about.

But I don't believe that actually the Fourth Amendment would actually require if there was no Section 702, the Fourth Amendment would require that the government could not intentionally target a U.S. citizen overseas and their communications.

So let me just conclude, I believe Section 702 should be understood as a sensible compromise between privacy interests and the continuing need to conduct aggressive foreign intelligence gathering. Congress has given its blessing to broad-based overseas surveillance that was already occurring pursuant to the President's inherent constitutional power.

Congress has now imposed limitations on those activities that go beyond what I believe the Fourth Amendment requires, but I think that's a small price to pay, and many of us agree, to minimize privacy intrusions into Americans'

overseas communications. And the courts are involved to provide oversight.

This is the type of political compromise and cooperation between different parties and different branches of government that we always wish, we always say we want, and so I think we should applaud it rather than condemn it.

MR. MEDINE: Thank you.

Ms. Levinson-Waldman.

MS. LEVINSON-WALDMAN: Thank you, of course, for having me here. I have a few brief comments and then I hope we'll also have a chance at some point potentially to respond to comments that were made during the first panel or during this panel.

So I'm just going to focus briefly on two primary issues that are reflected in my written submission for now.

First, I know of course that the Board is particularly interested in whether this about collection complies with the letter or spirit of Section 702. And based on the structure of the

statute, we believe that it doesn't.

Briefly, there are two main restrictions reflected in Section 702 on the collection of communications. So that would be the first, the acquisition cannot target U.S. persons or persons known to be within the United States. This is a geographic or nationality and residence restriction.

And second, that the purpose of the acquisition must be to acquire foreign intelligence information. And that's basically a content restriction. What that means is that the content of the communications that can be picked up by electronic surveillance is regulated by the foreign intelligence restriction, while the class of people who are subject to electronic surveillance is regulated by the targeting restrictions.

When communications that are about a target are collected, we believe sort of the what and the who of the collection are conflated, and that that's contrary to the clear structure of the

statute.

And we know that the results of the collection, our intention with the foreign intelligence requirement of the statute, that is, if communications that merely mention certain targets are collected then we know that significant quantities of communications that contain no foreign intelligence information whatsoever are acquired, which would appear to undermine the significant purpose requirement in the statute.

And of course this has been confirmed in the 2011 FISC opinion that was referred to that's been declassified. We learn in fact that the NSA does acquire tens of thousands of wholly domestic communication in the course of conducting that about collection.

And so for those reasons we do think that the about collection is contrary to the meaning and the structure of the statute.

And second, let me briefly mention one of the main contributions I think the Board can

make as part of its review, and I think that some of these questions came out in the first panel, which is to shed more light on some of the ways that Section 702 is being used.

It appears that what we don't know about Section 702, certainly for the public, still outweighs or outnumbers what we do know.

Obviously there will always be things that will be properly classified and kept secret, but it seems that there are many unanswered questions that the Board is in a position to help answer, help shed some light on.

So those questions would include certainly questions about how targets, and selectors, and key words are used. Some of those were answered in the first panel, but I think some of those answers also raised more questions.

There has been the suggestion, the strong suggestion from the 2011 minimization procedures that all encrypted communications can be retained by virtue of their being encrypted, and finding out if that, in fact, is true. And if

not, if the PCLOB can obtain and provide additional information about that provision.

And finally, and this is something that Laura mentioned as well, that domestic communications can be shared with law enforcement agencies if they are reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed.

In addition to raising, I think, a host of constitutional issues at the very least, and practical issues, one of the things that we don't know is whether there are minimum standards for how severe, for instance, such a crime has to be in order to share this information, which of course has been collected without a warrant.

So I hope that the answers to some of these questions also will come out during this process. Again, thank you for the opportunity to address the Board.

MR. MEDINE: Great, thank you very much for your opening statements. I'm going to ask you some questions but any panelist should feel free,

I may ask them to a specific person but anyone should feel free to jump in.

Professor Ku, you talked about the limited applicability of the Fourth Amendment to overseas collections, and maybe, and suggesting there's certainly no warrant requirement and a very generous reasonableness standard.

One question I have is the collections that we're talking about under 702 technically are happening in the United States. That is, the electronic communications provider is in the United States while admittedly the target is outside of the United States. Is that a distinction that you think has any constitutional significance?

MR. KU: That's a great question. I mean I think it reflects the difficulty of this, which is the technology is changing our, the way the Fourth Amendment was interpreted in some of these older cases, right.

So in the classic Fourth Amendment overseas case it was the guy searching through the

house or the apartment physically overseas of the U.S. citizen, or of the phone call that occurred on the foreign networks, right, in the foreign country.

Here we have this kind of weird situation where you have phone or communications sort of transiting through the United States. And I do agree that that might raise a harder Fourth Amendment issue, but I do think that the larger thing to keep in mind is that the geography matters because if there's a foreign person on the other side of the line, so to speak, that's I think in part the way the communication is an international communication. It has different implications for that perspective.

But I do agree that the Fourth Amendment, the territorial aspect of the Fourth Amendment would be less significant in that context.

I think the broader point though is that the courts have been very generous, both domestically and internationally about

surveillance conducted for foreign intelligence purposes.

So even, so the territorial distinction was something that FISA created, because prior to that I think FISA, the foreign intelligence gathering occurred both domestically and internationally, and the fact that it was for foreign intelligence was what mattered.

FISA has created this sort of territorial division, which I think is becoming less important with the changes in the types of communication we have.

MS. DONOHUE: If I may add to that. You know, Professor Ku brings up the exception for foreign intelligence gathering for purposes of surveillance. That's very different from the acquisition of information for purposes of prosecution. And here courts have very clearly ruled that even in cases of national security or domestic security, a warrant is required.

This is U.S. vs. U.S. District Court, a case handed down in 1972 in which there were three

individuals conspiring to bomb the CIA. And the court said that the executive branch, quoting Justice Brownell (phonetic) and others said the court -- the executive branch is not a disinterested neutral observer and cannot be put in the position of having to determine whether a search will be reasonable. They have to seek a third opinion on that.

In Katz as well in 1967, some of the justices in that case, Justice Byron White said, went beyond the decision and said basically we should not require a warrant procedure for the magistrate's judgement if the President of the United States, or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.

And other justices responded very angrily to that statement. Justice William Brennan, Justice William O. Douglas, they pointed out that there was a conflict of interest here. They said, look, neither the President nor the

Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court where the magistrate must be.

The Foreign Intelligence Surveillance Court of Review has also considered whether or not information obtained from FISA warrants could be used in the event of a prosecution.

In the case that brought down the wall in 2002, the court looked to Title I of FISA where probable cause had been established that an individual was a target, sorry, that the target was a foreign power or an agent of a foreign power and said in that case you have this review that has gone on specific to that target by the Foreign Intelligence Surveillance Court.

In Section 702, individuals who may be brought up on criminal charges are not themselves the target of any investigation. No probable cause has been established for their involvement as a foreign power or an agent of a foreign power.

Instead, once the content of

conversations are obtained, then the government may go through, analyze the information and look for evidence of criminal activity, which can then bring them into a courtroom to face criminal charges, and at no point is this warrant requirement, which the court has held for domestic security cases. So here you have a U.S. person on U.S. soil and the court has said in U.S. vs. U.S. District Court, you have to have a warrant in that situation.

So to use the veneer of, well, we're just collecting foreign intelligence and the executive branch has the right to do this under Article II, yes, perhaps the executive branch can gather intelligence but if there are criminal penalties associated then you also need to meet the requirements of the Fourth Amendment for U.S. persons.

MR. MEDINE: I'd like to give Professor Ku a chance to respond, although I can do it on my next round.

MR. KU: Okay. Well, I mean I'm not

going to go through all the cases. And I think that the way I understand this is the way you think about this is the foreign intelligence purpose, right. The foreign intelligence purpose has been sort of an important part about whether there's an exception to the warrant requirement, or if there's a foreign intelligence purpose, sometimes a primary purpose, or a purpose, depending on how you define it. And then there's the, whether that gives a question of reasonableness, where there's legitimate government interests that goes to the reasonableness.

The reason I'm emphasizing the significance of the foreign intelligence purpose aspect of this and the territorial aspect of this is because I do think it's relevant to analysis.

This is, in fact, what's going on here is a collision between our law enforcement and intelligence goals here, right. So the U.S. government is gathering a lot of information for foreign intelligence purposes. It's also using

sometimes that information.

Some of that information is, although not I think so far frequently, leaking into criminal prosecutions. But if we start from the perspective of foreign intelligence gathering, right, this is Article II, this is where we start, and this is something that's largely been unregulated.

What's changed is that the nature of communications have changed so that many of the communications that were essentially gathered unsupervised for foreign intelligence purposes are being sort of routed in a different way so that it falls within, technically speaking, what we might consider a different sort of format, which then looks more like a classic Fourth Amendment case.

But I think that the larger point I'm trying to emphasize here is that this is, there are real Fourth Amendment issues here with respect to law enforcement.

But this is also about foreign intelligence gathering. It's not just a total

sham. It's not as if the government is claiming here that this whole thing is a scheme in order just to gather information for criminal prosecution.

Essentially they're both interests here that are part of this analysis. And that legal analysis with respect to foreign intelligence gathering needs to be considered and it should frame our analysis of what's going on here as well.

MS. BRAND: Thank you. So it's a good segue actually what you said, Professor Ku, because I want to understand, Professor Donohue, what you were saying, and I may not have taken the best notes, so forgive me.

But walk me through the argument, because a second ago you said that you were making a distinction between collection for foreign intelligence purposes and I think you said collection that was focused, was for the purpose of prosecution.

So are you, is it your view that 702

collection is for the purpose of prosecution?

MS. DONOHUE: It's one of the two stated purposes for which the information can be retained once it is collected. So it can be --

MS. BRAND: But that's different. But I'm asking about you said collected for the purpose of prosecution, I thought. I mean what is, I guess what I'm trying to get at is, is this distinction between foreign intelligence purpose and criminal purpose relevant at the collection stage only, or at all stages, or what? Help me understand what you're talking about.

MS. DONOHUE: Yeah, so in the previous panel Brad addressed this point. He mentioned that in the context of it's the moment at which the information's obtained that a search occurs, right.

So if we do our Fourth Amendment analysis at that point, then the moment at which you're obtaining the wiretap evidence is the search, at which point you would require a warrant under these.

And I believe Professor Ku's point is, no, you don't need a warrant if it's for foreign intelligence purposes at the moment you acquire the information with the international nexus to it. And he's citing Verdugo-Urquidez where there was no nexus to the United States and a search occurred overseas.

The problem is in the case, and this gets back to my first point, which I apologize if I spoke too quickly at the beginning of the panel, which is with regard to the targeting. If it is not just information to or from the target, or held by the target, but any information about or relating to the target.

And here, it's interesting, I was a little bit confused by the earlier panel because according to the actual documents the NSA has released, the NSA can actually use computer selection terms and other information such as words, or phrases, or discriminators to scan content.

So if it can collect all of the

international communications and then scan the content of those communications, then I would argue that is a search for purposes of the Fourth Amendment at the point of collection.

MS. BRAND: But let me get to this distinction though between foreign intelligence and a criminal purpose, because 702 requires not only that the collection be a non-U.S. person abroad but also that there be a foreign intelligence purpose, that the information be reasonably believed to be, to collect foreign intelligence. I'm not quoting the statute.

But doesn't that statutory requirement suggest that it has to be for a foreign intelligence purpose? And it might also then collect evidence of a crime, which then there are procedures for what to do with that information.

But it seems like you're suggesting that you think that the collection itself is for a criminal purpose, and that's what sort of piqued my interest and I wanted to understand what you were saying there.

MS. DONOHUE: Sure. So to push on this a little bit, under FISA to be a foreign power one is not a U.S. person, right, one is a foreign power or an agent of a foreign power. Not all of the agents of a foreign power require criminal showings, but many of them do.

So to say that this is purely a foreign intelligence purpose when an individual can be targeted based on being either a foreign power or an agent of a foreign power, in which case there is criminal activity involved and there may be the element of criminality from the outset. So it's not as though criminality is not an aspect of the foreign intelligence gathering generally.

MS. BRAND: Professor Ku, do you have -- Jameel, it looks like you wanted to respond.

MR. JAFFER: Well, I was just going to speak to the foreign intelligence exception more generally, if you want to pursue this.

MS. BRAND: Go ahead. Go ahead.

MR. JAFFER: Well, so I just want to caution the Board about starting from the premise

that there is in fact a foreign intelligence exception to the warrant requirement. The cases in which courts have held that there is such an exception predate FISA. There's arguably one exception to that, but the vast majority of them predate FISA.

And so their rationale has been undermined by practice under FISA over the last thirty-five years. The rationale for those cases was in large part that the courts might not be capable of overseeing collection or surveillance for foreign intelligence purposes. But the courts have been doing precisely that now since 1978.

But even if you accept that there is in fact a foreign intelligence exception to the warrant requirement, you have to ask the question of how broad that exception is.

And all of those cases, those pre-FISA cases, involve cases involved situations in which there was probable cause to believe that the target was a foreign agent, the surveillance was approved personally by the President or the

Attorney General, and the primary purpose of the surveillance was to gather foreign intelligence information.

And Section 702 doesn't include any of those requirements. So no court has ever approved a foreign intelligence exception to the warrant requirement that is broad enough to read Section 702. Section 702 is a broader statute than any foreign intelligence exception recognized so far would allow.

I think that it may also be important to emphasize that concluding that the warrant requirement applies doesn't mean that the government has to get a warrant before surveilling legitimate foreign targets. It doesn't mean that in order to surveil, you know, some suspected terrorist outside the United States the government necessarily needs to get a warrant.

But at the very least it means that the government needs to take reasonable measures to avoid acquiring Americans' communications without warrants.

It means it has to not acquire them in the first place where it cannot acquire them.

When it does acquire them, it has to destroy the communications that it acquires relating to U.S. persons.

And when in narrow exceptions it retains those communications, there should be a back-end warrant requirement so the government doesn't access Americans' communications without a warrant. That's what compliance with the warrant clause would mean.

MR. MEDINE: Ms. Cook.

MS. COLLINS COOK: So thank you all for coming. I find these panels to be incredibly helpful and informative.

Ms. Donohue, I would like to -- Professor Donohue, I apologize, I'd like to follow-up on something you mentioned at the very end of your opening remarks, and that's your position that 702 raises First Amendment concerns.

I think it's clear from my previous separate statement on our 215 report that I don't

necessarily approach the First Amendment analysis the same way, but what I would find helpful from you is if you could just describe your approach to when the First Amendment would be implicated, when concerns arise, and when something would be unconstitutional based on First Amendment concerns.

So for example, would a traditional wiretap raise First Amendment concerns, and would it potentially be unconstitutional under First Amendment concerns?

Would a traditional grand jury subpoena for bank records or credit card statements that could reveal payments to lawyers or payments to various charities or associations, would that raise First Amendment concerns? Would it be unconstitutional under the First Amendment?

So if you could just walk me through on the spectrum where you're finding concerns and where you're finding violations.

MS. DONOHUE: Sure. And just to return back to Ms. Brand's point, I agree with Jameel on

the analysis about what point it would kick in for a warrant requirement is the point at which it's either about the information, because I feel like I didn't quite answer what you were asking me and I want to make sure that I do, I answer it.

It's the point at which you're getting information about that particular individual, which is a different target, and then you analyze that information, then at that point I would believe that the Fourth Amendment warrant requirement would apply.

Okay, so in response to the First Amendment question, so the courts have recognized that there is a close link between the First and the Fourth Amendment. And I frequently find whether it's in remote biometric identification systems in view of public space and facial identification, you know, that there is a First Amendment context there as well. So it tends to be in the shadows in the room.

In this particular context, the way that I see it present is with regard to the target

that is in the statute. It's very clear that the target cannot be selected --

MS. COLLINS COOK: I'm sorry, can you actually answer the question that I had posed, which was, for example, starting with a traditional --

MS. DONOHUE: Oh, yeah, so I do not see a traditional wiretap as implicating First Amendment. I do not see --

MS. COLLINS COOK: Why?

MS. DONOHUE: Because --

MS. COLLINS COOK: Even though it could, for example, reveal the fact that I belong to the ACLU, or I have called my attorney, or I'm discussing, you know, private contents and communications. So why not?

MS. DONOHUE: Because there's a balancing that occurs with regard to the element, in this case of probable cause that you have committed, are committing, or are about to commit a crime under Title III, in which case having gone before a neutral, disinterested magistrate, a law

enforcement officer says, oh, no, I suspect that Professor Donohue is engaged in this bad activity. And I think that that balancing test basically takes that situation out of a First Amendment context.

MS. COLLINS COOK: So let's take a grand jury, and then a pen register trap and trace. So a pen register trap trace, there's definitely no determination, no probable cause. So does a traditional pen register trap trace, which would reveal potential phone calls to the ACLU, to my lawyer, very private, the existence of potentially private conversations, does that violate the First Amendment?

MS. DONOHUE: Again, with prior judicial approval and review, no.

MS. COLLINS COOK: Okay. So let's take a grand jury subpoena which can be issued by a prosecutor. So in the absence of beforehand judicial review, does that violate the First Amendment?

MS. DONOHUE: No. I would say --

MS. COLLINS COOK: So what's the factor --

MS. DONOHUE: Well, it's the same for administrative warrants, I would say in the case of administrative warrants. Here's where the tipping point is for me with PRTT, let's take Section 215 as kind of a bulk metadata collection program, or Section, what is it, 402, right, for these bulk collections of pen register trap and trace type information.

When you have the bulk collection of information in a way that changes the political discourse in society, then I think you have a First Amendment question that arises.

MS. COLLINS COOK: Okay. So is if there is a perception that there is a change in political discourse, then you have a concern about a First Amendment? It's not necessarily prior judicial review, particularized probable cause?

I'm just struggling to understand, you know, at what point there's a First Amendment implication and at what point there's a First

Amendment violation, because to me, I think it's a bit of a sea change to look at either traditional or really these FISA authorities as violating the First Amendment. I do think that that's a fairly novel approach.

MR. JAFFER: But to be fair -- to be fair, the distinction between individualized surveillance and bulk surveillance is also a bit of a sea change. And so I think the question is whether the bulk surveillance, the fact that the government is now engaged in bulk surveillance, I mean I understand that there's some dispute over the vocabulary, but the fact that the government is engaged in bulk collection or bulk acquisition of this information makes the First Amendment relevant in a way that it perhaps wasn't relevant in the context of individualized surveillance of the kinds that you were describing.

I mean I think that your question perhaps goes more broadly to the question of incidental overhears, you know. When the government defends Section 702, one of the

government's defenses is that all of this information is, about Americans is overheard incidentally.

You know, I go into this in a little more detail in my written submission, but I don't think it's fair to call this kind of collection incidental in any conventional use of the term. The collection of Americans' information is entirely foreseeable, and in fact, it was the purpose of the statute.

If you look at the statements that administration, then Bush administration officials made to justify the statute or to advocate for the statute, they were quite forthright about the purpose of the statute. And the purpose in their view was to give the government broader authority to collect information, collect communications between people outside the United States, and people inside the United States.

And obviously there's no illegitimacy to the government's interest in collecting those communications. The question is whether there are

sufficient safeguards in place, but that's why I say that incidental is probably the wrong word.

But if the government is relying on the incidental overhear cases from the Fourth Amendment context, those cases were, involved very different contexts. Those were cases in which the surveillance was individualized. It was based on a probable cause warrant.

The scale of the surveillance of the incidental collection was much different. And the fact that there was judicial oversight at the front-end provided a kind of protection for incidentally overheard people that doesn't exist under a statute like 702.

MR. MEDINE: Let's give Jim the chance to ask some questions, then we can come around.

MS. DONOHUE: Okay.

MR. DEMPSEY: Thanks. Thanks to the witnesses.

A question for Jameel and for Rachel on the abouts. What actually is, quoting the words of the statute, what is the strongest textual

argument against about surveillance?

Because the statute says the targeting of persons, never really refers to even the collection of communications or interception, etcetera, so if you're collecting something about somebody, isn't that almost paradigmatically targeting the person? Where's the text?

MS. LEVINSON-WALDMAN: I mean I think one of the -- right, there's obviously ambiguity in the statute in part, and this is one the things that I mentioned in the written submission is that target isn't defined.

And I have to say some of the answers in the first panel, which answered some questions about target and selectors, I think also opened up new questions.

I do think the strongest statutory argument, literally looking at the language, is what the statute talks about.

So it says here, literally just looking at 1881 A, subpart A, Attorney General and Director of National Intelligence may authorize

jointly the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information.

So as I say, you sort of see implicitly, but I think you do see implicitly these two sort of halves of the targeting requirement, the foreign intelligence requirement and this kind of nationality and geographic restriction, and that when what you're doing is collecting about communications, what you're doing is kind of adding together, you're kind of conflating, you're morphing together these different parts of the statute so that the targeting has usually been literally thinking about the facility that's being used --

MR. DEMPSEY: Excuse me. The government has determined that a person is outside the United States and that collecting information about that person will yield foreign intelligence.

MS. LEVINSON-WALDMAN: Well, but I think that may be what's suggested by the about collection, but I think the foreign intelligence

determination is a separate one, right.

The government identifies these targets or selectors which have generally been to or from. And in fact we know, especially from Judge Bates's opinion that thousands, tens of thousands of communications are collected using the about targeting, the about collection, that are wholly domestic, that have no foreign intelligence value, which I think undermines an argument that there has been some determination of foreign intelligence value there, because to some extent the results are sort of speaking for themselves.

MR. DEMPSEY: Because then you would be questioning the legitimacy of the to and froms because they only do abouts about people that they also do to and froms, so you can't say that the foreign intelligence determination of the abouts is illegitimate because then you call into question the to and from.

MS. LEVINSON-WALDMAN: Well, but I think the to and from is pretty clearly contemplated by the statute, right? You target a

person, you are trying to find communications to or from them, understanding that those will have foreign intelligence value.

MR. DEMPSEY: Let me go to Jameel. Jameel, what is the best textual argument against abouts?

MR. JAFFER: Right. Well, let me first I think agree with what I think Rachel was saying at the outset, which is that the statute I don't think explicitly forecloses about surveillance or explicitly authorizes about surveillance.

But I think a fair assessment of the statutory structure and some of the statutory text leads to the conclusion that about surveillance was not contemplated by Congress. And I'll answer your question.

MR. DEMPSEY: The text, yeah.

MR. JAFFER: So here are a few aspects of the statute that I think show that Congress was contemplating, that the target would, himself or herself, be the person whose communications were acquired.

First, a definition of electronic surveillance. It says the acquisition of the contents of any wire --

MR. DEMPSEY: This is not electronic surveillance. 702 explicitly does not cover electronic surveillance.

MR. JAFFER: Well, I think that the point I'm making is relevant nonetheless.

MR. DEMPSEY: Electronic surveillance definition is irrelevant to 702. It is not -- 702 does not regulate electronic surveillance.

MR. JAFFER: I think the point that I'm trying to make is just that the entire statutory scheme, both FISA and the FAA, contemplate that the person who is the target will be the person whose communications are actually acquired.

If you look at the definition of aggrieved person, for example, which does apply in the FAA context, aggrieved person to implicitly contemplates that the person who will be raising the claim as an aggrieved person is a person whose communications are actually acquired.

And in fact, if you conclude otherwise what you are concluding is that the target would be an aggrieved person even if his or her communications weren't acquired, which I think is a nonsensical conclusion and one that the government itself would reject.

But I think it follows from accepting that about surveillance is contemplated by the statute.

And if I could just make a sort of broader point about about surveillance, we have sort of combed through the legislative history for discussions of this kind of surveillance, and it's possible we overlooked something, but we have not found any exchange in the legislative history around the FAA that suggests that Congress was contemplating about surveillance.

To the contrary, when people discuss, when legislators discuss the kind of surveillance that would take place under the statute, they discuss surveillance of the target.

And even on the government panel this

morning one of the panelists used the example, bad guy at Google.com, you know, which again is suggesting that the surveillance that's going on is of the target himself or herself.

And in defending the statute before the Supreme Court, the Solicitor General and the Justice Department more generally characterized the statute as one that allowed the government to collect targets' communications.

So you know, I think that this is an entirely a foreign concept, foreign to the legislative history and foreign to the text of the statute.

MR. MEDINE: Thank you. Judge Wald.

MS. WALD: Let me pick up on the about thing and pose one of those terrible hypotheticals. If you had a to and from, you had a targeted, a legitimately targeted person and in the process of collecting information you got, you came across this email between, I'll be facetious a bit, the grandmother of one of them to the grandmother of somebody else saying something

along the lines of, my grandson was talking to me and he was telling me all about this wonderful service he did by plotting, I'm using an extreme, plotting to blow up a facility kind of thing, I mean how would you take care of that situation where you had it between two people who are not the to and froms? You wouldn't ignore it, would you, or would you? I mean how would you handle that if you had no abouts?

MS. DONOHUE: I'm not sure whom that's directed to.

MS. WALD: I don't care.

MR. MEDINE: Who would you like it directed to?

MS. WALD: What?

MR. MEDINE: Who are you asking?

MS. WALD: Well, the two people who've talked about what about abouts, Mr. Jaffer and Ms. Levinson-Waldman, I think.

MR. JAFFER: Well, I'm not a hundred percent sure I understand the question. The question is, you know, if you were conducting

about surveillance and you come across evidence of a terrorist plot, do you really expect them to ignore it? Then no, I don't, you know.

But that's like asking, you know, if the government breaks into a home unconstitutionally and finds evidence of a terrorist plot, do I expect them to ignore it? I don't.

But we still need to ask the question what are the proper limits on the government's surveillance authority in the first place, and I think that we need to draw those limits in a way that's consistent with the Constitution.

I'm not sure that I'm answering your question.

MS. WALD: Well, you are except that I'm puzzled, too. I'm not sure I know the answer where, as I say, you had -- maybe that's an extreme example about where they have a plot, but where there's actually some foreign intelligence information which even everybody would agree had some relevance to a legitimately targeted

individual, and it's right there, and it's picked up.

MS. LEVINSON-WALDMAN: Then I think I would echo Jameel's points to some extent and sort of elaborate to say that I do think that there are always hypotheticals, presumably for any of these programs, for Section 702, for Section 215, for other collection programs that are going on where there could be some piece of information out there that might be useful that would be collected by a program.

I think it's dangerous to build surveillance programs and to think about the constitutionality and the practicality based on hypotheticals, and especially when we know that there is significant over-collection that occurs and significant collection of Americans' communications.

I think the hypotheticals are, may need to be thought about, but I don't think that they can drive how we think about the constitutionality and the statutory implications of the collection.

MS. WALD: In other words, you or anybody over there wouldn't consider if that happened, some other means that the government might have to take that about information and go to somebody, to some authority and say can we keep this, can we use this, etcetera, etcetera?

MS. DONOHUE: So what I'm a little bit confused about, and I did hear the previous panel say, oh, well, there would be all sorts of procedural implications if we had to return to a judge on the Foreign Intelligence Surveillance Court to get approval to do further monitoring.

What I'm a little bit confused about is if that information was appropriately obtained in the first place and it indicates that other people are implicated, why they wouldn't go back for a Title I electronic search and they would have what they need for that?

MS. WALD: Well, if it's two grandmothers, they're probably not -- they're just chatting. They're probably innocent. All I'm saying is I guess the only reason I raised it is

I'm trying myself to figure out are there not some gray areas here, and wondering if you had any solutions short of about authority which you find is too broad, and completely ignoring it?

But let me not use up my whole five minutes. Thank you.

I did want to ask you about, as you know, the President's review commission said they wanted to see a warrant, an actual, go get a warrant for probable cause before you could search the data using a U.S. person indicator.

My question to you is, and we've heard some reasons why they think that's very onerous, including the fact that the President's review commission's recommendation was it had to be a probable cause warrant that the person was about to commit something, do bodily injury, or about to commit some terrorism crime.

My question to you is if you think there are legitimate, and you do, problems under the Fourth Amendment with using U.S. person indicators to surveil the PRISM data, would

anything short of a probable cause warrant such as they recommended satisfy you, i.e., I'm just throwing this out, you know, having, going back to, say, to the FISA court and having them look at it to see if it, either post or pre, before they used it, approving this so-called, you know, selector, etcetera, that was in fact a reasonable cause to believe that the person had information or didn't have information?

MR. JAFFER: I don't think that would be sufficient. I think that you need a warrant at the back-end and --

MS. WALD: But what kind of a warrant warrants --

MR. JAFFER: A warrant based on probable cause and --

MS. WALD: Probable cause of what?

MR. JAFFER: Well, so I think it could be foreign intelligence probable cause, although I hope that the panel will, that the Board will think about the scope of the definition, the definitions of foreign agent, foreign power, and

foreign intelligence information.

But I think that foreign intelligence probable cause could be sufficient for that particular process, or obviously criminal probable cause.

But I also just want to say that I don't think back-end procedures alone are enough, no matter how strong they are. And I think that, you know, I know that the Board can't talk about the Washington Post report from yesterday, but if you just take it as a kind of hypothetical, you know, if you accept that back-end procedures are enough and that we'll focus solely on the protections on searching, and dissemination, and analysis of information in the government's hands, there's nothing to prevent the government from recording every phone call, copying every email, creating a permanent record of everybody's movements, associations, and communications. And the only question we'll be asking is when can the government access it.

But the creation of that kind of

massive database will have huge implications for the way that ordinary people operate in society, both the way that they interact with one another and the way that they interact with their government.

People who believe that the government is surveilling every movement and every communication, believe justifiably that it's doing it, will act differently. They won't go to controversial websites and they won't engage in controversial communications that are necessary for any democracy.

MS. WALD: I'll save, I know my time is up. I'll wait for the next round. I have another question.

MR. MEDINE: I want to go back to that back-end searching, basically the U.S. person searches, and this really is two questions.

One is the government panel asserts that this is lawfully obtained information and therefore should be permissibly used without any further Fourth Amendment implications. And why

that's not a persuasive argument.

And then two, if it's not persuasive, what is the procedure that you envision? And again, I think it's different from Professor Donohue where you're using that U.S. person information to get more information. You're just saying let's use the information we've already collected under some other, under authority for, say, criminal purposes or foreign intelligence purposes.

So I guess it's two parts. Why isn't is already legally usable? And if it's not, what procedure would you apply to access it? And that's to any panelists.

MS. DONOHUE: So as a statutory matter I would come back to the burden of proof with regard to whether that information that's being collected on targets, they are indeed U.S. persons or non-U.S. persons and located outside the United States.

So here the statute is silent, and I share Mr. Dempsey's textual analysis of the about

question. I think the statute is silent there as well. But in regard that the statute does say where you know that somebody is a U.S. person, you know, you have Sections 703 and 704 that you have to operate under.

MR. MEDINE: Again, we're not targeting the U.S. person, we're targeting a non-U.S. person, and Congress clearly knew that at the other end of that phone call could be a U.S. person and still authorized that kind of collection without a warrant.

And the question is, why isn't that sufficient to then say, okay, this information was lawfully collected, now we can do searches based on it?

MS. DONOHUE: Because it isn't certain that the person on whom you're collecting the information really is a non-U.S. person. So the burden of proof on the NSA is to say, to establish that this individual is a non-U.S. person.

But in fact, so the assumption that all

the collection that's going on currently is of non-U.S. persons I think is an erroneous one. And it's one -- and the reason why I think it's erroneous is because the NSA is under no obligation to check and see and make sure that that individual is not a U.S. person.

To the contrary, they have in their documents they say, well, they may check these databases, they may check these other databases. There's no obligation that they do so.

Mr. De in the previous panel referred to the totality of the circumstances type tests that say they have two strikes against, four strikes for, they look at everything. There is nothing that obliges them to then go back and dig up more information to find out in that particular circumstance.

And not only that, but actually if you look at the requirements for what is required to positively identify, to conclusively determine it in the minimization procedures, the bar is actually significantly high.

It means that you know their name, you know their title, your know their address, you know their personally identifiable information in the context of activities conducted by that person that are related to that particular person. A reference to a brand name, manufacturer's name, Monroe Doctrine, etcetera, that's not sufficient.

So not only are they under no obligation to establish that but in order to establish it, it's a very high bar. So it's not clear to me that that information is lawfully collected in the first place.

MR. MEDINE: Ms. Levinson-Waldman, do you want to weigh in on that?

MS. LEVINSON-WALDMAN: I think the other thing I was going to add, if I'm understanding the question correctly about why is it not okay to do searches on information that's been lawfully collected, I think there's also an element of bootstrapping.

So that it was lawfully collected for a purpose, for a foreign intelligence purpose, and

that you're right, of course Congress knew that U.S. person information was going to be incidentally collected through that process, but then there are these minimization procedures.

And so kind of almost bypassing those procedures and allowing that body of information to be collected without meeting a fairly high bar, some kind of probable cause warrant seems like kind of going back and bootstrapping your way into that information in a way that is very different from searches of, I think, any other, almost any other body of lawfully collected information, because the standard for which it's obtained, that foreign intelligence standard and purpose is so different.

MR. JAFFER: I mean I actually think there are two kinds of bootstrapping. The first is pointing to the fact that foreigners outside the United States lack Fourth Amendment rights in order to collect huge volumes of communications to which Americans are a party.

And then the other is pointing to the

foreign intelligence purpose to gather information which is then later used in criminal prosecutions. So that's to state the problem. It's not a solution to the problem, but I think that's where the concern comes from.

MR. MEDINE: Professor Ku.

MR. KU: If I could just add, I mean I'm not sure that's bootstrapping. I think that's sort of the purpose, right. The purpose is -- it's not that they're not also collecting it for foreign intelligence purposes.

It's also true that if in the old days they came across a letter from an American person to a foreign person, it seems unlikely to me that because an American sent the letter that means they can't -- but they lawfully obtained the letter, it's unclear to me why they couldn't use that letter.

And so I'm a little, possibly it's bootstrapping, but it's, there's a long history of going after foreigners and doing foreign surveillance.

I'm not sure that -- I think the only difference I think is technology does make it easier for it to flip back into the states, but I'm not sure that fundamentally this is a really different thing.

MR. MEDINE: Thank you. Ms. Brand.

MS. BRAND: Thank you. Well, it seems like there are some fundamentally opposing world views about the Fourth Amendment on the panel, and I want to, I mean this Board is not going to move Fourth Amendment law. So I want to get to what you think the law is and what you think the law should be, because I think there might be some conflation of those two things going on here.

First of all, Professor Ku, thank you for submitting your comments this morning, your written comments. I haven't had a chance to read them yet so I just want to ask you a question to make sure I understand where you're coming from.

You talk about inherent executive authority to conduct surveillance abroad or even of non-U.S. persons abroad. In your view, does

that inherent executive power operate alongside the Fourth Amendment, or irrespective of the Fourth Amendment, or does that create an exception to the Fourth Amendment?

MR. KU: Right, no, I don't think it creates an exception to the Fourth Amendment. It operates within the constraints, whatever they might be, of the Fourth Amendment.

But I would like to point out that historically this -- I mean so just to clarify. The reason I raise this, it goes to the point that historically the U.S. government as operated without statutory authority to conduct foreign surveillance. It's been, the power was granted, was thought of as coming from the Constitution.

So the statutory scheme has not been thought of as necessary to authorize the type of intelligence gathering that's going on.

Now the Fourth Amendment does apply, but as I also emphasized, it hasn't always applied. It didn't originally was thought of to apply at all, even to U.S. citizens overseas, but

I think we understand that the courts have come around to view that it does apply to U.S. citizens overseas. But I think it still has a limited impact compared to the way it applies for purely domestic searches. So that's how I would analyze that.

MS. BRAND: And how does it apply to purely domestic searches where there's a purpose of foreign intelligence gathering?

MR. KU: Well, I think that -- well, here I think that, you know, it does. The Fourth Amendment has been interpreted in recent cases to be a much more robust protection for searches domestically, although even in some of those cases, right, a warrant has not been required or the exception to the warrant requirement has been found for foreign intelligence purposes. So it still continues to exist within the domestic sphere.

I would say that for me, at least my understanding is a lot of this has been supplanted by the FISA system. The rise of the FISA system

has to some degree made the Fourth Amendment analysis a little bit less onerous because what's been happening is that everything's been funneled through the FISA system and the challenges to the FISA system has not been sort of as robust.

I think if we hadn't had FISA maybe we'd have had more cases that would have clarified exactly what the Fourth Amendment limits on domestic foreign intelligence searches would be. I do think that it applies more strongly to domestic searches and I think it has more significance.

But I do think that ultimately the foreign intelligence exception to the warrant requirement is a reasonable one that does need to be respected. It has a long tradition in history.

In my view, really FISA is sort of on top of that to add additional privacy protections that I think Congress has judged, and probably rightly so, we need. But I'm not sure the Fourth Amendment itself standing alone would necessarily require all of the sort of procedural limitations

and minimization protections that we have.

MS. BRAND: Okay. And Jameel, can you very briefly, because I have another question for you, you do not think there is any foreign intelligence exception to the Fourth Amendment? Is that what I heard you say earlier?

MR. JAFFER: I don't think that there's any foreign intelligence exception broad enough to justify 702, and no court has --

MS. BRAND: But there is -- I mean I guess what I'm trying to get at is, do you think that the Fourth Amendment applies equally to collection for the purpose of foreign intelligence gathering as it applies to collection when the purpose is to gather evidence of a bank robbery, for example?

MR. JAFFER: I think that there are certainly narrow circumstances in which the courts have held that there is a foreign intelligence exception.

Again, those cases predate FISA, and so you know, you have to evaluate whether those cases

survived the thirty-five years of experience under FISA.

MS. BRAND: Okay. And then you referred earlier to, I think you were referring to, well, you're referring to 702 generally as large scale collection. I'm not sure if you were including both upstream or PRISM in that assessment.

But if you were here for the first panel and if you take the government's facts as they stated them to be true, what about that program strikes you as large scale? What's your justification for that description?

MR. JAFFER: Well, so two responses to that. The first is I think it's important to draw a distinction between statutory restrictions and executive restraint. So there's a question of what the statute allows and then there's a question of how the government is implementing it.

Obviously I know much less about how the government is implementing it than I do about what the statute on its face allows because I can

read the statute and I have access to only a portion of the government's documents.

But then as to, you know, whether it's large scale collection or not, I think that the problem is that everybody is using these words in different ways. The panelists this morning said that they weren't drawing a distinction between acquisition, surveillance, and collection. But their own documents do draw a distinction.

If you look at USD 18, for example, which is the Defense Department's implementation of the executive order on intelligence collection, it draws a distinction between electronic surveillance and acquisition on the one hand and collection on the other.

And collection involves the tasking of that, or tasking of communications, whereas electronic surveillance and acquisition do not.

And so, you know, we have always thought of this, putting the vocabulary to the side for a second, we've always thought of this in two stages. There is a kind of, just to -- there

is a kind of, you might call it scanning, you might call it collection, but there's a kind of large scale acquisition of data, and then there's the government tasking that data, and then there is the government's tasking that data with selectors.

So to be a little more concrete, if the government installs on a switch somewhere installs a device that either diverts all of the communications or a large portion of the communications, or scans a large portion of the communications, we would call that bulk collection.

I'm not sure that anything turns on vocabulary but we should all make sure we're talking about the same concepts.

MR. MEDINE: Ms. Cook.

MS. COLLINS COOK: Actually that was right at the top of the last piece. I think we've used, and in this conversation alone we've used scan, inspect, acquire, collect, access.

And so I guess my question is, if you

have access, so in your hypothetical you've installed something that gives you access to this stream of communications, is that a seizure or a search for the purpose of Fourth Amendment analysis in your view?

MR. JAFFER: Well, I think it would depend what you were accessing. You know, the question would be have you invaded a reasonable expectation of privacy?

But we have taken the position that, for example, the bulk accessing of telephone metadata is an invasion of a reasonable expectation of privacy, and we would certainly take the same position with respect to the bulk acquisition of telephone calls or emails.

The MYSTIC program, again, just discussing it as a kind of hypothetical, that program in my view involves the bulk collection of telephone calls, voicemail messages, and telephone calls, even if the government doesn't access more than a small proportion of them.

MS. DONOHUE: May I add something to

that just very quickly? I was a little bit confused in the earlier panel because on the one hand they were saying this is a very limited program. On the other hand they say that this SIGAD is the most used NSA SIGAD.

The slides that have been released say it draws from Microsoft, Google, Yahoo, Facebook, Paltalk, YouTube, Skype, AOL and Apple, that it gets voice over Internet protocol, email, chats, all this information, and it's hard to square that.

And what they say is the value of the program, with its limited nature --

MS. COLLINS COOK: I'm sorry, can we talk about -- I appreciate your desire to talk about the previous panel but I had a specific question out that I'm really trying to understand the panelists' view on when the Fourth Amendment is implicated and how.

And so if it's under your hypothetical if you have the acquisition of all phone calls from a country with subsequent access, at what

point would the Fourth Amendment attach?

MR. JAFFER: I would say certainly the moment you put it in your databases, by that moment the Fourth Amendment has attached.

MS. COLLINS COOK: So flipping that, if it's access to a wide swath of communications but acquisition into the government's possession or control, when would the Fourth Amendment attach?

MR. JAFFER: I'm sorry, but I've lost track of the difference between access and acquisition.

MS. COLLINS COOK: And this is part of the, I think you've used scanned, but some ability to review a stream of communications and pull, filter, something to that effect.

MR. JAFFER: Right. The scanning or the filtering would implicate the Fourth Amendment in my view.

MS. COLLINS COOK: That's helpful. I wanted to follow up on a different set of questions and just close the loop.

If the determination was made that the

acquisition of the information pursuant to 702 was lawful, it's lawfully acquired information, would you still take the position that a subsequent search, and by that I mean a query using a U.S. person identifier, would need some sort of probable cause determination, that there would be a separate Fourth Amendment analysis?

And can you explain why? I guess is this because there's a view that there's a lack of particularity of the front-end and therefore you have to have subsequent some particularized finding?

MR. JAFFER: Yes.

MS. DONOHUE: That would be my position as well.

MS. COLLINS COOK: Okay. One question for Professor Ku, if I could. We've heard that 702 is silent, I think it's fair to say on the precise question of abouts. There are some structural arguments here and some purpose arguments that you can look to, but it's silent.

In view of the evolution of our

understanding of Article II of FISA, how would you as a constitutional matter assess a silence in 702? Because Title VII is both an authorization and a restriction on Article II authority, so.

MR. KU: Right. So I think, I don't know if I have any sort of grand insights on the purely textual analysis, although I do think that the constitutional background is what can help us here with respect to, if we understand where we're coming from can help us analyze this.

If we understand that constitutionally that the U.S. government was engaged in broad searches prior to the enactment of 702 then you have to sort of think about, well, to what degree.

This is not really about authorizing, this is really about restricting, imposing restrictions on what I think the U.S. government had the authority to do prior to the enactment of the statute.

And so if you look at it from that perspective then, if it doesn't, the silence or the lack of clarity or specificity would then I

think lead me from that perspective to suggest that the President retains that power.

I would analogize this a little bit to the point that was made in the earlier FISA statute, how they excluded radio completely from the original FISA, radio communications, they just said nothing about it.

And there are a lot of people that argue that was on the assumption that most of the foreign intelligence was radio in 1973 and that the President would continue going on gathering as much radio signals intelligence as he could. And then at a certain time, no one used radio anymore.

But the point is that if you add the restriction in the statute it doesn't -- the previous or the other authority the President has to conduct the surveillance should in theory continue, and I think would likely to continue here too, assuming he had the authority prior to the enactment.

MR. MEDINE: Mr. Dempsey.

MR. DEMPSEY: A quick comment and then

a question. Going to the definition of distinctions between collect, acquire, etcetera, my comment is we really have to take yes for yes and no for no and move on. The government has said, to my mind totally clearly, they are not relying upon the USD 18 concepts in implementing 702, so I think that we just have to move on from that. That's my comment.

My question is the following, and this is for Jameel or anybody, Rachel, in terms of the querying of data otherwise lawfully acquired, what is the best case law that would limit the proposition that data lawfully acquired can be subsequently queried without limitation?

MR. JAFFER: Well, so on your comment, I think you're certainly right that the government said on the panel earlier today that they were not relying on the distinction, any distinction between acquisition and collection.

But I think that the government also acknowledged that it was engaged in about surveillance, and to engage in about surveillance,

my understanding is that there is no way to engage in about surveillance without inspecting in some sense every communication within the universe of those that you are monitoring or surveilling. There's no way to do it.

Now you can call that bulk collection or you can call it something else, but that scanning of every communication in a particular universe raises constitutional issues, and if all you're saying, Mr. Dempsey, is we should just address those constitutional issues, then I entirely agree.

MR. DEMPSEY: So now as the querying of otherwise lawfully acquired communications, and let's take, you know, if I steal your computer, I think, and then I give it to the government, the government lawfully acquired it. I may have stolen it. Or certainly in the Title III context the government lawfully acquires, or in the normal search and seizure context, or in the voluntary disclosure context, where is there case law limiting the proposition that lawfully acquired

information cannot subsequently be queried essentially without prior authorization, without meeting any threshold? What is, is there any case law limiting that?

MS. DONOHUE: So we're starting to see cases come out of border security issues where computers -- border security issues, and I'd be happy to send you the names of the cases afterwards, where computers have been lawfully seized under customs laws but then they cannot be searched for all of the information on them because of the privacy implications that are involved and lack of a sufficient nexus to the suspected criminal activity.

So those cases might be one source that you would look to in a new age of data where so much information is available.

MR. JAFFER: You know, I think it's important to ask the question the other way around as well, which is, you know, where is there case law showing that the Constitution is indifferent to the government collecting huge

volumes of communications without any individualized suspicion or particularity, and then sort of bootstrapping its way into free rein or --

MR. DEMPSEY: Again, if we're in a situation, I'm just trying to pose the situation of let us assume, just let us assume that the collection was lawful.

MR. JAFFER: I'm not suggesting for these purposes that the collection was unlawful. What I'm saying is that the collection here is different in kind from the kind of collection that the courts have been concerned with in other cases involving the use of information lawfully acquired. You know, it was important to those cases not just --

MR. DEMPSEY: So then the license plate readers, the information collected by the license plate readers is lawfully acquired and then the government can subsequently query that license plate database. I mean that's standard procedure.

MR. JAFFER: I'm not sure that it's

established with any certainty that the bulk collection, that the querying of a database of bulk collected license plate reader information doesn't raise Fourth Amendment concerns, and I think that that's still an open question.

MR. DEMPSEY: Well, I'm looking for some cases. Professor Donohue has some border cases --

MS. DONOHUE: I'd be happy to send you the border doctrine cases.

MR. DEMPSEY: That may be relevant. I would welcome any other cases limiting that proposition.

MR. MEDINE: Judge Wald.

MS. WALD: This is probably an unfair question but I'll ask it anyway. Given the fact that the grievances about 702 as it operates today have included a whole series of things, one we didn't discuss here but it's been raised in written stuff is the lack of FISA review of particularized targeting designations. I know it's allowed by the statute, but nonetheless the

capture and use of incidental U.S. information to search database, the use and retention of the U.S. information.

But my question is, if you had to focus on one or maybe two important changes that you would like to see made now in 702, what would they be? Very quickly, anybody that wants to answer it.

MS. DONOHUE: I would say limiting the information to, or from, or held by the actual target and inserting a mechanism of judicial review if information is uncovered that would lead to subsequent criminal prosecution prior to analysis of the databases that are held.

MS. WALD: Okay, great. Down the line.

MR. JAFFER: The only thing that I would add to that is destruction of inadvertently acquired communications. Communications that the government itself acknowledges should not have been acquired in the first place should be destroyed immediately.

MS. WALD: Destruction, they say

they're purging them but you mean something --

MR. JAFFER: There are broad exceptions to the --

MS. WALD: I know there are exceptions, but you mean -- okay.

Do you have any, Professor Ku?

MR. KU: Actually, I mean this may be kind of not what you're looking for, but I do think that actually I would prefer the FISA section clarify the default that I've been arguing for, that it doesn't encroach, to clarify further that it doesn't encroach on, Section 702 doesn't encroach on the President's, you know, foreign intelligence authority. That would, I think, help our interpretation of the statute.

MS. LEVINSON-WALDMAN: And I just would mention three things. One is I agree more robust involvement by the FISC.

MS. WALD: I'm sorry, more?

MS. LEVINSON-WALD: More robust involvement by the FISC in terms of review. There's some review now that is sort of a

box-checking procedure, and have that review be more --

MS. WALD: Just the way they do what they do now, but more carefully?

MS. LEVINSON-WALDMAN: Well, I'd say not even, it's not so much that I think that they're not careful with it now, it's that the statute actually limits the scope of some of the review that they do, that they sort of don't get behind the curtain.

MS. WALD: Including the targeting.

MS. LEVINSON-WALDMAN: Right. I guess the second, thinking about, so if you think about Section 702 but having the minimization procedures be a natural part of that statute.

Certainly limiting and potentially eliminating the use of information for law enforcement purposes. And obviously this is something that the NSA, that the President's review group spoke to as well and made that recommendation.

And then the third quite honestly would

be to lift the standard back up to agent of a foreign power from the foreign intelligence requirement. And the foreign intelligence purpose is so loose and that that seems to be --

MS. WALD: For targeting?

MS. LEVINSON-WALDMAN: For targeting, yes, that's correct.

MS. WALD: Okay. I've got maybe one minute left so a quick question. Some of you, I don't remember now, all of you in a prior one, when we were doing 215, talked about the desirability/necessity of having an adversarial element in the FISA proceedings.

A very quick notion of how would you see an adversary, however appointed, in a 702 proceeding? In other words, what function could they serve, he or she serve in a 702?

215 was a little bit more evident. A novel technological case coming up to the court, what would you say, do they have any, would they have any function in a 702?

MS. DONOHUE: So I would imagine them

having a function absolutely, yes. The ACLU tried to do this and was not allowed to intervene on a motion on a First Amendment grounds and it was denied by the court in part on the grounds that they would never succeed on the First Amendment to actually intervene.

I think having an advocate there would allow them to more carefully review minimization procedures, to more carefully review targeting procedures. It would allow them to evaluate the role that they play with regard to targeting.

MS. WALD: In individual cases in 702?

MS. DONOHUE: And in individual cases, yes, but you would have to change to insert some sort of a warrant requirement equivalent for criminal prosecution or further examination of the records.

MR. JAFFER: And I think that our biggest concern is with judicial rulings that have far-reaching implications and not just implications in the individual cases. So I think that when you're talking about the individual

cases, I do think that, you know, in theory an adversarial process would be a useful thing.

On the other hand, I think that the closer you get to an individualized warrant application, or court order application, or surveillance application, the more it looks like traditional Title III or a search warrant context, which is ex parte.

But you know, when you get to judicial opinions that authorize about surveillance at some level of generality, that is something that ought to be argued in open court, you know, with a closed hearing to follow if there is legitimate, if there are legitimate sources and methods to be protected.

But if I can just use the process to add one answer to your previous question, I agree very strongly with what Rachel said that reforming or revising the standard, the targeting standard is crucial.

Right now there is, there's really no limit on who the government can target overseas.

The example that the government panelist kept coming back to is bad guy at Google.com or bad guy at Yahoo.com. But it could as easily be journalist at Yahoo.com, or human rights activist at Yahoo.com. And I think it's crucial that some limits be drawn around the category of people whom the government can legitimately target.

MS. WALD: And by the FISA court?

MR. MEDINE: We only have a couple of minutes. If there's any members of the Board who want to ask any additional questions.

MS. COLLINS COOK: Can I ask just one quick follow-up question on this point actually?

MR. MEDINE: Sure.

MS. COLLINS COOK: And this is to Ms. Levinson-Waldman. You had said lift the standard back to agent of a foreign power or a foreign power. What were you referring to when you said back to?

MS. LEVINSON-WALDMAN: Right, I mean I guess back to, we're sort of envisioning to some extent Section 702 is sui generis and when it came

into being it was a foreign intelligence requirement. But I guess thinking of FISA more broadly, narrowing that foreign intelligence standard in some way to match what is in other sections.

Obviously one option would be matching what's in other sections of FISA, agent of a foreign power, I think that would be our preference, but narrowing that in some way. Back was probably an imprecise way of referring to it.

And if I could add one other brief thing, I think our other, you know, if we have a wish list it would be, and again, I'll say restore, but thinking about other parts of FISA, having the collection be, and you know, these may be one or the other but having the collection, the foreign intelligence be the primary purpose rather than a significant purpose, that that has also allowed, you know, potentially a fair amount of slippage in terms of what the collection is for.

MR. MEDINE: Any other final questions? I want to thank the panelists very much for

joining us today. It was a very enlightening discussion. We're now going to take a lunch break and we will resume with our third panel at 1:45. Thank you.

(Off the record)

MR. MEDINE: Good afternoon, and thanks everyone for rejoining us. And I want to introduce our third panel, which will be on transnational and policy issues.

We are joined by John Bellinger, who is a partner at Arnold & Porter, Dean Garfield, who is the President and CEO of the Information Technology Industry Council, Laura Pitter, who is a Senior National Security Researcher at the Human Rights Watch, Ulrich Sieber, who is the Director at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany, and Chris Wolf, who is a partner at Hogan Lovells.

Each of the panelists will make a brief opening statement and then we will proceed with the Board questioning.

I guess we can start alphabetically

with Mr. Bellinger.

MR. BELLINGER: It's me first then. Well, thank you all very much for having me in, the members of the Board. I'm going to focus my comments on whether international law places any restrictions on electronic surveillance of foreign nationals outside the United States.

I think you know I served as the legal advisor for the Department of State from 2005 to 2009, as the legal advisor for the National Security Council from 2001 to 2005, and then I was the national security advisor to the head of the Criminal Division at Justice Department before that, so I have extensive experience, both in intelligence activities and international law.

So in recent months I think you know many scholars and human rights advocates have argued that NSA surveillance of foreign nationals violates a so-called universal right to privacy recognized in international law.

They base their argument on Article 17 of a human rights treaty called the International

Covenant on Civil and Political Rights, which the U.S. ratified in 1992.

Article 17 provides, and I quote, no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, end quote.

The argument that NSA surveillance violates Article 17 of the ICCPR is incorrect for several reasons. And I will say in my view international law, neither the ICCPR or any other part of international law placed international legal restrictions on the NSA, any of the NSA programs.

With respect to the ICCPR, first, for the last sixty-four years the United States government has taken the consistent position that it does not apply outside the borders of the United States. The U.S. took this position when we negotiated the treaty in 1950, and we re-articulated it in 1995, when the Clinton administration submitted its first report to the U.N. Human Rights Committee, which is the group

that oversees compliance with the ICCPR.

My predecessor at the time, the then legal advisor Conrad Harper, explained to the committee that the ICCPR imposes obligations on the United States only inside the United States. And that's because Article 2 of the ICCPR, which defines its scope, says that a state party is bound to respect and ensure the rights in the ICCPR only to all individuals within its territory and subject to its jurisdiction.

And as my predecessor, Conrad Harper said at the time, this is a dual requirement that establishes that treaty obligations apply only if both conditions are satisfied. An individual must be under United States jurisdiction and within United States territory.

And now the negotiating position of the United States of the treaty confirms that interpretation. The phrase, within its territory, was added at the request of the head of the U.S. delegation, Eleanor Roosevelt at the time in 1950. And she explained that, quote, the purpose of the

proposed addition is to make it clear that the draft covenant would apply only to persons within the territory and subject to the jurisdiction of the contracting states.

There was a vote held on that addition and that addition was adopted 8 to 2 in 1950. Subsequent efforts to change that have failed.

And again, in his statement to the Human Rights Committee in 1995, Conrad Harper explained that the words were added, quote, with the clear understanding that such wording would limit the obligations to within a party's territory.

Now it's true, and I know that Laura Pitter is going to talk about this, that the Human Rights Committee and a lot of human rights groups in other countries don't agree with the long-standing U.S. interpretation, but the Human Rights Committee's statements don't have binding legal effect on the United States or to any other country. We give respect to them but they're not binding on us.

Both the Bush and the Obama administrations have confirmed the Clinton administration's position that the ICCPR does not apply extra-territorially.

In fact, just five days ago in Geneva we were making our periodic report to the Human Rights Committee and the acting legal advisor, Mary McLeod, told the committee, quote, the United States continues to believe that its interpretation that covenant applies only to individuals both within its territory and within its jurisdiction is the most consistent with the covenant's language and negotiating history.

So we really have fifty years of U.S. practice on this point recently reaffirmed by the Obama administration.

But even if the ICCPR did apply extra-territorially, the treaty would still not place limits on NSA surveillance because persons in other countries are not subject to U.S. jurisdiction.

The Human Rights Committee itself has

defined the phrase subject to a party's jurisdiction to include people within the power or effective control, or effective control of the forces of a state party acting outside its territory. So not even the Human Rights Committee is suggesting that everybody who may be subject to NSA surveillance is actually within the power or effective control of the United States.

And I would want to hear more from my colleague who I've met before, Professor Sieber, but even if they're unhappy with NSA surveillance, I am not aware of any foreign government that believes that the ICCPR or any other provision of international law imposes an obligation to respect the privacy rights of non-citizens.

In fact, candidly, most foreign governments spend lots of time spying on foreign citizens. So they may be unhappy with what we're doing as a policy matter, human rights groups may suggest that there are binding legal norms, but I'm actually not aware that foreign governments are suggesting that there is an actual violation

of international law.

And finally, just to close on my analysis of the ICCPR, and then I'll wind up, even if the ICCPR did impose certain obligations on United States extraterritorial conduct, even if people outside the United States were considered to be within the jurisdiction of the United States, Article 17 of the ICCPR still only bans, quote, arbitrary and unlawful interference with privacy.

Now we can certainly argue about constitutes arbitrary and unlawful interference but there is no international norm on that point. I'm sure lots of people can suggest that the NSA program is arbitrary, that it's unlawful, but when we're talking about international law there has to be actually a specific norm that people have agreed to, and there is no generally accepted framework under international law that defines what kind of surveillance is unlawful or arbitrary.

So the bottom line, despite statements

that we are violating the Article 17 of the ICCPR, it just simply does not apply, nor does any other provision of international law.

And so let me close by saying that just because international law doesn't actually create a universal right of privacy that's binding on the United States, I'm by no means saying that we ought to be insensitive to the rights of non-citizens. Certainly if I were still in the White House I would be saying, you know, we need to be respectful of concerns both of individuals or of leaders. That's why we make these policy decisions.

President Obama's recent presidential policy directive states that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.

So it's perfectly appropriate to take

into account privacy interests, but international law does not place binding legal obligations on us. Thank you.

MR. MEDINE: Thank you. Mr. Garfield.

MR. GARFIELD: Thank you. Thank you members of PCLOB on behalf of fifty-six of the most dynamic and innovative companies in the world, thank you for inviting us to testify today. And thank you as well for your efforts to advance both national security and civil liberties.

From our perspective we have the firm view that those two concepts are mutually reinforcing and in fact are not mutually exclusive and so we want to do whatever we can to support your efforts.

I'd like to focus my testimony on two areas. One, what we're experiencing in the marketplace as a result of the NSA disclosures and, then share some solutions that may help remediate some of the challenges that we're facing.

On the first, the economic impact from

the NSA disclosures are significant and ongoing. The folks in this room are very familiar with Section 215 and the distinction between that and Section 702, but for folks outside of this room much of what they experience and what we're experiencing is diminishing trust, particularly diminishing trust in U.S.-based technologies. So rather than made in the U.S.A. being a badge of honor, it's increasingly becoming a basis to question the integrity and security of technologies.

That has a real world economic impact. In fact, there are a number of analyses out there that put the numbers of the impact in the tens of billions of dollars.

As significant, perhaps even more significant than the economic loss is the broader societal impact and the implications for the Internet more generally. We're celebrating this year the 25th anniversary of the commercialization of the Internet and are all very familiar with the benefits and the way it's transformed all of our

lives.

Increasingly, what we're seeing though are policies aimed at changing the open, ubiquitous, globally-integrated Internet into one of walled silos. And so the legislation that's actually being debated today in Brazil would create walled gardens around their data.

And it's not simply limited to Brazil. We're seeing the same in Europe, as you all know, where the parliament is questioning the continuing viability of the safe harbor, or in particular territories within Europe where they're calling for country-specific clouds that would again create these islands of walled silos rather than an open, integrated Internet, which we all know the implications of that.

And so what do we do about it? I'll offer up three sets of solutions that build on global principles that we released earlier this year after working with our members to forge consensus on it.

And I place the emphasis on global

because we firmly believe that in order to address these issues and to address them effectively, high level, global communication and engagement around surveillance is critically important.

The first aspect or screed of solutions is around transparency. This body, the PCLOB in its January report made the point that transparency is the foundation for democratic principles. We firmly agree. We also think it's the foundation for separating fact from fable.

And so to the extent that there's a greater awareness, particularly around 702 where there are protections in place already, for there to be greater awareness about that would be quite helpful.

As it relates to our companies, the ability to share with the public more about 702 and 215 and the requests that come in pursuant to those, as well as the accounts, particularly the numbers, would be incredibly helpful. And so greater transparency is one element of what we would recommend.

The second relates to oversight. And as I've said in other places, including my testimony on the hill, our solutions are offered with a great deal of humility because we don't know what we don't know. I don't pretend to be able to offer the exact framework for making sure that there is a civil libertarian advocate or a civil liberties advocate within the FISA or FISC court process. But developing a framework for enabling that, we think is very important.

Finally, the last set of solutions are based on working to rebuild the trust that has been eroded, and there, a few unequivocal statements from our government would be quite helpful.

By way of example, there has been a lot of reporting around steps that may or may not have been taken to undermine encryption standards. NIST has been very firm in taking steps to make sure that they bolster the encryption standards that are being developed.

But a statement from our government

that they don't, do not intend to take steps to undermine the integrity of our cyber -- to undermine the integrity of those standards would be incredibly important.

Similarly, taking steps to affirm that data acquisition pursuant to 702 is not being done in an indiscriminate manner, I think would also be incredibly helpful. With that, I'll pause.

MR. MEDINE: Thank you. Ms. Pitter.

MS. PITTER: First, thank you very much for this opportunity. Thank you for having me. We've filed a more lengthy statement with the Board so I'm just going to be a little bit more brief here.

I was asked to talk about U.S. obligations under the International Covenant for Civil and Political Rights so I'll start with that.

And obviously, I'm going to disagree with Mr. Bellinger on this issue, as did Harold Koh's recently released memo where he disagreed as well and tried to get the Obama administration to

take a different position, arguing that it was not actually in the U.S. interests to continue to not apply the ICCPR in an extraterritorial manner.

There has been debate about whether or not this treaty applies outside of U.S. borders and it stems from, as Mr. Bellinger said, the operative jurisdictional clause in the covenant which says that states have an obligation to respect and ensure that those within its territory and subject to its jurisdiction, the rights under the covenant.

So the word jurisdiction in that clause has been interpreted to mean power and effective control. But the U.S. does not accept that. It takes a strictly territorial stance. And this essentially means that a state has to abide by the covenant within its territory but then it can willfully violate the covenant outside its territory, killing and pillaging at will outside its borders, which doesn't really make any sense.

Treaty law requires that the language of the treaty be interpreted in accordance with

its context, as well as its object and purpose. And the context in this case was post-World War Two when the treaty drafters were aiming at empowering people with rights universally and not diminishing them, and responding effectively to Nazi atrocities.

To interpret the treaty in that limited way would allow, for example, Nazi Germany to run a concentration camp in Poland, as Marco Milanovic, a prominent scholar on this issue has pointed out.

And the U.S. is the clear outlier on this. Only the U.S. and Israel take such a strict interpretation of the treaty.

So how does this apply to surveillance and the right to privacy? Some have argued that even if the ICCPR applies extra-territorially it should only be in the case where the government has physical control over the individual, like in the context of detention or torture. And that doesn't apply to surveillance simply because the individual is not within a state's effective

control.

But the problem is that their communications are. And so to not recognize even a duty to respect the right to privacy in this context creates a kind of absurd situation where the U.S. would be barred from going into someone's house in Germany and taking letters out of someone's drawer but not barred from reaching into their computer and doing the very same thing remotely.

These are novel questions, and I won't deny that. The Human Rights Committee, which is the main interpretive body of the ICCPR, has not adjudicated this matter.

And though there is a body of case law in other jurisdictions, particularly in the European Court of Human Rights, that have the issue and they do provide some guidance on a framework for how to analyze surveillance laws.

That said, those decisions, they came out before the Snowden revelations so they're not informed by a lot of the information that's come

in the public domain about the vastness of the collection that's going on.

But these issues are novel in the U.S. too. Just because there may not be necessarily a case en point does not mean the obligations or the rights don't exist. They are in the treaty.

Just as like many in the U.S. have argued that U.S. law has to catch up with technology and recognize a reasonable expectation of privacy in metadata, international law has to acknowledge that when it comes to surveillance, though an individual may not necessarily be in a state's physical control, their communications are, and the right to privacy can be violated remotely through technical means.

But just because the obligation applies extra-territorially does not mean that the surveillance has to stop. There is a framework within which surveillance can take place, but also be in accordance with human rights obligations. The surveillance has to be lawful and non-arbitrary and necessary to a legitimate cause

that's proportional to that legitimate aim.

By all accounts, that's not what 702 is. 702 may all be for the purpose of protecting U.S. national security, which would be a legitimate aim, but are there more narrowly tailored ways to achieve that aim?

And if the answer to that question is no, and I'm going to quote from the review group here, the question is not whether granting the government authority makes us incrementally safer but whether the additional safety is worth the sacrifice in terms of individual privacy, personal liberty, and public trust. And also, is it really worth the other harms that will result?

We're in a situation now in which countries are rushing to enact laws that would localize data collection and companies are rushing to offer alternatives to customer data being stored in the U.S.

And from a technological standpoint data flows are not necessarily based on geography but travel the cheapest, most efficient route.

This means a transfer to someone in the same country can mean data passing through many countries without the sender even knowing it. So a failure to respect the right to privacy extra-territorially imposes, exposes U.S. data to vulnerability when it's situated in other states.

The President has already essentially recognized all this. His presidential policy directive purports to bring the rules on retention and dissemination of data collection on foreigners closer to those that govern data on U.S. persons.

But it did not end bulk collection and specifically exempted data temporarily acquired to facilitate targeted collection.

Also, this was through an executive order not legislation, so it could be changed by future administrations.

The bottom line is that the U.S. is in a unique position because most of the world's data flows through its borders. And this confers an obligation to respect the privacy rights of those individuals whose communications fall within the

U.S. jurisdiction, but also to refrain from interfering with the ability of other countries to protect data, protect their own citizens' data. And a failure to recognize the value of this undermines U.S. business and long term national security interests.

The administration says it will make some changes but the law remains the same and that too has to change.

MR. MEDINE: Thank you. Mr. Sieber, Professor Sieber.

MR. SIEBER: Thank you very much for your kind invitation. It's a pleasure to be here.

International legal obligations for U.S. surveillance programs for which you are asking can be based on two different sources, interests of states and interests of persons. The two are interrelated since the protection of a state's territory also has effectual protective functions for its citizens.

Let me start therefore with a few remarks on this broader approach before turning to

specific human rights, which have been addressed here.

General international law and Article 2 of the U.N. Charter protects the sovereign equality and territorial integrity of all states.

A state therefore violates territorial sovereignty if it accesses, copies, or manipulates non-public data in computer systems located in a foreign state because such acts initiate in data processing on the servers located in a foreign territory.

There are no norms in public international law that permit violating other states' sovereignty by across the board world-wide surveillance.

There is also no customary rule of international law that permits the infringement of sovereignty resulting from acts of espionage.

In addition, espionage committed from the premises of embassies violates the obligations under Article 3 of the Vienna Convention on Diplomatic Relations.

These infringements of the territorial integrity of many states by large scale surveillance programs have two impacts for our topic. First, with respect to policy considerations, infringements of the territorial integrity of foreign states violate international law, plus in addition also national cyber crime statutes that are globally agreed upon in the Budapest Convention.

These violations pose serious threat to the continuing trust and the integrity of the U.S. and its IT industry. This infringement may be more serious than the violations of privacy rights, the scope of which are controversially in dispute in most countries.

Secondly, transnational surveillance programs on foreign territory take over the security functions of the affected states. This transnational control deprives citizens of protection by their own state and any other legal protective systems in these security measures, since their home state cannot protect them against

unknown foreign violations of their privacy and the intercepting foreign state often does not recognize any aliens' rights outside its territory where the interception is taking place.

In such a global system the citizens, including U.S. citizens, are deprived of any protection, especially if authorities of different countries exchange certain data.

Thus we are all losing a protective system which mankind has won in a long historical battle dating back to the Enlightenment. Thus, if we are engaging in transnational surveillance programs we must at least recognize certain basic human rights apply to all humans, regardless of nationality and place of residence. And if we want to create an effective global solution this must be supported by international human rights, to which I will now turn.

In the field of international human rights I will also concentrate on Article 17 of the International Covenant of Civil and Political Rights. The International Court of Justice, the

U.N. Human Rights Committee, both in its case law and in its General Comment 31, as well as many national courts and governments acknowledge the extraterritorial applicability of the ICCPR.

I also simply refer to the well-founded memorandum presented by Harold Koh, former legal advisor at the U.S. State Department in 2010 and 2013, with respect to the ICCPR. Koh is convincingly for the extraterritorial applicability of the conventions.

According to the prevailing opinion, the ICCPR is extra-territorially applicable to anybody within the power or effective control of the acting state party or its agents.

In the physical world, extraterritorial applicability of the ICCPR is thus limited to situations in which the government has total or special control, spatial control over a territory.

Since communications and privacy rights are by their very nature exercised in the virtual world and are prominently infringed upon there, the control of this virtual world by highly

extensive surveillance programs should be a decisive factor.

If we do not accept these conclusions we still must deal with an argument of the German Constitutional Court, which also might be relevant for the American discussion. The court argues that telecommunication interception not only infringes upon privacy rights by the first act of recording the telecommunication, it also infringes on these rights by the following data transmission to their home country, the analysis, the linking, the long-lasting storing, and by further transmissions to other recipients.

All these acts are repeating and deepening the infringements of privacy rights and they are undoubtedly committed on the territory of the surveilling states. Thus, even in cases of foreign intelligence gathering, we are not dealing only with actions outside the national territory.

Accepting the arguments for the transnational applicability of specific international human rights would promote then a

deeper discussion on the substantive scope of international human rights protection of privacy.

A first attempt to define the contours of the international concept of privacy can be seen in the already mentioned U.N. General Assembly Resolution 68167 of last December on the right to privacy in the digital age.

When this discussion proceeds, it will be most important to recognize that threats from abroad are different from internal threats. Thus the principle of proportionality as developed by international and national courts will lead to very different results in different circumstances, such as for data collection to homeland, in Afghanistan, or today in the Ukraine.

These necessary differentiations under the principle of proportionality can recognize many U.S. security concerns. Thus applying certain transnational privacy rights would not prevent a reasonable security policy, especially also since the ICCPR is self-executing in the U.S.A. and national foreign citizens could not

initiate judicial proceedings against the U.S.

In sum, I would advocate for an international solution and discussion in order to maintain or regain the leading role of the U.S. as an advocate for the rule of law and human rights in democratic societies, as well as for the trust in its IT industry and its clouds.

If time is not yet ripe for an international human rights solution, then more emphasis should be placed on national efforts to provide more guarantees for non-U.S. persons.

For that reason I welcome the respective U.S. Presidential Directive 28 of last January to applying certain safeguards for all individuals, regardless of the nationality of the individuals to whom the information pertains or where that individual resides.

This policy is also the position of the German constitutional law. In case of your interest it would be a pleasure for me to provide you with more details on these comparative legal aspects later on in the discussion. Thank you.

MR. MEDINE: Thank you. Mr. Wolf.

MR. WOLF: Thank you, Mr. Chairman. As Chairman Medine said at the outset, I'm the partner in the law firm of Hogan Lovells, where I lead the firm's global privacy practice.

And in 2013 Hogan Lovells published a white paper examining the similarities and differences among various legal regimes that authorize and limit governmental access to data.

And our work began before the Snowden NSA disclosures in response to the claims of certain EU cloud service providers that storage of data in the EU made it safer from surveillance than storage with a U.S.-based cloud provider.

Obviously following the Snowden revelations the argument in support of allegedly secure from surveillance regional clouds has been renewed loudly.

A previous white paper we did on governmental access to data internationally noted the availability of mutual legal assistance treaties and other forms of cross-border

governmental sharing addressing faulty claims of regional cloud service providers about the invulnerability to foreign government access that local cloud storage might provide.

Our 2013 white paper specifically looked at Section 702 surveillance and the frameworks in Australia, Canada, France, Germany, and the United Kingdom. My written and oral testimony today synthesizes the findings from this white paper and includes additional information on similar laws in Brazil, Italy, and Spain that we intend to publish soon.

I will note that our white paper foreshadowed last week's report of the European Parliament criticizing the practices of certain EU member states for the lack of transparency and controls on their surveillance activities.

My principle point today following our white paper is straightforward. While the policies and practices of the United States addressing surveillance and related privacy concerns obviously need to be and are being

reassessed, the U.S. has on its books greater due process and independent oversight of surveillance activities than many of our fellow democracies.

As you know, Section 702 surveillance requires court approval, surveillance is limited to foreign intelligence information, and oversight mechanisms exist for 702 surveillance.

As our white paper revealed those same limitations are not always found in the law of many of our counterparts. Australia, Canada, France, Germany, Italy, and the United Kingdom do not require court approval for national security surveillance.

In France, the intelligence agency is allowed to conduct surveillance to protect economic and scientific assets, even when national security interests are not at stake.

On the issue of intelligence agencies secretly and without any process at all asking companies for data, we have found that Australia, Canada, France, Germany, and the U.K. allow their governments to ask private entities voluntarily to

disclose data to the government.

In the U.S. the government is not allowed to seek voluntary transfers. A neutral judicial body must approve the government's request for data.

Last week's resolution by the European Parliament recognized extensive surveillance systems in EU member states, and the lack of control and effective oversight that some EU member states have over their intelligence community.

The resolution also questioned the compatibility of some member state's massive economic espionage activities within the EU, with the EU internal market and competition laws. The parliament did not go into the detail of our white paper, but its resolution reflected the baseline findings of our research, that there are substantial deficiencies in transparency about and controls over national security access to data in countries outside the U.S.

Thus when also considering the cross-

border sharing arrangements available to governments for information they collect through surveillance, it is misleading in the extreme to contend that so-called regional clouds provide individuals with security from government surveillance.

I commend this Board for engaging in an assessment of U.S. surveillance practices and looking at how these practices relate to our counterparts. There are no guarantees in the U.S. or elsewhere that agencies will abide by the laws restricting national security surveillance, but the degree of authorization required and the kind of review that occurs is obviously relevant to a determination of how well personal privacy and personal liberty are protected.

Thank you again for the opportunity to present the findings of our white paper and I'll look forward to your questions.

MR. MEDINE: Thank you very much.

I want to turn to the ICCPR for a moment, and as I understand it there are really

two issues here. One is the jurisdictional test, and if you pass that then the substantive test with regard to evaluating whether the 702 program affords appropriate protections or is arbitrary in some fashion.

I want to start with the jurisdictional issues, and that is, I guess there are three interpretations of the applicability of the treaty. One is that there has to be both territorial presence and jurisdiction. The other is there could be one or the other. And I guess the co-approach, which is they sort of split it, and that is there is a respect requirement across the board and an ensure requirement only subject to the territorial and jurisdictional issues.

I want to ask about the jurisdictional side. As we know from discussion earlier today and what's been made public is the information that's being collected under the 702 program is being collected in the United States, albeit about non-U.S. persons.

I guess my question is for the

panelists, how should we, how should one interpret jurisdiction? It's not going to be up to us to interpret it, but in terms of understanding jurisdiction, is it jurisdiction over the information, which may be here, is it jurisdiction over the person, who may be elsewhere? And how would that apply, both in sort of friendly and unfriendly countries, in terms of the scope of our responsibilities?

MR. BELLINGER: I'll take a stab at that. Let me say a couple of things. One, just to reiterate that the U.S. has in fact reaffirmed its position again that the ICCPR does not apply extra-territorially and the point that the individuals have to be under the power and control.

You know, I get sort of the novel suggestion that anybody who is subject to electronic surveillance is therefore under U.S. power and control. But I don't think that's actually a credible argument.

Even the Human Rights Committee I think

would not go so far as to say that if one can touch a foreign national through surveillance that that is someone who is under U.S. power and control.

The fact that the surveillance may be then collected ultimately inside the United States I think does not change the fact that the collection is being done of persons who are outside the United States. And so I think that does not change the, either the essential jurisdictional element that it does not apply extra-territorially outside the United States, and that those individuals are within the power and control of the United States.

Again, these are things that one might wish were so, and I'm not sure that there's as much of a disagreement between me and Laura Pitter as she suggests.

If one were writing a new treaty and could get people to agree to certain things one might agree that there might be, you know, policy limitations that one might accept.

But the way this particular treaty is written now, certainly the view of the United States government, and I frankly think I am not aware of any single government in the world, and I mean this is what I mean, governments who believe that their right to conduct electronic surveillance of people outside their territory is controlled by the ICCPR. I would be very surprised if we found any European government, as upset as they might be with electronic surveillance by the United States, who would say the Article 17 of the ICCPR limits our ability to collect outside our borders.

And in fact, the German government in a submission made to the European Court of Human Rights interpreting the European Convention on Human Rights argued that that convention did not limit its electronic surveillance of Uruguayans outside of Germany.

So again, the view of governments is that this does not have jurisdictional control over people who are outside their territory.

MR. MEDINE: I just wanted to follow up. What is the scenario where someone would be in our territory and not within our jurisdiction? Because the statute, the treaty says both territory and jurisdiction. Are there other situations where one would apply but not the other?

MR. BELLINGER: Well, certainly there would be people who would be, theoretically there could be people who are not in our territory and who could be subject to our jurisdiction. That was the problem that Eleanor Roosevelt was trying to solve at the time, to think about what the converse might create.

MR. MEDINE: Okay, thanks. Ms. Pitter.

MS. PITTER: Well, first of all, the German position was taken in 2008 before these revelations came forward and they've since sponsored a U.N. resolution which underscores the importance of respecting the right to privacy.

So I would say that, you know, Koh's interpretation is that there's on the one hand a

duty to ensure the rights in the covenant to those within a state's territory and jurisdiction, and then there's also a duty to respect the rights of individuals outside of the territory, the actual territory of the United States.

So there's the duty to respect is what's important here, and so there is an obligation under the ICCPR, even with the jurisdictional clause, to respect the rights to privacy of those outside the United States.

But this all, as you said, is happening in the United States. I mean the data is flowing through U.S. borders, although I'm not sure about the backbone upstream collection, where exactly that's taking place. So absolutely, yeah, absolutely, I mean I think that it would be the duty to respect the right to privacy is what's implicated here.

MR. MEDINE: Thank you. Judge Wald.

MS. WALD: I've got two questions I think for Mr. Bellinger. First is I think we recognize that the government has now reaffirmed

its earlier position about what the ICCPR means in relation to people abroad. But I wondered if you'd just say a word about how they dealt with the question of Article 31 of the Vienna Convention on the interpretation of treaties insofar as, as I remember it, you know, deference should be given to the official interpreters of the -- which in this case I believe, you know, have taken a much broader interpretation of that.

And I think a couple of our Supreme Court justices have said in several cases that when you're interpreting, when they're interpreting a treaty one should look to the interpretations, maybe for guidance, maybe not controlling, of other parties to the same treaty. Just a word or two on those two aspects of the reasoning which led to what is, is the reaffirmance of it.

MR. BELLINGER: Right, and I think what you're talking about is the General Comment 31 of the Human Rights Committee.

MS. WALD: Yeah, yeah.

MR. BELLINGER: Which certainly in the view of the United States, and again, I'm not aware of any government in the world who believes that the views of the Human Rights Committee actually are legally binding.

The Human Rights Committee was set up to monitor compliance and it makes statements which governments, including the United States, give respect to but we certainly don't, neither we nor other countries believe that that is the definitive interpretation of the treaty, nor do we believe that it's legally binding.

MS. WALD: Okay. My second question --

MS. PITTER: I was just going to add, sorry.

MS. WALD: Go ahead.

MS. PITTER: That it is, the Human Rights Committee is a very authoritative source regarding the interpretation of the covenant. And I mean the U.S. is under an obligation to give effect to the rights in the treaty in good faith. So what the Human Rights Committee has said in

that regard is very important.

MR. BELLINGER: And if I could just say, because these are important points right now, including for treaties, frankly the Human Rights Watch is extremely interested and having gotten through the senate the U.N. Convention on Disabilities.

So you know, Human Rights Watch can speak for itself, but certainly the view of the U.S. government and of most human rights organizations is that the statements made by these treaty compliance groups, while due great respect, are not binding on the United States.

If they were in fact considered to be binding on the United States, those would in fact fundamentally change U.S. obligations under the treaties and we would never get any treaties through the senate, including the treaty that both Laura and I would very much like to get through the senate, the U.N. Disabilities Convention.

MS. WALD: Okay. My second question very quickly is that acknowledging what

everybody's about, that this big debate in the international world will continue probably despite the most recent position we've taken, and given, you know, all of the people allied with it, the official interpreters, whatever they're called, Harold Koh, Sara Cleveland, Manfred Nowak, who's the U.N.'s leading expert on the ICCPR, my question to you deals with the last paragraph of your both oral and written testimony, and that is that you would see no problem with a policy which gave greater consideration to the rights of non-U.S. persons within the surveillance context, alluding to the fact that the President in his directive suggested that.

But I'm wondering if you, having served the position you did as counselor in the State Department, have any more specific ideas about in this context 701, or maybe even in other surveillance programs we could do just that?

MR. BELLINGER: Thank you, Judge. It is a great question. I have not actually given a lot of thought to that.

MS. WALD: Maybe a little.

MR. BELLINGER: My general sense from the surveillance that I saw was in fact that we are very targeted on specific intelligence requirements.

These are not broad dragnets of the surveillance of average individuals and so this is not a great violation of the rights of privacy of every single foreign national, that's very much focused on individuals who may pose a national security threat or for which the United States has a valid intelligence interest.

MS. WALD: Would you, for instance, think that taking national security, assuming you didn't have a national security risk, that basically non-U.S. persons we should try to approximate as much as we can within those restrictions the equal treatment in use, retention, that kind of thing of non-U.S. persons in our surveillance, or not?

MR. BELLINGER: I think that some of the things that the Obama administration,

President Obama has been focusing on to ensure that, particularly for the information that is collected, that we ensure that it is kept private.

I mean I would be personally, I haven't seen this happen, but I would be personally extremely concerned if we found that the United States had collected information about foreigners great or small, either a world leader or a lesser known person, and then we're not careful with that information and were to let it out. That would very much interfere with that individual's right to privacy.

I think, you know, as a national security official it's important for us to collect the information that we've collected, but we need to be extremely careful with it. So my sense is that as a policy matter these privacy concerns are important.

MR. MEDINE: Mr. Dempsey.

MR. DEMPSEY: My question I guess for Laura Pitter and maybe also for Mr. Sieber. Among the major, certainly the countries that Chris Wolf

looked at and cited, but among the other major democracies that do foreign intelligence surveillance, is there anyone that has a law which you would point to as a better model?

MR. SIEBER: Could you ask the question?

MR. MEDINE: Is there a country that has a better model of surveillance than ours? Is that --

MR. DEMPSEY: Yeah. In other words, what other country has a better model, a better law, more checks and balances, more controls, more limits?

MR. SIEBER: In general.

MR. MEDINE: In general, checks and controls balancing privacy and civil liberties and national security.

MR. SIEBER: It's a very broad question --

MR. DEMPSEY: Just pick one.

MR. SIEBER: Because you have to consider many, many aspects, not only the

extraterritorial implication. I just can give you some reliable differences a between the German system and the U.S. American, that's what I can witness on.

If you have a look at the German system you have to see that Germany has a very strong constitutional court and is very much attached to fundamental rights. This is a reaction to the Nazi cruelties and any steps towards this direction should be prevented. This is the reason for some very basic differences between the U.S. and Germany.

The first one, for example, is that intelligence agencies in Germany have no executive powers. So they cannot execute arrest warrants or anything like that. They just can collect the information. This is based on the idea that the lack of control which we have in this area of intelligence agencies must be balanced by lesser constrained measures.

Secondly, Germany has constitutionally founded strong separation of powers and separation

between the police and the intelligence agencies. This has been changed a little bit after 9/11 but still there is a fundamental separation.

Information exchange is only possible in a very limited way for very, very serious, serious crimes.

So I would say the differentiation between the institutions is stricter. We don't have multipurpose institutions like the FBI.

On the institutional side there is an absolute strong separation between these institutions, despite certain common datas and things which we have done after 9/11.

You could go further, if I compare it and look around at the control agencies which you have. In Germany it's separated. For internal surveillance we have a special commission appointed by the parliament, G-10 Commission who is doing the job. It's not called a court but the functions are similar.

And for foreign intelligence agency, the BND, there is a parliamentary commission who

does these things.

Maybe one last point, if you look at the aspect of protection of foreigners' rights and applicability of the constitution abroad, the German attitude is more in favor of applying the national constitutional guarantees.

With respect to the first question, which is foreign territoriality, section 1 of the basic law says that the basic law binds all public authority. And this is in general irrespective of whether it's in the country or outside the country.

There are differences of course, but they have more to do with the different circumstances, because the risks coming from abroad might be bigger than coming from within the countries, and for that reason I absolutely agree that the systems might be different for internal intelligence and external.

But it's not based on the fact that we do not apply the constitutional guarantees abroad, and it's definitely not based on the fact that we

are giving different rights to foreigners and to citizens, at least in this area of dignity rights, of human rights, and especially in the privacy rights.

So for example, there was a German decision of the court which was controlling intelligence gathering for abroad and which checked these systems.

So with respect to this question which we are dealing here, if I generalize it I would say we are more open to applying these fundamental rules. We do not reject it as it's not applicable. We don't go into these (inaudible) stay out of it. We would apply it, but then we have a proportionality principle and we check whether the things are justified.

And for example, in this decision I mentioned, the court said, yes, dangers coming from abroad are bigger, bigger dangers, and with balances and this law was in general justified with one exception.

It was applied also by law to internal

conflicts, and the constitutional court said it cannot apply just like that.

So I think these are the main interests which I could tell you. It's impossible to say better or worse. I would never, never do that.

MR. MEDINE: Thank you. Ms. Cook.

MR. DEMPSEY: We'll come back around.

MR. SIEBER: And if you permit afterwards I would like to say a few words with these International Convention 17, the applicability, but I don't want to --

MR. MEDINE: We'll come around at the end.

MS. COLLINS COOK: So I wanted to thank you all for coming and to congratulate you for being the panel that has come the farthest set of distances to participate today. I think it's very helpful to have this type of discussion in an open forum.

We've talked a fair amount today and all through the day about skepticism about U.S. law and U.S. practices. I think it's fair to say

there is also a high degree of skepticism about the contours -- let me get closer here.

I think it's fair to say that there's a high degree of -- if I can get through this question without hurting someone, this is really going to be my goal for the day.

(Laughter)

MS. COLLINS COOK: There's a high degree of skepticism about the contours and applicability of international law as well. So having experts who are able to speak to these issues is critical, I think, to us.

And I wanted to draw off of something, Professor Sieber, that you had mentioned and I have to confess it was not a focus of mine coming into today. I had been focused on the ICCPR and the potential applicability of Article 17.

But you talked about the interests of states, and if I understood what you said correctly, that the interest of a state in its own sovereignty is inviolate, that surveillance by one country in another country is a violation of that

sovereignty, there is no exception under customary international law that would make that any less of a violation of the state's sovereign status or rights.

So that's the academic point. That would lead me to think that no one was conducting surveillance on anyone else, that no country is doing surveillance.

But as a practical matter I think it's fair to say that every country is either engaging in foreign intelligence collection or attempting to engage in foreign intelligence collection.

So if you can explain to me how you can have a principle of customary international law, here the absence of an exception that is honored by not one country in the world, as I understand it.

MR. SIEBER: Yes, I remain with the saying that there is no permission of espionage under international law because the principle of self-defense, that needs an armed conflict for it. It's not there for the ordinary case.

And customary law would require an opinio juris, the conviction of the people that espionage is right.

But our estimations, that are split. If we are considering our own law, we say, yes, we do it and we give them a medal if they are successful. If we are considering the other, we say it's illegal.

So there are two regimes of law which come to different results. We live with that but we cannot say that international law has a general view that we can, that we can do it.

We have this problem in a very interesting case with the German reunification because when the two parts of Germany came together, there have been people doing espionage in East Germany and they are now under our jurisdiction.

This question came up and here again the Constitutional Court said there is no general violation of international law, and I think you agree with that. We have to live with this

conflict.

And in the global world that's normal. The world is getting so diverse that we have many conflicting regimes today now, so we can stand with that.

MS. COLLINS COOK: So I guess my question, perhaps Mr. Bellinger, you can speak to this, is it a violation of international law in terms of infringing the interests of another state to engage in sort of foreign surveillance?

MR. BELLINGER: I was going to jump on that as well. And the answer to that I think is clearly no. I am not aware of any country who believes that the U.N. Charter's statement on the protection of territorial integrity and sovereign equality of states actually prohibits electronic surveillance of another country.

Certainly if that were the understanding of our senate that in becoming party to the U.N. Charter that prohibited us from spying on another country because it would violate their sovereign equality or territorial integrity, then

we would get out of the U.N. Charter immediately. But I am not aware that any other country believes that as well.

So there is not, the principle of territorial integrity and sovereignty would apply to, say, for example, use of force. International law does not prohibit electronic surveillance or spying. Domestic law may.

And so that's really, you know, when we talk about international law, that basically means that there is a compact between countries. Judge Wald knows this very well, you know. Countries have to have agreed that they are not going to do these things to each other.

And in the U.N. Charter, the U.N. Charter was not saying we promise not to spy upon one another, we were saying we promise not to use force against one another.

U.S. surveillance in another country might violate the other country's law, but it is not a violation of international law.

MR. MEDINE: Let's go on to another

question. We'll give Ms. Brand a chance and then we'll come back.

MR. SIEBER: Because I think I have to contradict.

MS. BRAND: All right. Let's see if this microphone will work now.

Thank you all for being here today. One of the things I find frustrating about this discussion, not here specifically but in general is that there is a tendency to not distinguish between what is law and what is -- it's not working is it?

And what is either what people would like to be the law or what is a matter of policy.

And John, thank you for making that distinction very clearly in your remarks.

I was having a little bit of a harder time, Laura, following where you were moving from what you think is actually binding law to what is not.

And so I wanted to know if we are looking, setting aside policy, aspirational policy

for a moment, if we were trying to determine whether what the government is doing under 702 is legal, do you think there is some binding international law instrument that affects that questions?

MS. PITTER: Yes. I mean from my position it is a violation of Article 17 of the International Covenant on Civil and Political Rights. The United States does not recognize that, and that's part of the problem.

MS. BRAND: So let me just ask a question then. If the U.S. government doesn't recognize that, what is the body, what is the document, what is it that then makes that law binding on the U.S., on the agencies implementing 702?

MS. PITTER: It's the treaty itself. As Mr. Bellinger said, you know, a treaty is something that governments have agreed to abide by and to honor the commitments in the treaty in good faith.

MS. BRAND: And what is the body that

has the last say on the interpretation of the treaty, right? Because obviously the U.S. government interprets the treaty differently from the way you interpret the treaty.

Is there some other body besides the U.S. government itself whose interpretation of the treaty is then binding on the way the U.S. agencies implement it?

MS. PITTER: Well, the Human Rights Committee is one of the most authoritative sources on this, but --

MS. BRAND: But is it legally binding, right? That's my question, not is it persuasive, is it binding?

MS. PITTER: I mean from the opinion of many other governments it is. The treaty is binding upon them. The United States does not recognize the extraterritorial application of it.

MS. BRAND: And this is an honest question, give me an example of a country that views the ICCPR to have extraterritorial application with respect to surveillance of

foreigners abroad that itself that takes its own advice or heeds its own interpretation.

MS. PITTER: So this surveillance, as I said, is a novel issue. It's not something that's been addressed by the case law, and especially not since the revelations from Snowden which have disclosed, I think even to policy makers in many countries, the degree to which the law, the domestic law on the books is actually being applied, and the vastness of the programs, how much data is actually being collected.

So it's a novel interpretation, I mean it's a novel question, as it is in the United States --

MS. BRAND: I'm sorry to cut you off but we have a strict timekeeper here, the Chairman, and I want one last question.

I'm interested in your interpretation of what constitutes control and how being surveilled essentially would put someone within the control.

My concern about that interpretation in

part is that I'm not sure what meaning is left in the phrase, under its jurisdiction. If the statute talks about territory and jurisdiction, if jurisdiction means something in addition to territory, it seems like a meaningless phrase if it can include surveillance.

MS. PITTER: Well, it is meaningless in the sense that the United States has taken up, used the technology to conduct surveillance on a very mass scale. So it affects an enormous number of people.

The, you know, jurisdictional clause has been interpreted extra-territorially in the context of detention and torture, in which a smaller number of people have been affected. But when you're talking about surveillance --

MS. BRAND: But detention, I mean someone being detained or tortured is, I would say, much more clearly within the control of the government who has detained or is torturing them, right?

So my question is when you get into

surveillance and the person is clearly not within the physical custody of the government in question, what is it within the ambit of the treaty?

MS. PITTER: So you can look at it two ways there. You know, their communications are within the effective control of the government and so that's one way to look at the obligation.

But in addition, they have an obligation to ensure the rights within the covenant territorially, but also to respect the rights in the covenant extra-territorially.

So although they are not necessarily bound, you know, to enact legislation domestically regarding, you know -- well, they're not necessarily bound to ensure the rights of individuals with regards to privacy extra-territorially, they are bound to respect those rights extra-territorially.

MS. BRAND: I see my time is up.

MR. MEDINE: Mr. Garfield, in your statement earlier you indicated that the

revelations about the surveillance programs, particularly 702, has had significant international impact with regard to business dealings with U.S. firms, and you proposed a number of steps to ameliorate that, and I wanted to ask you about some of them.

And you also mentioned one of them, namely transparency in your remarks earlier. Do you have thoughts about what level of transparency would be helpful to companies, but taking into account national security concerns?

As you know, our first report on 215 did recommend greater transparency, but in terms of disclosures that a company can make about surveillance requests from the U.S. government, so long as that took into account national security.

And I guess in particular if you have comments on the agreement that was reached between the Department of Justice and a number of firms, whether that agreement goes far enough and provides sufficient detail to give comfort to business partners of those firms overseas.

MR. GARFIELD: Thank you for the question, first of all. The agreement with the Justice Department is viewed as a significant step forward. There are additional steps that can be taken that would be helpful as well.

One is the level of detail that the companies are able to share, including disaggregation of data between Section 215 and 702, or whether it's a national security letter. So a greater level of granularity would be helpful.

The second part of that is it is not only important that the companies be able to share out information but that the government share information as well and provide greater transparency, which is often lost in these discussions.

The debate that's been taking place today speaks to the importance of greater transparency because 702 already includes a number of protections that are not generally known, particularly internationally.

To Christopher Wolf's point, if they were more well-known it would be clearer the extent to which steps are being taken in the United States that are not necessarily being taken in other countries.

MR. MEDINE: And you also recommended, made a couple of other recommendations that you put forward were oversight, the importance of oversight and in discriminant collection.

And I guess the question is in the 702 program isn't there already oversight through the Foreign Intelligence Surveillance Court and some of the internal government processes?

And with regard to indiscriminate collection, I think as we heard earlier there has to be a foreign intelligence purpose, and so it's somewhat constrained. Do you think that with regard to this program it meets those requirements?

MR. GARFIELD: Correct. My recommendations there weren't intended to suggest that it in fact was indiscriminate. It was

suggested, it was a suggestion that taking steps to be clear about the protections that are in place and to the extent it is not, it is in fact not indiscriminate, to reaffirm that would be helpful as we go about doing our business internationally.

MR. MEDINE: And Mr. Wolf, you analyzed other country's laws and shown that they're not only not better but maybe not even as good as our laws by some criteria. What lessons should we draw from that in terms of how countries should conduct their surveillance programs?

MR. WOLF: So the purpose of our white paper and our research was really to be expository than to reach judgements and to pick winners and losers or to decide whose was better or best.

But we thought it was important in light of the claims that were being made, particularly by the cloud industry in Europe that there is national security access obviously that goes on in the EU and elsewhere around the world, and often without the controls and safeguards and

transparency that we have here.

So the overall conclusion that we reached is that this is a global problem. Obviously it's one that has been focused on intensively here in the United States because of the Snowden revelations, but it is an international issue that needs to be resolved internationally, particularly with the sharing that goes on among intelligence authorities.

It is heartening that the European Parliament in its resolution last week adopted the draft report that came out in January that focused on the European intelligence gathering practices.

We hope that the data protection authorities in Europe who've been vigorous critics of the NSA practices will comment on their own country's practices. They've been relatively silent on that, and we think the debate that has to be made should be among all those interested in privacy protection, and obviously that would include the privacy commissioners abroad.

MR. MEDINE: Obviously countries have a

lot of self-interest in conducting surveillance programs. Do you see a forum in which countries can or even should agree with the methods by which they conduct surveillance?

MR. WOLF: So that's well above my pay grade. I really don't have a view on that.

I do have, if I can just mention on the transparency point, we did a white paper in August that then general counsel of the Commerce Department Kerry cited in his speech at the German Marshall Fund that actually showed on a per capita basis access by national security and law enforcement on a per capita basis is larger outside the United States in many instances.

MR. MEDINE: Judge Wald.

MS. WALD: I have two questions for Ms. Pitter. Given what most or many observers concede are widely varying practices in different countries about surveilling their own and other country's citizens, would you advocate, as we sitting here have to make some observations, maybe recommendations on 702, would you advocate that we

unilaterally, we recommend unilaterally putting in place one and the same protections for non-U.S. person surveillance that we have for U.S. citizens? Or two, raising the non-U.S. citizen person protections to the level that the official bodies of these international organizations that we've talked about say they should be?

If you come out on the second, what specific criteria do we have to go on as to what those practices would be?

In other words, there's a slightly cynical end to the question, what would be the additional protections in real time to privacy interests of non-U.S. persons if the U.S. took a position that the ICCPR does apply to our activities outside territorial U.S., but that we've already met those standards, such as seems to be the case with some of the other countries who espouse the official broader interpretation of ICCPR but then go on their way, as Mr. Wolf suggested, and don't really raise those?

MS. PITTER: This is to me?

MS. WALD: Yes, this is to you.

MS. PITTER: So, I mean I think one clear change that needs to be made is the purpose of the surveillance needs to be much more targeted. The definition of foreign intelligence information is just much too broad. It encompasses, you know, things that, conversations that could be just about generally the foreign affairs of the United States.

And I know we heard in the panel testimony earlier that that is somewhat reined in by certifications but those are not public and we've not seen them.

There should be a lot more transparency in the law. I think the difference in the German law is that there is a lot more transparency. The capacity also is less in Germany. I mean the U.S. has vast capacity, so you know it affects a lot more people.

But definitely a more narrow, a more targeted approach, and applying, you know, necessary and proportionate principles to the

surveillance as well, I think would go a long way.

There's probably plenty of room for recommendations. I probably can't get into all of them here but that would be --

MS. WALD: In general would your standard be that there should be a presumption that we treat non-U.S. persons like U.S. persons in our surveillance activities, or rather that we go to the best practices we can pull from that people who endorse the ICCPR, even if we don't actually endorse that application?

MS. PITTER: So I think that there can be differences in the law itself but it has to, the differences have to be ones that don't impair the impact of the right itself.

So the right to privacy has to be part of, it has to be made part and parcel of the assurances, but they can be different for practical reasons when it comes to --

MS. WALD: Can you give us, in my remaining few seconds, some application of what you've just said to 702?

MS. PITTER: Well, I'd like to go into, you know, a more detailed analysis here but right now there's --

MS. WALD: Well, just quickly.

MS. PITTER: There's not a warrant requirement, for example, under 702 for individuals, but there should be -- it may be that it's not a practical requirement to have a warrant for individuals outside of the United States.

And it's not just individuals under 702, it's also facilities and about targeting as well.

But the procedures that are in place to protect against sort of suspicionless, you know, there's no standard for what authority has to find before it can target an individual. The main distinguishing principle is that it's a foreigner, and that that information is going to be acquired for foreign intelligence purpose, for foreign intelligence purpose, so that is too broad.

MS. WALD: Okay.

MS. PITTER: Does that make sense?

MS. WALD: Yes. All right, very quickly I guess, Mr. Wolf, your testimony, you know, recited the report about the lesser, basically the lesser protections most other countries including our close allies give to privacy, at least despite some of their countries adherence to the ICCPR's broader definition of privacy, yet you also note that the economic risks to U.S.-based telecommunication companies from threats both from competing companies inside those countries and from the governments themselves that they may balkanize and insist on collection and storage activities being conducted in-country poses a real risk.

Is it above your pay grade to give us some indication of what line or policies the U.S. should follow given those two competing concerns?

MR. WOLF: Well, I think our concern in doing the work that we did on the white paper was the misperception that was arising --

MS. WALD: Let's assume you've done those and that they are real, but also are real

the threats to the competitiveness of U.S. companies if foreign governments and peoples get very excited and want to keep everything inside their own countries.

MR. WOLF: So our position is that they're deceiving themselves if they think that when they keep data presumably within the four borders, four corners of their own country that it's safer from surveillance, not only from their own surveillance authorities, but of course through the sharing arrangements from surveillance authorities from elsewhere around the world, and that the Balkanization of data is not a useful global phenomenon at all.

MS. WALD: Well, what can the U.S., or what could we recommend they bring them together?

MR. MEDINE: Judge, your time has expired. Mr. Dempsey.

MS. WALD: Right. You can think about it.

(Laughter)

MR. DEMPSEY: On my last round we were

talking about what were, if any country's laws that did a better job here, and Mr. Garfield, you were ready to jump in. Do you remember what you wanted to jump in on? I wanted to give you a chance to make the point, if you still remember what it was.

MR. GARFIELD: It really was the point that was made in response, which is that in fact our experience in carrying out our business is that there aren't many, if any, other countries that have as many safeguards in place.

The lack of open discussion through multinational engagement as well as transparency here in the U.S. furthers that false perception that somehow other nations are doing more than we are. And that is certainly something that whether through legislation or recommendations from the PCLOB, we can do something about.

MR. DEMPSEY: The question for Laura Pitter, a couple of other witnesses have raised this and a couple of times I grabbed for the book in order to raise it and didn't get a chance to,

the definition of foreign intelligence, as I read it, it means information that relates to the ability of the United States to protect against actual or potential attack, grave hostile acts of a foreign power, sabotage, international terrorism, international proliferation of weapons of mass destruction, or clandestine intelligence activities. None of those are too broad, I would think.

And then it says, information with respect to a foreign power or foreign territory that relates to the conduct of the foreign affairs of the United States.

I mean isn't that precisely what foreign intelligence is supposed to be about, information with respect to what foreign countries are doing that might affect our foreign affairs? Why is that too broad?

MS. PITTER: I think that the first category of information that you said could, it would be permissible. But the general foreign affairs of the United States allows for the

collection of a vast amount of information that does not necessarily have any national security purpose.

MR. DEMPSEY: No, but it has foreign affairs purpose. It is by definition about the intent of foreign governments, and are you saying that other countries self-restrain themselves from trying to understand what their adversaries are doing, even in matters that don't involve attack and so on?

MS. PITTER: I mean if other country's laws are overbroad and vague then they're in violation of, you know, the International Covenant on Civil and Political Rights as well.

MR. DEMPSEY: Well, I think John would say that if everybody is doing it, it probably isn't a violation of the treaty. Everybody didn't bind themselves not to do what they all were doing at the time they bound themselves to the treaty.

MS. PITTER: Well, you know, the revelations about how this is applied are just coming out now and there are going to be

challenges and there already are challenges to the law.

And I think we're going to find that there is room certainly for reining in the overbroadness of some of the statutes as they exist right now.

I think that because it allows for the communications of things that don't necessarily have to do with national security, that it just, it's overbroad and it's impacting, you know, the United States in other ways.

MR. DEMPSEY: In what way is the collection of information about foreign affairs overbroad?

MS. PITTER: Because it could be, you know, someone talking about, you know, their opinions about the foreign affairs of the United States --

MR. DEMPSEY: Not someone talking about their opinions, it's the information with respect to a foreign power. So this is not Joe Schmoe in Germany saying I like or don't like the United

States, this is about what Germany thinks about the United States.

MS. PITTER: It merely has to relate to the foreign affairs of the United States --

MR. DEMPSEY: Yes.

MS. PITTER: In my opinion it's too broad. It allows in for much too broad a type of communication.

MR. DEMPSEY: No, I'll yield. I'd like to have another round, a third round if we could, but I'll yield for now.

MS. COLLINS COOK: Mr. Bellinger, I think you had put your finger up midway through that and I'd like to follow on this conversation as well because it struck me.

First, where would you draw the line? And I'm struggling to determine what precisely is impermissible about collecting foreign intelligence in the category of foreign affairs as set forth in FISA.

MR. BELLINGER: Yeah, so thanks for that question. And I think this is a very

important point, and Judge Wald started it and you have continued it.

We have to be really very clear about what international law is. International law is not principles that we think would be fine, policy principles that you and I might agree.

International law, if we are serious about international law, and this actually is the definition of international law, are things that nations agree to, to be bound by, by treaty or that is customary internationally, meaning that countries do it so often that everybody does it and they do it by a sense of binding legal obligation.

So two points here, and Judge Wald, I heard you say that while it is true that other countries actually take a broader definition of whether the ICCPR applies extra-territorially, I'm not aware of any country in the world that believes that the ICCPR actually binds them with respect to electronic surveillance, that that right to privacy in Article 17 actually limits

their ability to conduct electronic surveillance of foreign nationals. So that is just not a treaty obligation that countries have accepted, even under the ICCPR.

It might be something that human rights groups wish were the case, but it is not something that governments have accepted, and certainly not something the United States government has accepted.

And then just one more round on the Human Rights Committee. Again, the treaty itself does not say that the decisions of the Human Rights Committee, which is basically a group of academic experts, are binding. Governments who write treaties know how to write language.

For example, the U.N. Charter says that we undertake to comply with rulings of the ICJ. But the human rights monitoring groups, countries have not said that we undertake to comply with their decisions.

And in fact, the senate, and all of you know this, the senate would never agree to cede

responsibility for the future interpretation of a treaty to a group of academic experts. That would take completely out of the hands of the shared understanding between the executive and senate, the interpretation of a treaty.

So you know, the United States, and this is the view of the Obama administration as well, you know, recognizes that other people may not agree on the extraterritorial application of the ICCPR, but you know, no country believes that the ICCPR actually limits electronic surveillance.

MS. COLLINS COOK: So I just wanted to as a follow-up question to Ms. Pitter. Thank you. I know we've aimed a lot of our questions at you.

I think there's a sense within the United States government, a little bit of exasperation, the concern is that our surveillance lacks transparency or that we are somehow outside the mainstream of what other countries are doing.

And I look at 702 in particular and I see something where our legislative branch has specifically said exactly what our executive

branch can do. The executive branch, which is headed by democratically accountable individuals then oversees the execution of that authority, it is subject to the oversight of the judicial branch and it is subject to the oversight of our legislative branch.

So I guess my question is systemically what else could the United States be doing to help build the confidence and trust of other countries?

MS. PITTER: So the oversight so far has all been in secret. I think that's one problem. I mean even the first panel today said they were in the process of declassifying a large number of documents and they were looking at doing that because they recognize the importance of transparency.

The oversight has not, I mean if you look at what happened with 215, even --

MS. COLLINS COOK: I was talking about Section 702, which is the focus of our --

MS. PITTER: We don't know the details of the oversight regarding 702, so the only

information I have about oversight would be regarding 215. And we saw that the judicial oversight in that context, you know, would up, there was an opinion that had an impact on the vast number of communications of Americans that was kept secret from the Americans, so --

MS. COLLINS COOK: Well, let me push back a little bit on this notion that the oversight is not transparent.

So again, we have a statute that tells the world exactly what the executive branch must present to the judiciary, what findings the judiciary must make, what authority judiciary has vis-a-vis that application, and the framework for this surveillance.

We have a public statute that also tells you exactly what the executive branch is obligated to share with Congress. So where's the lack of transparency in that?

MS. PITTER: Well, the judicial oversight for the 702 program is annual. They look at just the procedures. They don't actually

look at the individual targeting requirements. That's done by an NSA analyst at his computer desk.

MS. COLLINS COOK: Actually I think if you were here for the first panel the testimony by the first panel was that that is not in fact the case, that it is an ongoing process of oversight. There are regular reporting requirements, both to the court and to the Congress, so.

MS. PITTER: I was, I did hear the first panel, and I believe he said that those targeting decisions by the analysts are reviewed eventually, but it's not something that's done at the beginning. So the --

MS. COLLINS COOK: So if there's not public review of specific targeting decisions, so this, the United States government saying we would like to collect foreign intelligence information about this specific selector, that's a lack of transparency that is problematic for you?

MS. PITTER: Well, the transparency, even the certifications that the FISC court gets,

there's no, they don't even see the identifiers or the selectors, they just approve the procedures. So you know, that's a problem with the oversight. In terms of --

MR. MEDINE: I'm going to let Ms. Brand pick up since we're at time. So thank you.

MS. BRAND: Okay. I guess maybe this question is directed at John but if anyone wants to jump in, that's fine.

If the ICCPR did have application to the U.S. government surveillance of non-U.S. persons abroad, setting aside the territorial issue for a minute, what does privacy mean in that context?

I have found the lack of a universally accepted definition of privacy very frustrating writ large across everything that we do, and I mean the same issue pertains here. So I guess is there a universally accepted definition of privacy? Is there a definition of privacy that is binding on the U.S. government? If not, how would we find, who would supply such a definition? If

you can sort of help us understand that.

MR. BELLINGER: Yeah, so that's a great question. And that's really the third prong. I mean the reason that the ICCPR doesn't apply is, one, there's the within its territory and subject to its jurisdiction. Then even if it were subject to our jurisdiction, then it has to be within the power and control.

And you know, no one is really going to legitimately argue that, as I think you said earlier, power and control in the view of those who take that interpretation of power and control is someone that you actually physically have in your custody, not electronic surveillance.

And then there's the issue, even if those applied, is something unlawful or arbitrary violation of privacy? And there are not definitions that are universally accepted.

You know, people can argue about these things but for it to be law that a country actually violates, there has to be an agreed definition on privacy and there has to be an

agreed definition on what is arbitrary, and there just are not those definitions.

You know, again, someone can say that someone has an absolute right not to have any country pry into anything that they're doing and that that's a violation of their privacy, but there's not an accepted definition of that.

I mean I could frankly imagine if one were to accept the first part of your premise, which is that it were to apply extra-territorially, and let's also say that it were someone within the U.S. jurisdiction, let's say someone, the United States is actually holding a terrorist in another country and we agreed that the ICCPR applied, we agreed the person was within our power and control, and then we were to do extensive interviews of that person about the person's private life, and then we just publish it willy-nilly, not as part of a criminal proceeding but essentially just as a leak, well, you know, there might be an argument that that might be an arbitrary intervention with that person's right to

privacy.

But I think that's -- there's not a definition of privacy, or of arbitrary, or unlawful that is binding as a matter of international law.

MS. BRAND: Chris or Laura, any thoughts on that question?

MS. PITTER: Would you repeat that question again?

MS. BRAND: Just what does privacy mean in the ICCPR context? Where does the definition come from? How would you find the definition?

MS. PITTER: Well, it guards against unlawful and arbitrary interference with an individual's privacy, so there has to be a respect for correspondence, for example, and a respect for an individual's personal space, and there has to be an ability to have personal space to communicate.

MS. BRAND: Where are you getting that definition?

MS. PITTER: Well, that's, I mean

that's coming from the interpretation of, the right to privacy is connected to freedom of expression, freedom of association. It impacts that. And you know, the right to correspondence comes from that as well. So I mean it's defined in the treaty itself, and --

MS. BRAND: What is the definition? Humor me.

MS. PITTER: I mean --

MS. BRAND: I can look it up, never mind. But it sounds like what you're giving me is sort of your sense of what privacy entails, not a sort of legally defined or legally articulated definition. Chris?

MR. WOLF: So a privacy lawyer's answer goes back to Brandeis and Warren who said the right to privacy is the right to be left alone. But they recognized and I think it's been recognized ever since, that was 1890, that there are exceptions for the good of society, for law and order, for social good.

And that's really where the rubber hits

the road. What are the permissible exceptions for national security surveillance? And you know, that's the discussion that needs to be had globally.

You know, Judge Wald asked what should the U.S. government do? I think it should promote that discussion as a global matter, and at the same time I think it should promote the decoupling of national security surveillance from cross-border data flows for commercial purposes.

The threat to withdraw safe harbor, for example, the declaration that the transatlantic trade and investment partnership shouldn't address data because of what happened with national security surveillance is a non sequitur.

Those issues need to be dealt with between governments, but that shouldn't interfere with cross-border data flows, which have to have privacy protections built-in, no question. But those are not something, that isn't something, the surveillance issue is not something that the companies themselves can really address and

they've done about as much as they can in pushing for transparency, pushing very hard.

MR. MEDINE: Dean, did you want to add something?

MR. GARFIELD: The question was asked earlier about what the appropriate venue is and I would say a reminder that the strategic and economic dialogue didn't exist beyond five years ago, and so this is one issue that's getting left behind in the discussion, the importance of creating a framework and a venue for greater multinational dialogue around the surveillance issue. And I think the PCLOB in its recommendations can have a dramatic effect in this area.

MR. SIEBER: It's clear that we have not an international definition because the countries are too different. However, in the countries and national law, and European law and in other legal bodies these definitions are emerging. And of course they have to develop.

What is sure is that there is a core

area of privacy where we all would agree that privacy is infringed. For example, if you directly do intelligence gathering on the sexual life of somebody who is not a suspect, there's no reason, that's a clear core area infringement of privacy.

Now if you go further, it's becoming of course a difficult, mass surveillance of people against which there is no suspicion would be one aspect where we'd have to investigate.

Another one is to create a complete picture of the private life of somebody going back to his birth, whatever did he do, did he demonstrate in school? So collecting enormous mass of data on one person would be another aspect, just illustrating. There are cases which fall under something like that.

And we should work on this definition and the fact that we do not have something like that would not lead me to the conclusion we shouldn't go in these things.

It's the same with this attitude on

extraterritorial application and things like that. These questions are so new that you cannot find any government's position here. So for me, that's not a valid argument. If you are pioneers on these questions, we cannot say the governments are not yet there.

I agree with you it's a political question on this issue.

One final point where I do not agree what was said is the question with respect to territoriality. If you are collecting data in a foreign country from (inaudible) it's clear that's legal. You are not infringing the foreign territory.

But if you go to a foreign territory and you switch on servers, you download countries -- the electronic pulses, you are changing and you do a function that usually the police does, this is a clear infringement of territoriality.

And you can see this especially in the cyber crime convention where we are fighting about these questions. We have Article 32 B with a big

struggle between the U.S. and Russia, which is bringing down the complete process of the cyber crime convention. We all agree that except these cases mentioned in Article 32 of the cyber crime convention ratified by the U.S., any police activities doing access to foreign countries are of course infringements of privacy. Nobody would claim that this is legal. We could stop the process of the cyber crime convention if your statement would be, all right, like that in this generality.

So I would say that we have to remain -- these surveillance activities do not in any case infringe territoriality but there are many cases, especially looking at the cyber crime convention, our agreements which we have on this committee, we all would say that's a clear infringement of the sovereign territoriality of a country. And it is also undisputed that the protection of territoriality is guaranteed, not only by Article 2 of the U.N. Charter, but also by customary law. It's one of the basic principles

since the Westphalia Peace Accord.

MR. MEDINE: Let's give John a chance to respond.

MR. BELLINGER: I'll be brief. On the second point, again I would say that I don't think any country in the world would say that the Article 2 of the U.N. Charter's protection of the territorial integrity and sovereignty of states would mean that they cannot conduct essentially espionage activities from anywhere. I just don't think that's what the U.N. Charter says.

But more importantly, the first thing you said really goes to the heart of our discussion here, where you said this is an evolving national dialogue about privacy and it is a dialogue that is going on nationally in different countries, and it therefore is going on internationally.

But the question at least that was put to several of us, to me and Laura in particular is, is there a binding international law standard right now? And the answer to that is clearly no.

Germany may have laws inside Germany, given its particular past. Other countries may have particular national laws. Sooner or later countries may get together and agree on things, but right now there is not an international legal standard, either in the ICCPR or anywhere else that limits electronic surveillance from the United States, or again, from any other country.

Other countries would not agree that there's not an international legal standard -- or that there is an international legal standard.

MR. MEDINE: We have time for just a quick round that Jim had requested. Let me just ask just to clarify one point, John, the treaty ICCPR is not self-executing. What does that mean and is there any forum in which enforcement action could take place?

MR. BELLINGER: That means that it would require implementing legislation for it to be, so it's binding as a matter of international law and we have implemented it already and are in compliance with it in certain ways because of laws

that we already had on our books, or might thereby have our Congress pass. But it does not have automatic legal effect merely by the United States becoming party to it.

MR. MEDINE: And is there any forum in the world where we could be held accountable for compliance with the ICCPR?

MR. BELLINGER: The U.N. Human Rights Committee monitors our compliance and comments upon things that we are doing. That's what happened last week when we presented our report. And the United States commented on or responded to these comments, but that's not judicially or legally enforceable.

MR. MEDINE: Thanks. Judge Wald.

MS. WALD: Just a quick comment. Am I not right, John, that not in this context of surveillance, but hasn't England at times relied in some of its judicial decisions on the ICCPR for the, to disallow, I think in dealing with some detainees or asylum people, etcetera?

So my impression was there are courts

who have actually relied upon the ICCPR, not in the surveillance context but in other contexts.

MR. BELLINGER: You and I would have to look at those together. It may have been the European Convention on Human Rights. There has been a fair amount of jurisprudence recently on the extent to which the European Convention on Human Rights creates obligations on British and European forces who actually do have someone within their control of their military outside of Britain, or Germany, or elsewhere.

MS. WALD: Okay. I'll let you off. Very quickly I have one question, quickly, for Mr. Garfield, and that is that the statement that your organization provided to us spoke of the need for meaningful oversight by an independent body in government as to the surveillance programs, including access to collected data.

Just wondered very quickly, who you had in mind, was it the IGs, us, FISA, Congress? Did you have particular independent bodies who would provide the meaningful insight, which included in

your statement oversight of collected, access to the collected data?

MR. GARFIELD: We did not.

MS. WALD: Okay, that's a succinct answer.

MR. MEDINE: Gives you a concise answer.

MR. DEMPSEY: Rather than a question I'll just offer an invitation, which is if any of the witnesses could provide us with guidance on the question I posed, what would be a better way of structuring a foreign intelligence system.

I think at the end of the day any concept of law, any set of rules is going to recognize that different countries are going to have somewhat different structures. So the German structure is robust but different from the United States. The United States believes it has a robust system with different elements than Germany has, etcetera.

Has anybody put together or could anybody put together a list of the elements of a

system and then some sense of how you come up with what is the minimum?

We talked a lot about judicial oversight but Germany does not have. The court reviews the statutory structure but not the individual implementation, does not do individual targeting on the strategic surveillance in Germany. In the U.K. it's all administerial, not judicial.

Secondly, if any further thoughts on how we get from here to there. So several witnesses have said it's an evolving situation. We have new questions, questions which to my view are not answered in the existing documents. Let's just say that it's not answered. They don't apply. No one thought about this. It hasn't been answered. How do we move forward, we, the world, or maybe the U.S. and Europe, which have more shared values than we sometimes admit, how do we move forward in getting that kind of commitment?

And the industry in Garfield's paper is that a global, I think implicitly recognizes we

need global understanding, even if not all of the laws are the same.

So any thoughts that you can offer us. Not right now because we want to move along, but any further follow-up thoughts you could offer us in writing, please, it would be very helpful on both of those points.

MS. COLLINS COOK: I just wanted to thank you all for coming. As I said at the beginning I think it's important to have these discussions. I won't assign homework or request any follow-up, but it's an education process for us, as well as for the American people, particularly on these issues.

So if there is information you think should be a part of the public record, which will remain open, I'm sure David will explain, it is welcomed.

MS. BRAND: I won't take up anymore of your time since we are at the end of our schedule here. But I want to thank all of you for coming. It was very helpful to me, so thank you for taking

the time to prepare and to be here.

MR. MEDINE: Thanks again to all the speakers and the Board staff that made this hearing possible. The Board's activities for today are now complete.

The Board encourages all those who are interested to submit, panelists and members of the public, to submit written comments on this topic at our website of www.regulations.gov. And the deadline for submitting comments is March 28th. All comments submitted will be available for review by the public. A transcript of today's hearing will be posted on PCLOB.gov.

And I will now move to adjourn the hearing. All in favor of adjourning the hearing please say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous consent to adjourn, we will now adjourn. The time is 3:40. Thank you.

(Whereupon, at 3:40 p.m., the hearing was adjourned.)

CERTIFICATION

I, LYNNE LIVINGSTON, A Notary Public of the State of Maryland, Baltimore County, do hereby certify that the proceedings contained herein were recorded by me stenographically; that this transcript is a true record of the proceedings.

I further certify that I am not of counsel to any of the parties, nor in any way interested in the outcome of this action.

As witness my hand and notarial seal this _____ day of _____, 2013.

_____

Lynne Livingston

Notary Public

My commission expires: December 10, 2014

B

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix R

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

Follow-up Questions Regarding Section 702 Certifications
June 17, 2011

1. The government's Response to the Court's Briefing Order of May 9, 2011 ("June 1 Submission") states that Internet transactions acquired by NSA in its upstream collection may contain not only multiple discrete communications (some of which are neither to, from, nor about a tasked selector), but also [redacted] June 1 Submission at 25.

a. Please provide some examples of the [redacted] For instance, could such acquisitions include [redacted]

b. What is the likelihood that such [redacted] pertain to persons other than the users of tasked selectors, including persons in the United States or U.S. persons?

2. The June 1 Submission states that "no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication." June 1 Submission at 9.

a. What is meant by "wholly domestic communication" in this statement? Does the term include the discrete communications that might be embedded within acquired transactions?

b. What is the likelihood that an analyst viewing information obtained through a transactional acquisition would have a basis for determining that a discrete communication embedded within the transaction is purely domestic?

3. a. Might the non-targeted portion of a transaction ever be the sole basis for that transaction being responsive to an analyst's query?

b. Upon retrieving information in response to a query, can an analyst readily distinguish that portion of a transaction that contains the targeted selector from other portions of a transaction?

4. a. Please describe the manner in which the government minimizes discrete communications and other information that is contained within acquired Internet transactions but that is neither to, from, nor about the user of a targeted selector.

b. In particular, please explain how the government applies the provisions of NSA's minimization procedures that use the term "communication" to the discrete communications and other non-target information contained within the transactions that are acquired. See, e.g., NSA Minimization Procedures § 2(c) (defining "[c]ommunications of a United States person"); § 2(e) (defining "foreign communication" and "domestic communication[]"), § 3(b)(4) (discussing determination whether a communication is "foreign" or "domestic"), and § 5 (discussing handling of domestic communications).

c. Would all communications and [redacted] within a transaction be treated the same when the minimization procedures are applied, or would there be different treatment?

5. a. Once NSA has identified a portion of a transaction that does not contain targeted information, is it possible to mask or otherwise minimize the non-target information contained within the transaction?
b. Why is NSA unable to delete and replace, or alter, an original transaction that contains non-target information? See June 1 Submission at 27-28.

6. The government states that an Internet transaction that is acquired "is . . . not divisible into the discrete communications within it even once it resides in an NSA corporate store." June 1 Submission at 22. Please reconcile that statement with the government's acknowledgment that "an analyst would . . . be able to copy a portion of the rendered view of a transaction contained in a NSA corporate store and then paste it into a new record on a different system." Id. at 27 n.25.

7. Please reconcile the government's statement that the "communicants" of to/from communications are "the individual users of particular selectors" (see June 1 Submission at 30) with [redacted] elsewhere in its response to the Court's questions (see, e.g., id. at 6 (discussing application of IP filtering)).

8. What is the factual basis for NSA's assertions that "a United States person would use [redacted] only in a minute percentage of cases" and that "[redacted] See June 1 Submission at 11, 12.

9. What is the factual basis for NSA's suggestion that [redacted] See June 1 Submission at 8 n.9

10. The government repeatedly characterizes as "unintentional" NSA's collection of discrete non-target communications as part of transactional acquisitions, [redacted] Assuming arguendo that such collection can fairly be characterized as unintentional, please explain how 50 U.S.C. § 1806(i) applies to the discrete, wholly domestic communications that might be contained within a particular transaction.

11. Please provide a thorough legal analysis supporting your view that the knowing and intentional acquisition of large volumes of Internet transactions containing discrete communications that are neither to, from, nor about a targeted selector (as well as other information not pertaining to the users of targeted selectors) is merely "incidental" to the authorized purpose of the collection as a whole, and therefore reasonable under the Fourth Amendment.

12. The statute requires the targeting procedures to "be reasonably designed to ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States and [to] prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). How can procedures that contemplate the knowing acquisition of huge volumes of transactions that will include quantifiable amounts of information relating to non-targets, including information of or about U.S. persons abroad or persons located in the United States, meet this statutory requirement?

13. In its discussion of the Fourth Amendment, the government asserts that "upstream collection" in general is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs." June 1 Submission at 16.

a. To what extent can the same be said for the acquisition of Internet transactions [redacted] in particular?

b. Is the acquisition of Internet transactions via upstream collection the only source for certain categories of foreign intelligence information? If so, what categories?

c. Please describe with particularity what information NSA would acquire, and what information NSA would not acquire, if NSA were, in comparison to its current collection, to limit its acquisition of Internet communications to: (1) acquisitions conducted with the assistance of [redacted]; and (2) the upstream collection of discrete communications to, from, or about tasked selectors that are [redacted] (id. at 2, n.2).

14. The Fourth Amendment also requires the Court to examine the nature and scope of the intrusion upon protected privacy interests. How can the Court conduct such an assessment if the government itself is unable to describe the nature and scope of the information that is acquired or the degree to which the collection includes information pertaining to U.S. persons or persons located in the United States?

15. In light of the government's emphasis on the limited querying of Section 702 acquisitions that is currently permitted (see June 1 Submission at 23), why is it reasonable and appropriate to broaden the targeting procedures to permit querying using U.S.-person identifiers?

16. The government acknowledges that it previously "did not fully explain all of the means by which . . . communications are acquired through NSA's upstream collection techniques" (June 1 Submission at 2), yet states that the "[Attorney General] and [Director of National Intelligence] have confirmed that their prior authorizations remain valid" (id. at 35). At the time of each previous Certification under Section 702, were the Attorney General and the Director of National Intelligence aware that the acquisitions being approved included Internet "transactions" [redacted]? If so, why was the Court not informed. If not, why are the prior Certifications and collections still valid?

~~SECRET//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

2011 JUN 28 PM 4:51

WASHINGTON, D.C.

[redacted]

NOTICE OF FILING OF GOVERNMENT'S RESPONSE
TO THE COURT'S SUPPLEMENTAL QUESTIONS OF JUNE 17, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits the attached factual and legal response to the

~~SECRET//ORCON,NOFORN~~

Classified by: ~~Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ~~
Reason: 1.4(c)
Declassify on: ~~28~~ June 2036

supplemental questions provided by this Court to the Government on June 17, 2011, concerning the above-referenced matters. Given the complex nature of the Court's questions and the Government's responses, the United States is prepared to provide any additional/supplemental information the Court believes would aid it in reviewing these matters. The Government may also seek to supplement and/or modify its response as appropriate during any hearing that the Court may hold in the above-captioned matters. ~~(S//OC,NF)~~

Respectfully submitted,

[redacted]

[redacted]

National Security Division
United States Department of Justice

~~SECRET//ORCON,NOFORN~~

VERIFICATION

I declare under penalty of perjury that the facts set forth in the attached Government's Response to the Court's Supplemental Questions of June 17, 2011, are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 28th day of June, 2011. ~~(S)~~

[redacted]

Signals Intelligence Directorate Compliance Architect
National Security Agency

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

GOVERNMENT'S RESPONSE TO THE COURT'S FOLLOW-UP QUESTIONS OF JUNE 17, 2011

1. The government's Response to the Court's Briefing Order of May 9, 2011 ("June 1 Submission") states that Internet transactions acquired by NSA in its upstream collection may contain not only multiple discrete communications (some of which are neither to, from, nor about a tasked selector), but also [redacted] June 1 Submission at 25.

a. Please provide some examples of the [redacted] For instance, could such acquisitions include [redacted]

b. What is the likelihood that such [redacted] pertain to persons other than the users of tasked selectors, including persons in the United States or U.S. persons?

As was more fully explained in the Government's June 1 Submission, the presence of a tasked selector is required in order for the National Security Agency's (NSA) upstream Internet collection devices to identify and then acquire Internet communications in the form of transactions. *See* June 1 Submission at 1, 24-26. The Court's question in 1.a. further asks whether such transactions could include [redacted]. Personal information, including that of persons other than a user of a tasked selector, could be acquired by NSA in relation to any one or more of these communication services to the extent it is included within a transaction. This, however, is true even with respect to discrete communications to,

[1] [redacted] ~~(S)~~

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

Classified by: ~~Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ~~
Reason: 1.4(c)
Declassify on: ~~28 June 2036~~

from, or about a tasked selector, depending on what the communicants chose to include within, the communication. [redacted] ~~(TS//SI//NF)~~

Although personal information may be included in a transaction, the manner in which NSA conducts its upstream collection significantly diminishes the likelihood that such information would pertain to U.S. persons or persons in the United States. As discussed more fully in the Government's response to question 14 below, NSA acquires certain transactions because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's targeting procedures, is a non-United States person reasonably believed to be located outside the United States. NSA acquires transactions that contain a discrete communication about a tasked selector using technical means that are designed to ensure that such acquisition is directed at a person reasonably believed to be located outside the United States. The Court has previously recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, Docket No. 105B(g):07-01, Mem. Op. at 87 (USFISC April 25, 2008) (footnote omitted) (hereinafter "*In re Directives to Yahoo!* Mem. Op."). Thus, it is reasonable to presume that most of the discrete communications that may be within an acquired transaction are between non-United States persons located outside the United States. ~~(TS//SI//OC/NF)~~

2. The June 1 Submission states that "no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication." June 1 Submission at 9.

a. What is meant by "wholly domestic communication" in this statement? Does the term include the discrete communications that might be embedded within acquired transactions?

By "wholly domestic communication" the Government means a communication as to which the sender and all intended recipients are located within the United States. The Government includes within this term any discrete communication within a transaction where the sender and all intended recipients of the discrete communication were located in the United States at the time the communication was acquired. With the previously described limited exception involving [redacted] NSA analysts have yet to identify a wholly domestic communication in any transaction acquired through NSA's upstream collection systems. ~~(TS//SI//NF)~~

b. What is the likelihood that an analyst viewing information obtained through a transactional acquisition would have a basis for determining that a discrete communication embedded within the transaction is purely domestic?

The likelihood that an NSA analyst would recognize that a transaction containing either a discrete communication (e.g., an e-mail message) or multiple discrete communications [redacted] contains a wholly domestic communication depends on a number of factors, including: [redacted] ~~(TS//SI//OC/NF)~~

3.a. Might the non-targeted portion of a transaction ever be the sole basis for that transaction being responsive to an analyst's query?

Yes. All information acquired by NSA as a result of tasking the targeted foreign person's selector -- whether initially determined to be foreign intelligence information to, from, or about that targeted foreign person (or foreign intelligence information concerning other foreign persons or organizations) or incidentally acquired information concerning other currently non-targeted persons -- can be queried by analysts for foreign intelligence information. As a result, it is possible that any portion of a transaction could be the sole basis for that transaction being responsive to an analyst's foreign intelligence query of NSA databases. Such queries (which are subject to review), however, must be formulated by an analyst in accordance with NSA minimization procedures which require that computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, be limited to those selection terms reasonably likely to return foreign intelligence information. *See, e.g.,* Amendment 1 to

[2] [redacted] ~~(TS//SI//NF)~~

DNI/AG 702(g) Certification [redacted] Ex. B, filed Aug. 12, 2010, § 3(b)(5) (hereinafter "Current NSA Minimization Procedures").[3] ~~(TS//SI//NF)~~

3.b. Upon retrieving information in response to a query, can an analyst readily distinguish that portion of a transaction that contains the targeted selector from other portions of a transaction?

Yes. The tasked selector that resulted in NSA's acquisition of any particular transaction is discernable by analysts reviewing information in response to a query. The analytic tools used to display an acquired transaction allow NSA analysts to identify the tasked selectors that resulted in the acquisition of the transaction, thereby enabling analysts to determine the portion(s) of the transaction in which that selector appears. In some instances, the analyst may need to review the entirety of the transaction (including the underlying metadata or raw data) to identify where the tasked selector appears, but even in these situations, the tasked selector is included and identifiable. [redacted] ~~(TS//SI//NF)~~

4.a. Please describe the manner in which the government minimizes discrete communications and other information that is contained within acquired Internet transactions but that is neither to, from, nor about the user of a targeted selector.

4.b. In particular, please explain how the government applies the provisions of NSA's minimization procedures that use the term "communication" to the discrete communications and other non-target information contained within the transactions that are acquired. See, e.g., NSA Minimization Procedures § 2(c) (defining "[c]ommunications of a United States person"); § 2(e) (defining "foreign communication" and "domestic communication[]"), § 3(b)(4) (discussing determination whether a communication is "foreign" or "domestic"), and § 5 (discussing handling of domestic communications).

4.c. Would all communications [redacted] within a transaction be treated the same when the minimization procedures are applied, or would there be different treatment?

---

[3] The Government seeks the Court's approval of revised NSA Section 702 minimization procedures that would enable NSA analysts to use United States person identifiers as selection terms if those selection terms are reasonably likely to return foreign intelligence information. *See, e.g.*, DNI/AG 702(g) Certification [redacted], Ex. B, filed Apr. 20, 2011, § 3(b)(5) (hereinafter "Proposed NSA Minimization Procedures"). Under these revised NSA Section 702 minimization procedures, the use of such selection terms must be approved in accordance with NSA procedures designed to ensure that the selection terms are reasonably likely to return foreign intelligence information. *Id.* The Government is still in the process of developing the NSA procedures governing the use of United States person identifiers as selection terms. Until those procedures are completed, NSA analysts will not begin using United States person identifiers as selection terms. ~~(TS//SI//NF)~~

As required by FISA, *see* 50 U.S.C. §§ 1881a(e), 1801(h), and 1821(h), NSA's minimization procedures address the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons. *See* Current Minimization Procedures, § 1.[4] When NSA acquires an Internet transaction that contains multiple discrete communications, NSA considers each of those communications to be separate "communications" under its minimization procedures. Thus, for example, an NSA analyst would consider each discrete communication within a larger Internet transaction as a separate communication for purposes of determining whether the communication is a foreign or domestic communication under NSA's minimization procedures. *See, e.g.,* Current and Proposed NSA Minimization Procedures, § 2(e). ~~(TS//SI//OC/NF)~~

The manner in which acquisitions are conducted under Section 702 operates to minimize the acquisition of information about United States persons. First, certain transactions are acquired because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's FISC-approved targeting procedures, is a non-United States person reasonably believed to be located outside the United States. This Court has recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!* Mem. Op. at 87 (footnote omitted). Accordingly, it is reasonable to presume that most of the discrete communications that may be within the acquired transaction -- even those that are not to or from a tasked selector -- are between non-United States persons located outside the United States. Second, with respect to transactions that contain a discrete communication about a tasked selector, the technical means by which NSA prevents the intentional acquisition of wholly domestic communications are designed to ensure that the acquisition of transactions is directed at persons reasonably believed to be located outside the United States. As a result, these persons reasonably also can be presumed to be non-United States persons, and most of their communications -- including those that are not about a tasked selector -- can be presumed to be with other non-United States persons located outside the United States. *Id.* This combination of targeting non-United States persons located outside the United States and directing acquisitions at persons located outside the United States operates to significantly diminish the amount of information pertaining to United States persons or persons in the United States that NSA acquires through its upstream collection. *See* [redacted] Mem. Op. at 23 (recognizing that "[t]he targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that U.S. person information will be obtained"). ~~(TS//SI//OC/NF)~~

To be sure, it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain U.S. person information. The acquisition of such information is an unavoidable by-product of the acquisition of the foreign intelligence information (i.e., the communication to, from, or about a tasked selector) within the transaction. Yet it is important to note that, for purposes of the application of NSA's current and proposed minimization procedures, the Government does not consider its acquisition

[4] NSA's proposed minimization procedures currently before the Court address these same issues. *See* Proposed NSA Minimization Procedures § 1. ~~(S)~~

of a discrete communication within a transaction that is not to, from, or about a tasked selector to be "inadvertent." Subsection 3(b)(1) of NSA's current and proposed minimization procedures require inadvertently acquired communications to be destroyed if they are "identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or as not containing evidence of a crime which may not be disseminated under these procedures." Current and Proposed NSA Minimization Procedures, § 3(b)(1). ~~(TS//SI//NF)~~

As described below in the Government's response to question 10, the Government considers a discrete communication that is not to, from, or about a tasked selector within a transaction to be acquired "incidentally," rather than "inadvertently." In the context of minimization, "incidental" and "inadvertent" should not be considered synonymous. Given that the acquisition of the transaction is intentional, and given the Government's knowledge that such transactions may also include information that is not to, from, or about a tasked selector, the acquisition of this additional information is not "inadvertent." By contrast, the additionally acquired information is "incidental" in that it is not the basis for the collection but is rather a necessary yet unavoidable consequence of acquiring foreign communications to, from, or about a tasked selector. *See* [redacted] Mem. Op. at 40 (concluding that the Government's minimization procedures "constitute a safeguard against improper use of information about U.S. persons that is inadvertently *or* incidentally acquired") (emphasis added).[5] Otherwise, subsection 3(b)(1) of NSA's current and proposed minimization procedures would require the destruction of the *entire* transaction -- even the very foreign intelligence information that resulted in the transaction's acquisition in the first place -- if any discrete communication therein contained United States person information and was not to, from, or about a tasked selector. ~~(TS//SI//OC/NF)~~

Such an absurd result simply cannot be squared with Congress's explicit intent that non-pertinent information should be destroyed only if "feasible." *See* H.R. Rep. No. 95-1283, pt. 1, at 56 ("By minimizing retention, the committee intends that information acquired, which is not necessary for obtaining[,] producing, or disseminating foreign intelligence information, be destroyed *where feasible*." (emphasis added)). Congress recognized that in some cases, pertinent and non-pertinent information may be co-mingled in such a way as to make it technologically infeasible to segregate the pertinent information from the non-pertinent information and then

[5] The Government notes that at a single point in its June 1 Submission, it incorrectly described the acquisition of a discrete communication that is not to, from, or about a tasked selector within a transaction to be acquired "inadvertently." *See* June 1 Submission at 13 ("The issue for the Court in light of the above-described nature and scope of NSA's upstream collection is whether, in light of a governmental interest 'of the highest order of magnitude,' NSA's targeting and minimization procedures sufficiently protect the individual privacy interests of United States persons whose communications are inadvertently acquired."). However, the Government otherwise consistently described the acquisition of such communications as "incidental," *see, e.g.*, *id.* at 15 ("NSA's upstream collection may incidentally acquire information concerning United States persons within transactions containing multiple discrete communications, only one of which is to, from, or about a person targeted under Section 702."); *id.* at 19 ("The fact that other, non-pertinent information within the transaction may also be incidentally and unavoidably acquired simply cannot render the acquisition of the transaction unreasonable."); *id.* ("[T]o the extent that United States person information is incidentally acquired in the acquisition of a whole transaction by NSA's upstream collection, such information will be handled in accordance with strict minimization procedures."). ~~(TS//SI//NF)~~

destroy the latter. *See id.* ("The committee recognizes that it may not be feasible to cut and paste files or erase part of tapes where some information is relevant and some is not."). Here, it is not technologically feasible for NSA to extract, post-acquisition, only the discrete communication that is to, from, or about a tasked selector within a transaction. Thus, in order for NSA to retain the foreign intelligence information within a transaction, it must retain the entire transaction, including any incidentally acquired information about U.S. persons or persons in the United States contained therein. ~~(TS//SI//NF)~~

This incidentally acquired information in transactions is subjected to the same restrictions on use and dissemination that govern information obtained through other means pursuant to Section 702 (such as through collection at Internet Service Providers).[6] The Court has previously found these restrictions on use and dissemination in NSA's current minimization procedures to be consistent with the Act and the Fourth Amendment. *See, e.g, In re DNI/AG Certification* [redacted] Mem. Op. at 8-12 (USFISC [redacted] 2010); *In re DNI/AG Certification* [redacted] Mem. Op. at 8-15 (USFISC [redacted] 2009). Of course, the Government seeks the Court's approval of revised NSA Section 702 minimization procedures that would enable NSA analysts to use United States person identifiers as selection terms if those selection terms are reasonably likely to return foreign intelligence information. As discussed in its response to question 14 below, the Government respectfully suggests that these revised NSA minimization procedures are also consistent with the Act and the Fourth Amendment. ~~(TS//SI//OC/NF)~~

In sum, NSA treats each discrete communication contained within a larger Internet transaction as a separate communication for purposes of its minimization procedures. Although it is possible that certain discrete communications containing United States person information will be retained, as described above, they remain subject to the same restrictions on use and dissemination imposed by NSA's minimization procedures. ~~(TS//SI//OC/NF)~~

5.a. Once NSA has identified a portion of a transaction that does not contain targeted information, is it possible to mask or otherwise minimize the non-target information contained within the transaction?

No. The analytic tools used to display the acquired data to NSA analysts do not have a capability to mask information or otherwise minimize the non-target information contained within a transaction. See additional details provided in response to question 6 below. ~~(TS//SI//NF)~~

[6] Moreover, as discussed in response to question 3.b. above, NSA's inability to separate the discrete communications post-acquisition also means that the discrete communications are not displayed in NSA's SC-SSRs as separate communications, but rather clearly retain their connection to the entirety of the original transaction, making it more apparent to NSA analysts the discrete communication's relationship to a tasked selector. ~~(TS//SI//OC/NF)~~

5.b. Why is NSA unable to delete and replace, or alter, an original transaction that contains non-target information? See June 1 Submission at 27-28.

The answer to this question is included in the response to question 6 below. ~~(TS//SI//NF)~~

6. The government states that an Internet transaction that is acquired "is... not divisible into the discrete communications within it even once it resides in an NSA corporate store." June 1 Submission at 22. Please reconcile that statement with the government's acknowledgment that "an analyst would . . . be able to copy a portion of the rendered view of a transaction contained in a NSA corporate store and then paste it into a new record on a different system." Id. at 27 n.25.

As discussed in the example of [redacted] information on pages 27-28 of the June 1 Submission, the data within such transactions is organized in a fashion meant to be displayed using [redacted], which is not necessarily a format in which discrete communications that may be contained within the transaction are distinguishable. In order for NSA to identify and separate a transaction containing multiple communications into those component parts, the transaction would require processing, parsing, and reformatting for those components intended for subsequent retention as separate communications. This is true at the point of acquisition and at any point post-acquisition, including at the point of display to the analyst, whether the intent is to separate out a particular communication from the transaction for the purpose of deleting it, replacing it, masking it, or otherwise altering it. [redacted] ~~(TS//SI//OC/NF)~~

Absent [redacted] capabilities as discussed above, attempts by NSA analysts to delete, replace or otherwise alter (e.g., mask or otherwise minimize the non-target information contained within the transaction) a portion of a transaction intercepted through NSA's upstream collection techniques could similarly corrupt the integrity of the collection, destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including any particular communication therein for analytic or other purposes. Maintaining the integrity of original transactions is paramount to NSA's retention and dissemination processes. Specifically, NSA has developed and implemented a comprehensive purge process designed to improve the completeness of data purges. The efficacy of this process depends in large measure on NSA's ability to trace data back to the original object (such as a transaction) in a SIGINT Collection - Source Systems of Record (SC-SSR). Maintaining the integrity of original transactions is also important for ensuring quality control of NSA's foreign intelligence analysis of Internet communications, which frequently may contain more than one tasked selector or could be used by more than one analyst, depending on the target, mission, or specific foreign intelligence need to which it pertains. Thus, preserving the integrity of the data is dependent upon the retention of the original transaction in its original form as stored in the SC-SSR. ~~(TS//SI//OC/NF)~~

The government's representation that an Internet transaction that is acquired "is... not divisible into the discrete communications within it even once it resides in an NSA corporate store" was intended to convey that it is not technologically feasible for NSA to create [redacted] processes to divide transactions into discrete communications. Footnote 25 on page 27 of the June 1 Submission refers to the fact that it is possible for individual analysts to copy some of the information from a transaction in NSA corporate stores into a new document or file stored on a separate system, such as a [redacted] *See, e.g.*, DNI/AG 702(g) Certification [redacted] Trans. of Proceedings at 20-21 ([redacted] 2010) (for a discussion of [redacted]). The fact that such a copy or extract can be made, however, does not mean that the underlying transaction can then be altered in the corporate store. For example, if an analyst copied a portion of a transaction from an SC-SSR into a [redacted] and then purged the transaction from the SC-SSR, the data copied into the [redacted] would likewise have to be purged -- even if it contained foreign intelligence information copied from a communication to, from, or about a tasked selector -- because it could no longer be traced back to an object present in an SC-SSR. ~~(TS//SI//OC/NF)~~

7. Please reconcile the government's statement that the "communicants" of to/from communications are "the individual users of particular selectors" (see June 1 Submission at 30) with [redacted] elsewhere in its response to the Court's questions (see, e.g., id. at 6 (discussing application of IP filtering)).

The Government believes its statement that [redacted] in the case of to/from communications is fully consistent with the Government's description of how NSA [redacted] to determine if one end of a to/from communication is outside of the United States. As stated on page 30 of the June 1 Submission, the communicants in to/from communications are the individual users who are the senders and intended recipients of those communications, rather than [redacted] ~~(TS//SI//OC/NF)~~

With respect to IP filtering, however, in many instances it is not possible for NSA to [redacted]. *See* June 1 Submission at 6-7. [redacted] *See, e.g., id.* at 11. ~~(TS//SI//OC/NF)~~

As described in the June 1 Submission, there are scenarios under which NSA could unknowingly and unintentionally acquire a to/from communication in which the sender and all intended recipients are in the United States at the time of acquisition -- for example, if that

communication [redacted][7] In the unlikely event that NSA does unintentionally acquire such a communication, NSA will purge the communication unless its continued retention is authorized by the Attorney General in accordance with 50 U.S.C. § 1806(i). If the communication is itself contained within a transaction that contains other discrete communications, the whole transaction will be purged unless its continued retention is authorized by the Attorney General in accordance with 50 U.S.C. § 1806(i), regardless of whether those other discrete communications are foreign. ~~(TS//SI//OC/NF)~~

8. What is the factual basis for NSA's assertions that "a United States person would [redacted] only in a minute percentage of cases" and that [redacted]? See June 1 Submission at 11, 12.

These factual assertions by NSA are based upon the assessments of NSA Signals Intelligence (SIGINT) personnel, who have been involved in NSA's Section 702 acquisitions since the initiation of that collection, and many of whom have experience [redacted] NSA's factual assertions in the June 1 Submission are also based on its review of a sampling of Section 702-acquired communications, which is described on page 9 of the June 1 Submission. As is more fully discussed in that filing, NSA's review of [redacted] records between these two tests revealed only [redacted] records indicative of a non-targeted user [redacted] in the United States. Further research revealed that these [redacted] records were actually copies of the same transaction, and NSA found no indication that any wholly domestic communications were within this transaction. NSA assesses that the results of these tests are consistent with the assessments made by NSA's SIGINT personnel in the June 1 Submission. ~~(TS//SI//OC//NF)~~

9. What is the factual basis for NSA's suggestion that [redacted]? See June 1 Submission at 8 n.9.

[redacted]

[7] As previously described, it would be very unlikely for [redacted] in which the sender and all intended recipients are located inside the United States. See June 1 Submission at 11. Moreover, with the previously described limited exception [redacted] *see id.* at 6 & n.5, NSA analysts have yet to identify a wholly domestic communication acquired through NSA's upstream collection systems. *See id.* at 9 (noting NSA's experience to date and describing NSA's test samples, stating that the only records possibly indicative of a United States-based user [redacted] did not reveal that any wholly domestic communications had been acquired). ~~(TS//SI//OC/NF)~~

[redacted]

10. The government repeatedly characterizes as "unintentional" NSA's collection of discrete non-target communications as part of transactional acquisitions, [redacted] Assuming arguendo that such collection can fairly be characterized as unintentional, please explain how 50 U.S.C. § 1806(i) applies to the discrete, wholly domestic communications that might be contained within a particular transaction.

Subsection 1806(i) provides that "[i]n circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication,[8] under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located in the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicates a threat of death or serious bodily harm to any person." (U)

The Government's June 1 Submission described for the Court that at the time of acquisition, NSA's Section 702 upstream Internet collection devices are generally not capable of distinguishing transactions containing only a single discrete communication to, from, or about a tasked selector from transactions containing multiple discrete communications, not all of which

[8] Subsection 1806(i) originally covered only radio communications, but was amended in 2008 to cover all communications to make it technology neutral. *See* 154 Cong. Rec. S6133 (daily ed. June 25, 2008). (U)

may be to, from, or about a tasked selector at the time of acquisition.[9] *See* June 1 Submission at 7, 27-28. The Government considers the acquisition of communications within a transaction that are not to, from, or about a tasked selector to be incidentally acquired communications. However, the Government does not intend to acquire transactions containing communications that are wholly domestic in nature and in fact has implemented [redacted] means to prevent the acquisition of such transactions. While those [redacted] means could fail (as was the case involving the previously reported [redacted], or be circumvented [redacted] NSA is nevertheless not intending to acquire wholly domestic communications. Thus, in the context of acquiring Internet transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector, the Government recognizes that subsection 1806(i) could potentially be implicated to the extent that one of those discrete communications is a communication in which the sender and all intended recipients were located in the United States at the time of acquisition. Accordingly, in the event NSA recognizes a wholly domestic communication which is not to, from, or about a tasked selector which it has unintentionally acquired in the course of conducting its Section 702 upstream Internet collection, NSA would handle the entire transaction in accordance with subsection 1806(i) and either purge it or, if appropriate, seek authorization from the Attorney General to retain it. ~~(TS//SI//OC/NF)~~

NSA's minimization procedures, adopted by the Attorney General in consultation with the Director of National Intelligence, allow the Director of NSA to execute a waiver permitting the retention of wholly domestic communications. *See* Current and Proposed NSA Minimization Procedures, § 5. However, this provision applies to the acquisition of domestic communications when the Government has a reasonable, but mistaken, belief that the target is a non-United States person located outside the United States because NSA is intentionally but mistakenly acquiring such communications.[10] This domestic communications carve-out does not apply to an unintentionally acquired transaction that contains a wholly domestic communication (when recognized as such by NSA) along with other discrete communications, which is not to, from, or about a tasked selector. As described previously, NSA's Section 702 upstream Internet collection devices are generally incapable of distinguishing transactions containing only a single discrete communication to, from, or about a tasked selector from transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector at the time of acquisition; moreover, NSA cannot separate transactions containing multiple discrete communications into logical constituent parts post-acquisition. Thus, in the event that NSA's Section 702 upstream Internet collection resulted in the unintentional acquisition of a transaction containing a wholly domestic communication, consistent with subsection 1806(i), NSA would purge the entire transaction, unless the Attorney General has authorized its retention after first

[9] NSA additionally advised the Court that except in certain limited circumstances, NSA cannot separate transactions into logical constituent parts post-acquisition either without rendering the transaction unusable for analytic or other purposes. *See* June 1 Submission at 27 & n.27. ~~(TS//SI//OC/NF)~~

[10] *See* Government's Analysis of Section 1806(i), DNI/AG 702(g) Certification [redacted] Docket No. 702(i)-08-01, filed Aug. 28, 2008; [redacted] Mem. Op. at 25-27. ~~(TS//SI//OC/NF)~~

determining that its contents indicated a threat of death or serious bodily harm to any person.[11] ~~(TS//SI//OC/NF)~~

11. Please provide a thorough legal analysis supporting your view that the knowing and intentional acquisition of large volumes of Internet transactions containing discrete communications that are neither to, from, nor about a targeted selector (as well as other information not pertaining to the users of targeted selectors) is merely "incidental" to the authorized purpose of the collection as a whole, and therefore reasonable under the Fourth Amendment.

Fourth Amendment reasonableness is concerned only with the effect on Fourth Amendment protected interests. Thus, in evaluating reasonableness under the Fourth Amendment, the relevant issue for the Court in considering the acquisition of communications incidental to the purpose of this collection is the extent to which such incidental communications involve United States persons or persons located in the United States. *Cf.* [redacted] Mem. Op. at 37-38 (recognizing that non-U.S. persons outside the United States "are not protected by the Fourth Amendment" (citing *United States v. Verdugo-Urqidez*, 494 U.S. 259, 274-75 (1990)). For the reasons more particularly explained in the Government's responses to question 1 above and question 14 below, most of the communications incidentally acquired pursuant to this collection have no effect on any Fourth Amendment protected interests. The Government acknowledges that it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain information pertaining to United States persons or persons located in the United States. That, however, does not mean that the acquisition of multiple discrete communications is any more likely to result in the acquisition of United States person information than in the collection of single, discrete communications to, from, or about a non-United States person located outside the United States. This is particularly true because the technology NSA uses to prevent the acquisition of wholly domestic communications also acts to limit the acquisition of communications among and between United States persons.[12] ~~(TS//SI//OC/NF)~~

---

[11] See also the Government's response to question 7 above, which explains that there are other scenarios under which NSA could unknowingly and unintentionally acquire a wholly domestic communication. In the unlikely event that NSA does unintentionally acquire such a communication, NSA will purge the communication upon recognition unless its continued retention is authorized by the Attorney General in accordance with subsection 1806(i). If the communication is itself contained within a transaction that contains other discrete communications, the whole transaction will be purged unless its continued retention is authorized by the Attorney General in accordance with subsection 1806(i), regardless of whether those other discrete communications are foreign. ~~(TS//SI//OC/NF)~~

[12] For example, the Court has expressed particular concern regarding the acquisition of [redacted] ~~(TS//SI//OC/NF)~~

Moreover, even with respect to those instances in which U.S. person information is acquired, courts in both the FISA and criminal (Title III) contexts have recognized that the acquisition of communications incidental to the purpose of a collection may be necessary to achieve the goal of a search or surveillance, as well as reasonable under the Fourth Amendment. *See, e.g., In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1015 (Foreign Int. Surv. Ct. Rev. 2008) (hereinafter "*In re Directives*") ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.") (citations omitted)); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000), *aff'd sub nom. In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157 (2d Cir. 2008), *cert. denied sub nom. El-Hage v. United States*, 130 S.Ct. 1050 (2010) ("[I]ncidental interception of a person's conversations during an otherwise lawful [Title III] surveillance is not violative of the Fourth Amendment."). ~~(TS//SI//OC/NF)~~

In cases where NSA acquires Internet transactions that include multiple discrete communications, the Government considers any discrete communications not to, from, or about the tasked selector to be incidentally acquired. Specifically, the Government's purpose in acquiring such a transaction is to acquire the foreign intelligence information likely contained within the discrete communication to, from, or about a tasked selector. However, because it is technologically infeasible for NSA's upstream collection systems to extract only the discrete communication that is to, from, or about a tasked selector, the only way to obtain the foreign intelligence information in that discrete communication is to acquire the entire transaction. Thus, the acquisition of the other discrete communications within the transaction is properly considered "incidental," because it is a necessary but unavoidable consequence of achieving the Government's goal of acquiring the foreign intelligence information contained within the discrete communication to, from, or about a tasked selector. *See* H.R. Rep. No. 95-1283, pt. 1, at 55 (1978) (noting that "in many cases it may not be possible for technical reasons to avoid acquiring all information" when conducting foreign intelligence surveillance); *see also id.* at 56 ("[I]t may not be possible or reasonable to avoid acquiring all conversations."); *cf. United States v. McKinnon*, 721 F.2d 19, 23 (1st Cir. 1983) ("Evidence of crimes other than those authorized in a [Title III] wiretap warrant are intercepted 'incidentally' when they are the by-product of a bona fide investigation of crimes specified in a valid warrant."). ~~(TS//SI//OC/NF)~~

That is not to say, however, that the acquisition of non-pertinent information is reasonable in all cases simply because the collection of that information is "incidental" to the purpose of the search. *United States v. Ulrich*, 228 Fed. Appx. 248, 252 (4th Cir. 2002) (noting that "fishing expeditions" or "a random exploratory search or intrusion" violate the Fourth Amendment) (quotation marks omitted). Here, NSA's acquisition of transactions is conducted in accordance with FISC-approved targeting procedures reasonably designed to ensure that the acquisitions are directed "toward communications that are likely to yield the foreign intelligence information sought, and thereby afford a degree of particularity that is reasonable under the Fourth Amendment." [redacted] Mem. Op. at 39-40 (footnote omitted). The fact that such transactions may contain non-pertinent information -- even in significant amounts -- does not by itself render the acquisition of those transactions unreasonable under the Fourth Amendment. *See Scott v. United States*, 436 U.S. 128, 140 (1978) (recognizing that "there are surely cases,

such as the one at bar [involving a Title III wiretap], where the percentage of nonpertinent calls is relatively high and yet their interception was still reasonable"); *Abraham v. County of Greenville*, 237 F.3d 386, 391 (4th Cir. 2001) ("[I]ncidental overhearing is endemic to surveillance."); *United States v. Doolittle*, 507 F.2d 1368, 1372 (5th Cir. 1975) ("There is no question that some irrelevant and personal portions of gambling conversations were intercepted or that certain nonpertinent conversations were intercepted. But this is inherent in the type of interception authorized by Title III, and we do not view the simple inclusion of such conversations, without more, as vitiating an otherwise valid wiretap.")[13]; s*ee also, e.g., Board of Educ. v. Earls*, 536 U.S. 822, 837 (2002) ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotations marks omitted)). ~~(TS//SI//OC/NF)~~

As such, the incidental collection at issue here is reasonable under the Fourth Amendment because it is a necessary and unavoidable by-product of NSA's effort to obtain the foreign intelligence information contained within a discrete communication that is a part of a larger transaction which could contain non-pertinent communications. *See United States v. Wuagneux*, 683 F.2d 1343, 1352-53 (11th Cir. 1982) (observing that "a search may be as extensive as reasonably required to locate the items described in the warrant," and on that basis concluding that it was "reasonable for the agents [executing the search] to remove intact files, books, and folders when a particular document within the file was identified as falling within the scope of the warrant"); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence sought may be seized"). Moreover, as described in the response below, NSA takes the steps it can to ensure that it conducts its Section 702 upstream collection in a manner that minimizes the intrusion into the personal privacy of United States persons. ~~(TS//SI//OC/NF)~~

12. The statute requires the targeting procedures to "be reasonably designed to ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States and [to] prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). How can procedures that contemplate the knowing acquisition of huge volumes of transactions that will include quantifiable amounts of information relating to non-targets, including information of or about U.S. persons abroad or persons located in the United States, meet this statutory requirement?

[13] These cases upholding the Fourth Amendment reasonableness of Title III surveillances that resulted in the acquisition of significant amounts of nonpertinent communications are particularly noteworthy given that Title Iain's requirement to minimize the acquisition of such communications is considerably stricter than FISA's. *See* H.R. Rep. 95-1283, pt. 1, at 56 ("It is recognized that given the nature of intelligence gathering, minimizing acquisition should not be strict as under [Title III] with respect to law enforcement surveillances."). ~~(TS//SI//NF)~~

For the reasons more particularly discussed in its response to question 1.b.ii. in the June 1 Submission, which took into account the means by which communications to, from, or about a tasked selector are acquired through NSA's upstream Internet collection techniques, the Government respectfully submits that NSA's targeting procedures are reasonably designed to ensure that an authorized acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located within the United States. *See* June 1 Submission at 3-12, 20-24. As discussed in the Government's June 1 Submission, for acquisition of both to/from communications and abouts communications, the person being "targeted" is the user of the tasked selector, who, by operation of the targeting procedures, is a non-United States person reasonably believed to be located outside the United States. *See* June 1 Submission at 3-4. This remains true for all Section 702 upstream acquisitions, including the acquisition of transactions containing several discrete communications, only one of which may be to, from, or about the user of a tasked selector. ~~(TS//SI//NF)~~

Specifically, the sole reason a transaction is selected for acquisition is that it contains the presence of a tasked selector used by a person who has been targeted in accordance with NSA's targeting procedures.[14] Indeed, at the time a transaction is acquired, NSA cannot always know whether the transaction includes other data or information representing communications that are not to, from, or about the target, let alone always have knowledge of the parties to those communications. *Cf.* [redacted] Mem. Op. at 18-19 (noting that with respect to abouts communications, "the government may have no knowledge of [the parties to a communication] prior to acquisition"). It therefore cannot be said that the acquisition of a transaction containing multiple discrete communications results in the intentional targeting of any of the parties to those communications other than the user of the tasked selector. *Cf. Bin Laden*, 126 F. Supp. 2d at 281 (acknowledging that in light of *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990), and Title III "incidental interception" case law, overseas surveillance of a United States person terrorism suspect would have posed no Fourth Amendment problem "if the Government had not been aware of [his] identity or of his complicity in the [terrorism] enterprise"). The fact that a transaction acquired pursuant to the targeting procedures may also contain communications to, from, or about persons other than the user of the tasked selector does not mean those persons are likewise being targeted by that acquisition. *Cf.* H.R. Rep. No. 95-1283, pt. 1, at 50 (explaining, with regard to electronic surveillance as defined by 50 U.S.C. § 1801(f)(1), that "[t]he term 'intentionally targeting' includes the deliberate use of surveillance techniques which can monitor numerous channels of communication among numerous parties, where the techniques are designed to select out from among those communications the communications to which a particular U.S. person located in the United States is a party, and where the communications are

14 [redacted] ~~(TS//SI//NF)~~

selected either by name or by other information which would identify the particular person and would select out his communications"). Rather, as discussed in the response to question 11 above, the acquisition of such non-pertinent communications is incidental to the purpose of the collection as a whole and therefore reasonable under the Fourth Amendment. ~~(TS//SI//NF)~~

Similarly, to the extent that one of the discrete non-pertinent communications within an acquired transaction is a communication in which the sender and all intended recipients were located in the United States at the time of acquisition, the acquisition of this wholly domestic communication would be incidental and, as discussed in response to question 10 above, unintentional. NSA's targeting procedures require that, in conducting upstream collection of abouts communications, NSA either employ "an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas" or '[redacted]' *E.g.*, Amendment 1 to DNI/AG 702(g) Certification [redacted] Ex. A, filed [redacted] 2010, at 1-2; *see also* [redacted] Mem. Op. at 19. The Court has previously found that these [redacted] means were "reasonably designed to prevent the intentional acquisition of communications as to which all parties are in the United States," while recognizing that it is "theoretically possible that a wholly domestic communication could be acquired as a result of the [redacted] Mem. Op. at 20 & n.17. As discussed in the June 1 Submission, apart from one exception involving [redacted] NSA analysts have yet to identify a wholly domestic communication acquired through NSA's upstream collection systems. *See* June 1 Submission at 8-9. Accordingly, the Government continues to believe that NSA's [redacted] means for preventing the acquisition of wholly domestic communications remain efficacious, and that the theoretical scenarios in which NSA would acquire a wholly domestic communication do not prevent the Court from continuing to find that NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be in the United States. ~~(TS//SI//OC/NF)~~

To the extent that NSA does unintentionally acquire and then recognize such a wholly domestic communication within an acquired transaction, as described in response to question 10 above, NSA would be required to purge the entire transaction, unless the Attorney General determined "that the contents indicate[d] a threat of death or serious bodily harm to any person." ~~(TS//SI//OC/NF)~~

13. In its discussion of the Fourth Amendment, the government asserts that "upstream collection" in general is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs." June 1 Submission at 16.

a. To what extent can the same be said for the acquisition of Internet transactions [redacted] in particular?

b. Is the acquisition of Internet transactions via upstream collection the only source for certain categories of foreign intelligence information? If so, what categories?

c. Please describe with particularity what information NSA would acquire, and what information NSA would not acquire, if NSA were, in comparison to its current collection, to limit its acquisition of Internet communications to: (1) acquisitions conducted with the assistance of [redacted]; and (2) the upstream collection of discrete communications to, from, or about tasked selectors that are [redacted] (id. at 2, n.2).

The Government's assertion that upstream collection is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs" is equally applicable to its acquisition of Internet transactions. This is true because the Government's acquisition of Internet transactions is not a subset of its upstream collection of Internet communications. Instead, acquisition of Internet transactions is the technical means by which all upstream collection of Internet communications accounts are acquired. ~~(TS//SI//NF)~~

Section 702 upstream collection of Internet communications provides NSA with certain types of information (further described below) which are extremely valuable to its national security mission. Disseminated end product reports derived from this collection have proven to be of critical value to high-level customers, including the White House, State Department, Joint Chiefs of Staff, the National Counterproliferation Center, Central Intelligence Agency (CIA), Defense Intelligence Agency, Federal Bureau of Investigation (FBI), and others. In addition,

[redacted] ~~(TS//SI//NF)~~

[redacted] ~~(TS//SI//NF)~~

Section 702 upstream collection offers unique opportunities to detect target information, including but not limited to the following examples:

[redacted]

[redacted] ~~(TS//SI//NF)~~

[redacted] As such, and as the Court has recognized, NSA's upstream collection is "*uniquely capable* of acquiring certain types of targeted communications containing valuable foreign intelligence information." *In re DNI/AG Certification* [redacted] Mem. Op. at 25-26 (USFISC [redacted] 2009) (emphasis added; internal citations omitted). ~~(TS//SI//NF)~~

Additionally, NSA's Section 702 upstream collection would not acquire many of the above categories of communications, and thus the foreign intelligence contained within these communications, if NSA's upstream collection were limited to acquisition solely of discrete communications to, from, or about tasked selectors that are [redacted] referenced in footnote 2 on page 2 of the June 1 Submission. Currently, [redacted] ~~(TS//SI//NF)~~

15 [redacted]
(TS//SI//NF)

[redacted]

~~(TS//SI//NF)~~

[redacted] ~~(TS//SI//NF)~~

The Court's question asks for "categories of foreign intelligence information" that can be obtained exclusively through NSA's acquisition of Internet transactions via upstream collection. This is a difficult question to answer, as types of foreign intelligence may be conveyed through a variety of communication means. For example, [redacted] as described above, it is entirely possible that this communication may only be acquired through NSA's Section 702 upstream collection of communications other than those [redacted] ~~(TS//SI//NF)~~

In an effort to fully answer the Court's question, however, the Government respectfully submits the following examples of instances where NSA has obtained substantial foreign intelligence information from Section 702 upstream collection. The examples detail only a few

[redacted]

~~(TS//SI//NF)~~

of the many instances in which Section 702 upstream collection has provided such substantial foreign intelligence. In many of these examples, Section 702 upstream collection provided important leads that led to [redacted]. Although all forms of Section 702 upstream collection have proved to be of critical importance to the NSA's national security mission, the examples below involve the acquisition by Section 702 upstream collection of communications other than [redacted]
~~(TS//SI//NF)~~

[redacted] ~~(S)~~

[redacted]

~~(TS//SI//NF)~~

[redacted] (S)

[redacted]

[redacted]

[redacted] ~~(TS//SI//NF)~~

[redacted] ~~(U//FOUO)~~

[redacted]

14. The Fourth Amendment also requires the Court to examine the nature and scope of the intrusion upon protected privacy interests. How can the Court conduct such an assessment if the government itself is unable to describe the nature and scope of the information that is acquired or the degree to which the collection includes information pertaining to U.S. persons or persons located in the United States?

Although, as discussed above, it is difficult for the Government to fully describe to the Court every possible type of information that may be contained within a transaction acquired through NSA's upstream collection, the Government respectfully suggests that the Court can nonetheless assess whether NSA's upstream collection of such transactions is reasonable under the Fourth Amendment. ~~(TS//SI//OC/NF)~~

First, the Supreme Court has recognized that an appreciation of all of the possible ways a search can intrude upon interests protected by the Fourth Amendment is not an indispensable component of assessing the reasonableness of the search. *See Dalia v. United States*, 441 U.S. 238, 257 (1979) ("Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant."); *cf. Payton v. New York*, 445 U.S. 573, 601-02 (1980) (recognizing that "for Fourth Amendment purposes, an arrest warrant founded on probable cause implicitly carries with it the limited authority to enter a dwelling in which the suspect lives when there is reason to believe the suspect is within," even though "an arrest warrant requirement may afford less [privacy] protection than a search warrant requirement"). Thus, the Government respectfully suggests that the Court can assess the Fourth Amendment reasonableness of NSA's upstream collection even if the Government cannot fully describe every possible type of information that collection may acquire. ~~(TS//SI//OC/NF)~~

Moreover, while it may be difficult for the Government to describe the full scope of the types of information that may be acquired by NSA's upstream collection, it is nevertheless possible to ascertain the degree to which that information would pertain to United States persons or persons located in the United States. For the reasons discussed below, the Government does not believe that information about United States persons or persons located in the United States would be acquired through NSA's upstream collection of transactions to a greater degree, in relative terms, than other types of communications acquired under Section 702. ~~(TS//SI//OC/NF)~~

First, certain transactions are acquired because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's FISC-approved targeting procedures, is a non-United States person reasonably believed to be located outside the United States. This Court has recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!* Mem. Op. at 87 (footnote omitted). Accordingly, it is reasonable to presume that most of the discrete communications that may be within the acquired transaction are between non-United States persons located outside the United States. Second, with respect to transactions that contain a discrete communication about a tasked selector, the technical means by which NSA prevents the intentional acquisition of wholly domestic communications is to ensure that the acquisition of transactions is directed at persons reasonably believed to be located outside the United States. Again, these individuals reasonably can be presumed to be non-United States persons, and most of their communications can be presumed to be with other non-United States persons located outside the United States. *Id.* This combination of targeting non-United States persons located outside the United States and directing acquisitions at persons located outside the United States operates to significantly diminish the likelihood that information pertaining to United States persons or persons in the United States will be acquired. ~~(TS//SI//OC/NF)~~

To be sure, it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain information pertaining to United States persons or persons in the United States. That, however, does not by itself mean that the volume of such information in transactions will be greater than in the collection of other types of communications that have previously been discussed and approved. [redacted] ~~(TS//SI//OC/NF)~~

Moreover, the fact that within an acquired transaction there may be multiple discrete communications containing information pertaining to United States persons or persons in the United States cannot by itself render the acquisition of that transaction unreasonable under the Fourth Amendment. As discussed above, the acquisition of such information is incidental to the purpose of the transaction's acquisition -- the acquisition of the discrete communication(s) to,

from, or about a tasked selector within the transaction. *See In re Directives*, 551 F.3d at 1015 ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.") (citations omitted)). ~~(TS//SI//OC/NF)~~

In any event, any information pertaining to a United States person or person located in the United States present in a transaction containing multiple discrete communications would be handled under the NSA minimization procedures in the exact same manner as if that information appeared in a discrete communication to, from, or about a tasked selector. For example, the use and dissemination of United States person information acquired from a [redacted] would be subject to the same restrictions as United States person information acquired from [redacted] ~~(TS//SI//OC/NF)~~

15. In light of the government's emphasis on the limited querying of Section 702 acquisitions that is currently permitted (see June 1 Submission at 23), why is it reasonable and appropriate to broaden the targeting procedures to permit querying using U.S.-person identifiers?

Although NSA's current minimization procedures prohibit the use of United States person names or identifiers to retrieve any Section 702-acquired communications in NSA systems, *see* Current NSA Minimization Procedures, § 3(b)(5), the statute requires no such limitation. Rather, it is reasonable and appropriate for the Court to approve the Government's proposal to enable NSA analysts to use United States person identifiers as selection terms because the request is consistent with the statutorily required minimization procedures. *See* Proposed NSA Minimization Procedures § 3(b)(5) (providing, in pertinent part, that "[c]omputer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, *will be limited to those selection terms reasonably likely to return foreign intelligence information*. Any United States person identifiers used as terms to identify and select communications must be approved in accordance with NSA procedures.") (emphasis added). ~~(TS//SI//OC/NF)~~

Minimization procedures must be designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly availably information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. 50 U.S.C. § 1801(h)(1). Where, as here, "it may not be possible for technical reasons to avoid acquiring all information," Congress has recognized that minimization procedures "must emphasize the minimization of retention and dissemination." H.R. Rep. No. 95-1283, pt. 1, at 55. Congress also acknowledged that "a significant degree of latitude be given in counterintelligence and counterterrorism cases" with respect to retention and dissemination of information. *Id.* at 59. In light of such latitude, "rigorous and strict controls" should -- and will -- be placed on the retrieval of United States person information and "its dissemination or use for purposes other than counterintelligence or counterterrorism." *Id.* ~~(TS//SI//OC/NF)~~

With respect to acquisition, the Government's proposal to use United States person identifiers as selection terms does not broaden the scope of what the Government can acquire under the certifications. Because, for the reasons detailed above, it is not possible "to avoid acquiring" the incidentally obtained information, the focus will be on the retention and dissemination provisions of the procedures. *Id.* at 55. As a general matter, NSA's minimization procedures contain detailed provisions regarding the retention and dissemination of United States person information that the Court has previously approved. *See, e.g.* [redacted] Mem. Op. at 21-32, 40-41. In addition, the Government's proposal provides that United States person identifiers may only be used "in accordance with NSA procedures" governing the circumstances under which U.S. person information can be queried. Although the Government is still developing such procedures, and NSA analysts will not begin using United States identifiers as selection terms until they are completed, the Government will ensure that the procedures contain "rigorous and strict controls" for the retrieval and dissemination of United States person information to ensure that only selection terms likely to produce foreign intelligence information are retrieved, and dissemination is limited to counterintelligence and counterterrorism purposes. Moreover, the Government's proposed changes to NSA's minimization procedures require that NSA maintain records of all United States person identifiers approved for use as selection terms and that NSD and ODNI conduct oversight of NSA's activities. *See* Proposed NSA Minimization Procedures § 3(b)(5). ~~(TS//SI//OC/NF)~~

16. The government acknowledges that it previously "did not fully explain all of the means by which . . . communications are acquired through NSA's upstream collection techniques" (June 1 Submission at 2), yet states that the "[Attorney General] and [Director of National Intelligence] have confirmed that their prior authorizations remain valid" (id. at 35). At the time of each previous Certification under Section 702, were the Attorney General and the Director of National Intelligence aware that the acquisitions being approved included Internet "transactions" [redacted]? If so, why was the Court not informed? If not, why are the prior Certifications and collections still valid?

The Government acknowledges that its prior representations to the Court -- and to the Attorney General and Director of National Intelligence -- regarding the steps NSA must take in order to acquire single, discrete communications to, from, or about a tasked selector did not fully explain all of the means by which such communications are acquired through NSA's upstream Internet collection techniques. *See* June 1 Submission at 2. That said, for the reasons described in the answer to question 5 in the June 1 Submission, both the prior Certifications and collection remain valid. *See* June 1 Submission at 31-38. ~~(TS//SI//OC/NF)~~

The Certifications executed by the AG and DNI and submitted to the Court for approval were based on an understanding that Section 702 collection would, at a minimum, acquire discrete communications that are to, from, or about a tasked selector. As described in detail previously, due to certain technological limitations, in general the only way that NSA can acquire certain Internet communications upstream that are to, from, or about a tasked selector is by acquiring an Internet transaction which may include a single, discrete communication to, from, or about a tasked selector (e.g., an e-mail message) or may include several discrete

communications, only one of which may be to, from, or about a tasked selector.[17] *See* June 1 Submission at 27-28. In this respect, the acquisition is comparable to the Government's seizure of a video, book, or intact file that contains a single photo, page, or document that a search warrant authorizes the Government to seize. *See, e.g., United States v. Rogers*, 521 F.3d 5, 10 (1st Cir. 2008) (concluding that a videotape is a "plausible repository of a photo" and that therefore a warrant authorizing seizure of "photos" allowed the seizure and review of two videotapes, even though warrant did not include videotapes); *Wuagneux*, 683 F.2d at 1353 (holding that it was "reasonable for the agents to remove intact files, books and folders when a particular document within the file was identified as falling within the scope of the warrant."); *United States v. Christine*, 687 F. 2d 749, 760 (3d Cir. 1982) (*en banc*) (emphasizing that "no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision. Nor does the Fourth Amendment prohibit seizure of an item, such as a single ledger, merely because it happens to contain other information not covered by the scope of the warrant."); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence may be seized"). None of these cases even hint that the warrant is somehow invalid because the magistrate did not know in advance that the search or seizure of authorized documents or photos would also encompass the search or seizure of additional, intermingled documents or photos, even in cases where such documents could have been physically separated from the larger files or books in which they were contained. Rather, it is well-established that warrants need not state with specificity the precise manner of execution, and, so long as it is reasonable, a search or seizure will be upheld even if conducted in a manner that invades privacy in a manner not considered at the time the warrant was issued. *See United States v. Grubbs*, 547 U.S. 90, 98 (2006) ("Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed.") (citation omitted); *Dalia,* 441 U.S. at 259 ("Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant."). ~~(TS//SI//OC/NF)~~

Moreover, having considered the additional information that is being presented to this Court, the AG and DNI have confirmed that the collection fully complies with the statutory requirements of Section 702, as well as the Fourth Amendment, and that therefore the prior Certifications and collection remain valid. *See* June 1 Submission at 35. ~~(TS//SI//OC/NF)~~

As discussed previously, transactions are only acquired if they contain at least one discrete communication to, from, or about a tasked selector. Each tasked selector has undergone review, prior to tasking, to ensure that the user is a non-United States person reasonably believed to be outside the United States. Moreover, with respect to "abouts communications," the targeting procedures are also reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known to be located in the

[17] [redacted] ~~(TS//SI//OC/NF)~~

United States at the time of acquisition. *See id.* at 3-12, 28-30. Just as the Government's acquisition of an entire book based on the fact that a single page falls within the scope of the warrant does not call into question the warrant's specificity, the incidental acquisition of additional communications that are not to, from, or about the tasked selector does not negate the validity of the targeting procedures that are relied on to acquire a particular transaction. ~~(TS//SI//OC/NF)~~

Moreover, the AG and DNI have confirmed that the additional information regarding incidentally acquired communications does not alter the validity of their prior Certifications. *See id.* at 35. As discussed in detail previously, the minimization and targeting procedures fully comport with all of the statutory requirements, including the requirement that the targeting procedures are reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located within the United States, *see id.* at 3-12, 20-24; and the procedures and guidelines are consistent with the requirements of the Fourth Amendment, *see id.* at 13-24. ~~(TS//SI//OC/NF)~~

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix S

EXHIBIT B

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

(U) Section 1 - Applicability and Scope

(U) These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of information, including non-publicly available information concerning unconsenting United States persons, that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act").

(U) If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity.

~~(S//NF)~~ Nothing in these procedures shall restrict NSA's performance of lawful oversight functions of its personnel or systems, or lawful oversight functions of the Department of Justice's National Security Division, Office of the Director of National Intelligence, or the applicable Offices of the Inspectors General. Additionally, nothing in these procedures shall restrict NSA's ability to conduct vulnerability or network assessments using information acquired pursuant to section 702 of the Act in order to ensure that NSA systems are not or have not been compromised. Notwithstanding any other section in these procedures, information used by NSA to conduct vulnerability or network assessments may be retained for one year solely for that limited purpose. Any information retained for this purpose may be disseminated only in accordance with the applicable provisions of these procedures.

(U) For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA).

(U) Section 2 - Definitions

(U) In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

(a) (U) Acquisition means the collection by NSA or the Federal Bureau of Investigation (FBI) through electronic means of a non-public communication to which it is not an intended party.

(b) (U) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person.

(c) (U) Communications of a United States person include all communications to which a United States person is a party.

(d) (U) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement.

(e) (U) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications.

(f) (U) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person.

(g) ~~(TS//SI//NF)~~ Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication [redacted] or multiple discrete communications [redacted]

(h) (U) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection.

(i) (U) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation.

(j) (U) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes.

(k) (U) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person:

(1) (U) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person.

(2) (U) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

(3) (U) A person who at any time has been known to have been an alien admitted for lawful permanent residence is treated as a United States person. Any determination that a person who at one time was a United States person (including an alien admitted for lawful permanent residence) is no longer a United States person must be made in consultation with the NSA Office of General Counsel.

(4) (U) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence.

(U) Section 3 - Acquisition and Handling - General

(a) (U) Acquisition

(U) The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition.

(b) (U) Monitoring, Recording, and Handling

(1) (U) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be

disseminated under these procedures. Except as provided for in subsection 3(c) below, such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event.

(2) (U) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 3, 4, 5, 6, and 8 of these procedures.

(3) (U//~~FOUO~~) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime for purposes of assessing how the communication should be handled in accordance with these procedures.

(4) (U) Handling of Internet Transactions Acquired Through NSA Upstream Collection Techniques

a. (~~TS//SI//NF~~) NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown.

1. (~~TS//SI//NF~~) Notwithstanding subsection 3(b)(4)a. above, NSA may process Internet transactions acquired through NSA upstream collection techniques in order to render such transactions intelligible to analysts.

2. (~~TS//SI//NF~~) Internet transactions that are identified and segregated pursuant to subsection 3(b)(4)a. will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States.

(a) (~~TS//SI//NF~~) Any information contained in a segregated Internet transaction (including metadata) may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. Any Internet transaction that is identified and segregated pursuant to subsection

3(b)(4)a. and is subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States will be handled in accordance with Section 5 below.

(b) (U//~~FOUO~~) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be handled in accordance with subsection 3(b)(4)b. below and the other applicable provisions of these procedures.

(c) (U//~~FOUO~~) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be marked, tagged, or otherwise identified as having been previously segregated pursuant to subsection 3(b)(4)a.

3. ~~(TS//SI//NF)~~ Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a. will be handled in accordance with subsection 3(b)(4)b. below and the other applicable provisions of these procedures.

b. (U) NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

1. ~~(TS//SI//NF)~~ If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will first perform checks to determine the locations of the sender and intended recipients of that discrete communication to the extent reasonably necessary to determine whether the sender and all intended recipients of that communication are located in the United States. If an analyst determines that the sender and all intended recipients of a discrete communication within an Internet transaction are located in the United States, the Internet transaction will be handled in accordance with Section 5 below.

2. (U) If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will assess whether the discrete communication is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

(a) (U) If the discrete communication is to, from, or about a tasked selector, any U.S. person information in that communication will be handled in accordance with the applicable provisions of these procedures.

(b) (U) If the discrete communication is not to, from, or about a tasked selector but otherwise contains foreign intelligence information, and the discrete communication is not to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, that communication (including any U.S. person information therein) will be handled in accordance with the applicable provisions of these procedures.

(c) (U) If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable U.S. person, or a person reasonably believed to be located in the United States, the NSA analyst will document that determination in the relevant analytic repository or tool if technically possible or reasonably feasible. Such discrete communication cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such use.

3. ~~(TS//SI//NF)~~ An NSA analyst seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications in a FISA application, intelligence report, or section 702 targeting must appropriately document the verifications required by subsections 3(b)(4)b.1. and 2. above.

4. ~~(TS//SI//NF)~~ Notwithstanding subsection 3(b)(4)b. above, NSA may use metadata extracted from Internet transactions acquired on or after October 31, 2011, that are not identified and segregated pursuant to subsection 3(b)(4)a. without first assessing whether the metadata was extracted from: a) a discrete communication as to which the sender and all intended recipients are located in the United States; or b) a discrete communication to, from, or about a tasked selector. Any metadata extracted from Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a. above will be handled in accordance with the applicable provisions of these procedures. Any metadata extracted from an Internet transaction subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located inside the United States shall be destroyed upon recognition.

(5) (U) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream

collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph.

(6) (U) Further handling, retention, and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further handling, storage, and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below.

(c) (U) Destruction of Raw Data

(1) ~~(S//SI~~ [redacted] Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers that do not meet the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers may not be retained longer than five years from the expiration date of the certification authorizing the collection unless NSA specifically determines that each such communication meets the retention standards in these procedures.

(2) ~~(TS//SI//NF)~~ Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. An Internet transaction may not be retained longer than two years from the expiration date of the certification authorizing the collection unless NSA specifically determines that at least one discrete communication within the Internet transaction meets the retention standards in these procedures and that each discrete communication within the transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications. Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and handled only in accordance with the standards set forth above in subsection 3(b)(4) of these procedures.

(3) ~~(TS//SI//NF)~~ Any Internet transactions acquired through NSA's upstream collection techniques prior to October 31, 2011, will be destroyed upon recognition.

(4) ~~(S//NF)~~ NSA may temporarily retain specific section 702-acquired information that would otherwise have to be destroyed, pursuant to section 3(a)-(c) above, if the Department of Justice advises NSA in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. The specific information to be retained (including, but not limited to, the target(s) or selector(s) whose unminimized information must be preserved and the relevant time period at issue in the litigation), and the particular litigation for which the information will be retained, shall be identified in writing by the Department of Justice. Personnel not working on the particular litigation matter shall not access the unminimized section 702-acquired information preserved pursuant to a written preservation notice from the Department of Justice that would otherwise have been destroyed pursuant to these procedures. Other personnel shall only access the information being retained for litigation-related reasons on a case-by-case basis after consultation with the Department of Justice. The Department of Justice shall notify NSA in writing once the section 702-acquired information is no longer required to be preserved for such litigation matters, and then NSA shall promptly destroy the section 702-acquired information as otherwise required by these procedures. Circumstances could arise requiring that section 702-acquired information subject to other destruction/age off requirements in these procedures (e.g., Section 5) be retained because it is subject to a preservation requirement. In such cases the Government will notify the Foreign Intelligence Surveillance Court and seek permission to retain the material as appropriate consistent with law. Depending on the nature, scope and complexity of a particular preservation obligation, in certain circumstances it may be technically infeasible to retain certain section 702-acquired information. Should such circumstances arise, they will be brought to the attention of the court with jurisdiction over the underlying litigation matter for resolution.

(d) (U) Change in Target's Location or Status

(1) (U//~~FOUO~~) In the event that NSA reasonably believes that a target is located outside the United States and subsequently learns that the person is inside the United States, or if NSA concludes that a target who at the time of targeting was believed to be a non-United States person is in fact a United States person at the time of acquisition, the acquisition from that person will be terminated without delay.

(2) (U) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person at the time such communications were acquired, will be treated as domestic communications under these procedures.

(e) ~~(S//NF)~~ In the event that NSA seeks to use any information acquired pursuant to section 702 during a time period when there is uncertainty about the location of the target of the acquisition because the [redacted] post-tasking checks described in NSA's section 702

targeting procedures were not functioning properly, NSA will follow its internal procedures for determining whether such information may be used (including, but not limited to, in FISA applications, section 702 targeting, and disseminations). Except as necessary to assess location under this provision, NSA may not use or disclose any information acquired pursuant to section 702 during such time period unless NSA determines, based on the totality of the circumstances, that the target is reasonably believed to have been located outside the United States at the time the information was acquired. If NSA determines that the target is reasonably believed to have been located inside the United States at the time the information was acquired, such information will not be used and will be promptly destroyed.

(U) Section 4 - Acquisition and Handling - Attorney-Client Communications

(U) As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed dissemination of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination.

(U) Section 5 - Domestic Communications

~~(TS//SI//NF)~~ A communication identified as a domestic communication (and, if applicable, the Internet transaction in which it is contained) will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing and on a communication-by-communication basis, that the sender or intended recipient of the domestic communication had been properly targeted under section 702 of the Act, and the domestic communication satisfies one or more of the following conditions:

(1) ~~(TS//SI//NF)~~ such domestic communication is reasonably believed to contain significant foreign intelligence information. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained, handled, and disseminated in accordance with these procedures;

(2) ~~(TS//SI//NF)~~ such domestic communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such domestic communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures

set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communication is required for law enforcement purposes;

(3) ~~(TS//SI//NF)~~ such domestic communication is reasonably believed to contain technical data base information, as defined in Section 2(j), or information necessary to understand or assess a communications security vulnerability. Such domestic communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that is, or is reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. (U//~~FOUO~~) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. ~~(S//SI~~ [redacted] In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signal Intelligence Director, NSA, determines in writing that retention of a specific communication for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or

(4) (U//~~FOUO~~) such domestic communication contains information pertaining to an imminent threat of serious harm to life or property. Such information may be retained and disseminated to the extent reasonably necessary to counter such threat.

~~(S//NF)~~ Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may promptly notify the FBI of that fact, as well as any information concerning the target's location that is contained in the communication. NSA may also use information derived from domestic communications for collection avoidance purposes, and may provide such information to the FBI and CIA for collection avoidance purposes. NSA may retain the communication from which such information is

derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL).

(U) Section 6 - Foreign Communications of or Concerning United States Persons

(a) (U) Retention

(U) Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

(1) (U) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. (U) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. ~~(TS//SI//NF)~~ In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signals Intelligence Director, NSA, determines in writing that retention of a specific category of communications for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) (U) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) (U) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities.

~~(TS//SI//NF)~~ Foreign communications of or concerning United States persons that may be retained under subsections 6(a)(2) and (3) above include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(b) (U) Dissemination

(U) A dissemination based on communications of or concerning a United States person may be made in accordance with Section 7 or 8 below if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) (U) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) (U) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) (U) the communication or information indicates that the United States person may be:

a. an agent of a foreign power;

b. a foreign power as defined in section 101(a) of the Act;

c. residing outside the United States and holding an official position in the government or military forces of a foreign power;

d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;

(4) (U) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) (U) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications or network security vulnerability, but only after the agency that originated the information certifies that it is properly classified;

(6) (U) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) (U//~~FOUO~~) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or

(8) (U) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document.

(c) (U) Provision of Unminimized Communications to CIA and FBI

(1) (U) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will handle any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(2) (U) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will handle any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(U) Section 7 - Other Foreign Communications

(U) Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.

(~~TS//SI//NF~~) Foreign communications of or concerning a non-United States person that may be retained under this subsection include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(U//~~FOUO~~) Additionally, foreign communications of or concerning a non-United States person may be retained for the same purposes and in the same manner as detailed in Section 6(a)(1), above.

(U) Section 8 - Collaboration with Foreign Governments

(a) (U) Procedures for the dissemination of evaluated and minimized information. Pursuant to section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided below in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with sections 6(b) and 7 of these NSA minimization procedures.

(b) (U) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated:

(1) (U) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA.

(2) (U) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data.

(3) (U) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA.

(4) (U) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA.

(5) (U) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures.

7/24/14
Date

Eric H. Holder, Jr.
Attorney General of the United States

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix T

EXHIBIT A

PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

~~(S)~~ These procedures address: (I) the manner in which the National Security Agency/Central Security Service (NSA) will determine that a person targeted under section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act"), is a non-United States person reasonably believed to be located outside the United States ("foreignness determination"); (II) the post-targeting analysis done by NSA to ensure that the targeting of such person does not intentionally target a person known at the time of acquisition to be located in the United States and does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States; (III) the documentation of NSA's foreignness determination; (IV) compliance and oversight; and (V) departures from these procedures.

I. (S) DETERMINATION OF WHETHER THE ACQUISITION TARGETS NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES

~~(S)~~ NSA determines whether a person is a non-United States person reasonably believed to be outside the United States in light of the totality of the circumstances based on the information available with respect to that person, including [redacted]

~~(S)~~ NSA analysts examine the following three categories of information, as appropriate under the circumstances, to make the above determination: (1) they examine the lead information they have received regarding the potential target or the facility that has generated interest in conducting surveillance [redacted]; (2) they conduct research [redacted] to determine whether NSA knows the location of the person, or knows information that would provide evidence concerning that location; and (3) they conduct [redacted] to determine or verify information about the person's location. NSA may use information from any one or a combination of these categories of information in evaluating the totality of the circumstances to determine that the potential target is located outside the United States.

~~Derived From: NSA/CSSM 1-52~~
~~Dated: 20070108~~
~~Declassify On: 20320108~~

~~(TS//SI)~~ In addition, in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or [redacted] In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.

~~(S)~~ Lead Information

~~(S)~~ When NSA proposes to direct surveillance at a target, it does so because NSA has already learned something about the target or the facility or facilities the target uses to communicate. Accordingly, NSA will examine the lead information to determine what it reveals about the physical location of the target, including [redacted]

~~(S)~~ The following are examples of the types of lead information that NSA may examine:

[redacted]

~~(S)~~ Information NSA Has About the Target's Location and/or Facility or Facilities Used by the Target

~~(S)~~ NSA may also review information in its databases, including repositories of information collected by NSA and by other intelligence agencies, [redacted], to determine if the person's location, or information providing evidence about the person's location, is already known. The NSA databases that would be used for this purpose contain information culled from signals intelligence, human intelligence, law enforcement information, and other sources. For example, [redacted]

[redacted]

~~(S)~~ **NSA** [redacted]

~~(S)~~ NSA may also [redacted] to assist it in making determinations concerning the location of the person at whom NSA intends to direct surveillance. For example, NSA may examine the following types of information:

[redacted]

~~(S)~~ **Assessment of the Non-United States Person Status of the Target**

~~(S)~~ In many cases, the information that NSA examines in order to determine whether a target is reasonably believed to be located outside the United States may also bear upon the non-United States person status of that target. For example, [redacted] Similarly, information contained in NSA databases, including repositories of information collected by NSA and by other intelligence agencies, may indicate that the target is a non-United States person.

~~(S)~~ Furthermore, in order to prevent the inadvertent targeting of a United States person, NSA [redacted]

[redacted]

(~~S~~) [redacted]

(~~S~~) Assessment of the Foreign Intelligence Purpose of the Targeting

(~~S~~) In assessing whether the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory, NSA considers, among other things, the following factors:

a. With respect to telephone communications:

- [redacted]

[1] (~~TS//SI//NF~~) [redacted]

- [redacted]

b. With respect to Internet communications:

- [redacted]

[redacted]

- [redacted]

II. ~~(S)~~ POST-TARGETING ANALYSIS BY NSA

~~(S//SI)~~ After a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis. Such analysis is designed to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States, and will enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States. Such analysis may include:

a) ~~(S)~~ For telephone numbers:

- [redacted]
- NSA analysts may analyze content for indications that a foreign target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

b) ~~(S)~~ For electronic communications [redacted]

- Routinely checking all electronic communications [redacted] tasked pursuant to these procedures [redacted] to determine if an electronic communications [redacted] was accessed from inside the United States. [redacted]

[redacted]

- [redacted]

- NSA analysts may analyze content for indications that a target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.[2]

~~(S)~~ If NSA determines that a target has entered the United States, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay. [redacted].

~~(S)~~ NSA analysts will also analyze content for indications that a target is a United States person.[3] Such content analysis will be conducted according to analytic and intelligence requirements and priorities. If NSA determines that a target who at the time of targeting was believed to be a non-United States person is believed to be a United States person, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay.

III. (S) DOCUMENTATION

~~(S)~~ Analysts who request tasking will document in the tasking database a citation or citations to the information that led them to reasonably believe that a targeted person is located outside the

---

[2] ~~(S)~~ [redacted]

[3] ~~(S)~~ [redacted]

United States. Before tasking is approved, the database entry for that tasking will be reviewed in order to verify that the database entry contains the necessary citations.

~~(S)~~ A citation is a reference that identifies the source of the information, [redacted] The citation will enable those responsible for conducting oversight to locate and review the information that led NSA analysts to conclude that a target is reasonably believed to be located outside the United States.

~~(S)~~ Analysts also will identify the foreign power or foreign territory about which they expect to obtain foreign intelligence information pursuant to the proposed targeting.

IV. ~~(S)~~ OVERSIGHT AND COMPLIANCE

~~(S)~~ NSA will implement a compliance program, and will conduct ongoing oversight, with respect to its exercise of the authority under section 702 of the Act, including the associated targeting and minimization procedures adopted in accordance with section 702. NSA will develop and deliver training regarding the applicable procedures to ensure intelligence personnel responsible for approving the targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information understand their responsibilities and the procedures that apply to this acquisition. NSA has established processes for ensuring that raw traffic is labeled and stored only in authorized repositories, and is accessible only to those who have had the proper training. NSA will conduct ongoing oversight activities and will make any necessary reports, including those relating to incidents of noncompliance, to the NSA Inspector General and OGC, in accordance with its NSA charter. NSA will also ensure that necessary corrective actions are taken to address any identified deficiencies. To that end, NSA will conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures, and conduct periodic spot checks of queries in data repositories.

~~(S)~~ The Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) will conduct oversight of NSA's exercise of the authority under section 702 of the Act, which will include periodic reviews by DOJ and ODNI personnel to evaluate the implementation of the procedures. Such reviews will occur approximately once every two months.

~~(S)~~ NSA will report to DOJ, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer any incidents of noncompliance with these procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the intentional targeting of a United States person, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States. NSA will provide such reports within five business days of learning of the incident. Any information acquired by intentionally targeting a United States person or a person not reasonably believed to be outside the United States at the time of such targeting will be purged from NSA databases.

~~(S)~~ NSA will report to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI

Office of General Counsel, and to the ODNI Civil Liberties Protection Officer, any incidents of noncompliance (including overcollection) by any electronic communication service provider to whom the Attorney General and Director of National Intelligence issued a directive under section 702. Such report will be made within five business days after determining that the electronic communication service provider has not complied or does not intend to comply with a directive.

~~(S)~~ In the event that NSA concludes that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person is believed to be a United States person, it will take the following steps:

1) Terminate the acquisition without delay and determine whether to seek a Court order under another section of the Act. If NSA inadvertently acquires a communication sent to or from the target while the target is or was located inside the United States, including any communication where the sender and all intended recipients are reasonably believed to be located inside the United States at the time of acquisition, such communication will be treated in accordance with the applicable minimization procedures.

2) Report the incident to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer within five business days.

V. ~~(S)~~ DEPARTURE FROM PROCEDURES

~~(S)~~ If, in order to protect against an immediate threat to the national security, NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the Attorney General and Director of National Intelligence, NSA may take such action and will report that activity promptly to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer. Under such circumstances, the Government will continue to adhere to all of the statutory limitations set forth in subsection 702(b) of the Act.

7/24/14
Date

Eric H. Holder, Jr.
Attorney General of the United States

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix U

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE: DNI/AG 702(g) .
CERTIFICATION [redacted] . [redacted], 2008
~~(S)~~ .
. . . . . Washington, D.C.

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE MARY A. McLAUGHLIN
UNITED STATES FISC JUDGE

APPEARANCES:

Department of Justice: (b)(6); (b)(7)(C) [redacted]
MATTHEW OLSEN

National Security Agency: [redacted]

P R O C E E D I N G S

THE COURT: Good morning again, everyone, and we are on the record. Well, thank you all for coming. I really appreciate it. Before I swear in the nonlawyers who will be speaking, let me just get everybody to introduce themselves, at least those who may be participating in this, and that perhaps I guess could be everybody. Is this [redacted] to my far left and [redacted] And then go ahead, sir.

[redacted]: (b)(6); (b)(7)(C), National Security Division.

THE COURT: All right.

(b)(6); (b)(7)(C): (b)(6); (b)(7)(C) from the National Security [redacted]

MR. OLSEN: Matt Olsen from National Security [redacted]

THE COURT: Then we're with (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) FBI.

(b)(6); (b)(7)(C), FBI.

(b)(6); (b)(7)(C), FBI Office of General [redacted]

[redacted] from NSA General Counsel's [redacted]

THE COURT: And especially those in the back, please speak up so the court reporter can hear you and the little mic can pick up. So that was [redacted] and this is?

[redacted]: I'm [redacted] the FISA technical lead from Oversight and Compliance at NSA.

THE COURT: Thank you. Yes, ma'am.

(b)(6) [redacted] I'm here on behalf of the Director of National Intelligence, Office of General Counsel.

[redacted]: [redacted] from NSA/OGC.

[redacted]: [redacted] from NSA.

[redacted] (b)(6): I'm (b)(6) [redacted] from the Office of General Counsel for CIA.

THE COURT: Very good. And why don't we have our staff introduce themselves as well.

(b)(6) [redacted]

THE COURT: All right. Thank you.

Now I would like to swear in the nonlawyers who may be speaking today. Whoever that consists of, do you want to rise? I'll do it all at one time. All right.

(The witnesses are sworn.)

THE COURT: Well, let me state for the record why we're here, although I think we all do know why we're here.

The purpose of today's hearing is for the Court to receive additional information and/or clarification with respect to its judicial review under section 702(i) of the FISA Amendments Act of 2008.

The Court, of course, did receive from the government on August 5, 2008, an ex parte submission entitled "Government's Ex Parte Submission of [redacted] and Related Procedures and Requests for an Order Approving Such Certification and Procedures."

At that point, the Court reviewed the submission, as the staff did, and after that the staff met with certain members of the government and relayed my questions and their questions to the government. We then received yesterday, August 26, a document entitled "Government's Preliminary Responses to Certain Questions Posed By the Court."

That was very helpful to get that, and I know you must have had to work hard to put it together on such short notice. So I appreciate it, and it was very helpful.

What I'd like to do today is go over some questions that I still have. I think your written response answered -- the questions that you did deal with I think were answered completely, and I probably won't be doing too much with them. I may just want to confirm a couple of things.

Then I have some additional questions that I think probably you're prepared for because the staff raised them, but I didn't

see them in your responses. Okay?

All right. Let me just start with, again, this first couple things I'm doing relates to what you filed yesterday, and again it's just to sort of pinpoint a couple of things on page 5 of yesterday's submission where you were responding to my question concerning [redacted]

In particular, I raise the issue of some concern about the phrase [redacted]

And you did a lengthy response to that, and I appreciated it, and I just want to sort of confirm and hone in on the fact that it is going to be a situation where you're all going to try -- they're going to try to figure out whether this person is a U.S. person. That was the only issue I had, was what's the due diligence that will go on.

And especially I'm impressed with the second bullet point where you said, [redacted] And then you go on and elaborate.

So I just want to get a confirmation that this is not a situation where, [redacted]

[redacted] I mean, it's after due diligence and analysis [redacted] That is correct, Your Honor. As you know, the statute requires us to have a reasonable belief that a target is located outside the United States. The targeting procedures are designed to ensure that NSA analyzes information that gives rise to that reasonable belief. So it is the targeting procedures that imposes the due diligence requirement on the NSA in that respect.

THE COURT: Okay. That's fine. And I think that answers my question.

My next question with respect to what you had given us is on No. 6, page 7, and it's the discussion of the post targeting analysis done by NSA in the targeting procedures, and my question was the procedure said that that [redacted] and I sort of asked that that be fleshed out a little bit, and you all did, and the first two points I understand.

I wasn't too sure, though, what the meaning of the third bullet point was. I mean, I understand the words, but I'm wondering if someone could flesh that out for me a little. It says, "In all cases, analysts remain responsible for following their target's location and for the validity of continued acquisition of information regarding the target."

[redacted] It's my understanding -- and, [redacted] correct me if I'm wrong -- NSA analysts track particular targets. So it is the analyst who determines the extent to which they need to rely on content analysis to determine a target's location as opposed to something more [redacted]. But it is ultimately the analyst's responsibility for maintaining a reasonable belief that that target is located outside the United States.

And I don't know if you'd like to elaborate on that, [redacted]

[redacted] That's correct, and every selector that goes into an NSA [redacted] database has an analyst's name identified with that so we know who bears the ultimate responsibility, and we have processes set up in place to ensure they're doing their work.

THE COURT: Could you just do a minute or two on the processes?

[redacted]: Yes, ma'am. How far back should I start?

THE COURT: I don't know what that means, "how far back," but just hone in on the fact that they're responsible for following their target's locations; in other words, for following it and the validity of the continued acquisition. So having made the initial foreignness determination, how do you go about making sure they are remaining responsible?

[redacted] The first thing they would do, they would [redacted]

[redacted] And if NSA did intercept information, the first thing they would be responsible for would be to review the content of that information to ensure they got the right target and that it was providing foreign intelligence.

Once they do that, they're going to periodically check that depending on [redacted] the analyst has to ensure that they've reviewed that target and that it is meeting a foreign intelligence purpose.

THE COURT: Okay. Any of the staff have any questions on that topic before I move away from it?

All right. Now, this next one relates to an issue that came up at the December '07 hearing before Judge Kotelly on the Protect America Act, and it relates to oversight reviews.

Obviously, the targeting procedures that we're talking about now, at least with respect to the location of potential targets, are similar to what was reviewed by Judge Kotelly and requires oversight reviews by personnel of Justice and the Office of the Director of National Intelligence.

I read the transcript of the hearing before Judge Kotelly, and she took a lot of testimony concerning the oversight up to that point. Can somebody fill me in on where we are today on

that? Has the methodology that's been used by the reviewers changed at all? Could somebody summarize the results of those reviews?

(b)(6); (b)(7)(C) The methodology has been changed. It's been refined. Back in December, because of the volume of selectors and because we hadn't worked through an exact process in how we would conduct our oversight, we weren't in a position to be able to review every single tasking decision that the NSA had made.

We would do it on a sampling basis. Sometimes we randomly picked certain days and we would look at tasking decisions for those days, or if we had a range of selectors that had been tasked, we would randomly select the sources of information upon which the foreignness determinations for those particular selectors were based.

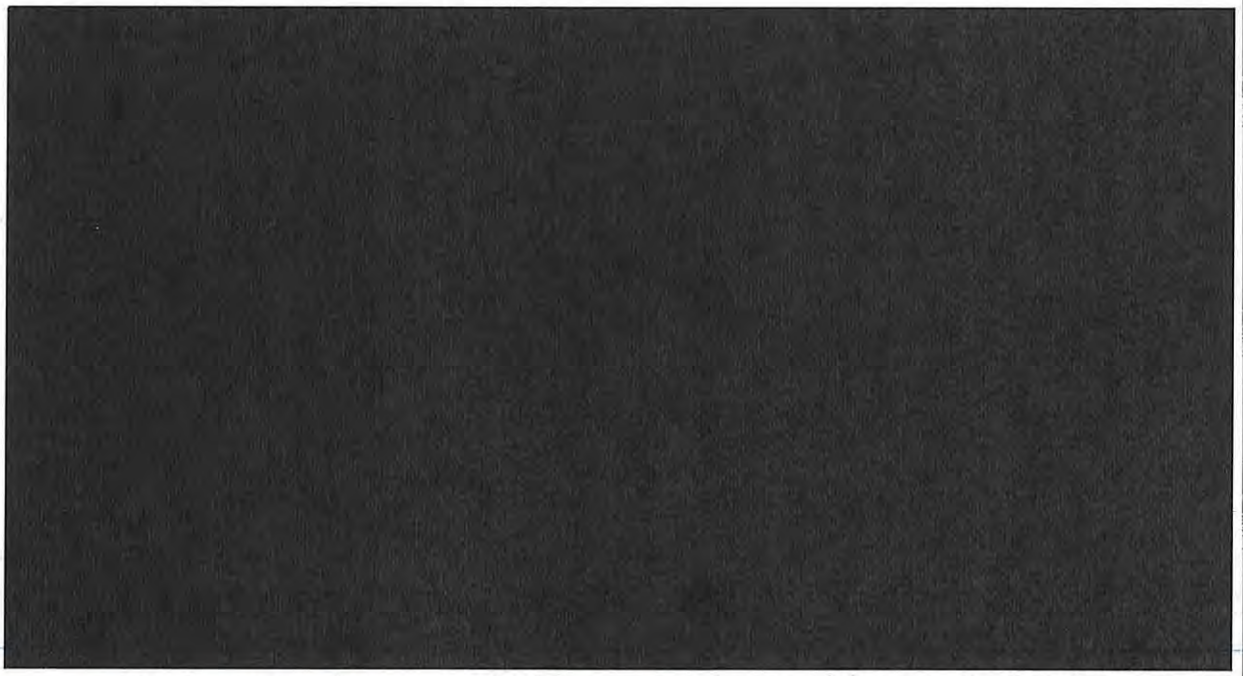
Since then, we've refined our process such that we're actually able to at the very least receive all of the documentation concerning every single tasking decision that NSA has made. Typically, they're sent to us in electronic format.

So we receive those, we print them off, and we review them to make sure that all of the documentation that the targeting procedures require is present, that being a notation about the foreign intelligence purpose of the collection and the source of the information upon which the foreignness determination for that particular selector was based.

~~As~~ we've gone on and we've refined our methodology and we've had back-and-forth with NSA over how we can improve their performance with respect to filling out particular fields in the sheets, as a result of that back-and-forth, we've actually had to review less and less sources because NSA is relying more and more on [redacted] we don't necessarily need to review per se.

I mean, the most common source of information that NSA relies upon is [redacted]

[redacted] selector is used by a [redacted] So therefore, we don't necessarily need to delve into too much more behind that foreignness determination [redacted]



So I guess in a nutshell, we've been able to do basically

more oversight because our oversight over time has become more efficient.

THE COURT: And how about -- and maybe you've in one sense maybe answered this in part, but what's the result of the reviews been? What are the problems you're seeing at this point?

(b)(6); (b)(7)(C) I would say the most common problem -- and "common" is a relative term here, because the volume of selectors is huge, and the number of problems that we're actually seeing is relatively small. As I've said, as we've engaged in oversight and engaged NSA in discussions on how they can improve the sheets and tasking determinations and things of that nature, the number of problems that we've seen have diminished over time.

I would say the most common problem is to the extent that a tasking determination is based on a wide range of information, there may be a problem with how the source of that information is cited, whether it be somebody just inadvertently mistyped [redacted] or inadvertently left out a [redacted] a key piece of information that was part of the broader range of circumstances upon which NSA made its foreignness determination.

So it's more the little technical things that we've been seeing problems with on a very small scale, and as I've said, it's diminished over time.

THE COURT: I think before Judge Kotelly you identified about [redacted] cases where it appeared that a targeted person was in the U.S., and again, I don't even think I know what time frame that was for, but in any event, can you do anything like that now? I mean, since that hearing in December of '07.

(b)(6); (b)(7)(C) Since that time, that number captured a number of different types of incidents that were reported to us. There are incidents where there's true noncompliance with the targeting procedures that results in basically an improper tasking, whether it be because the person was actually located in the United States or the person was a U.S. person and we did not have 2.5 authority to target that person.

That number also captured instances where NSA had a reasonable belief that the person was located outside the United States at the time of targeting but since that time has roamed into the United States, what we call a "roaming incident."

A third type of incident that that number captured is what we would call a tasking error where NSA would run a particular facility through its targeting procedures but in the act of actually targeting that, by keying in the account or phone number into the tasking tool, there was a typo or something of that nature.

At the time of the hearing, we hadn't fully determined which incidents fell necessarily into which category. Since

that time, we've had an opportunity to do that. And for incidents that were reported to us through May 9 of this year, [redacted] incidents involved instances where a target was targeted improperly under the targeting procedures.

We had [redacted] incidents -- one of the things that NSA is required to do when they identify somebody who has roamed into the States is to notify us of that within 72 hours of making that determination.

We had [redacted] instances where a person had roamed into the States but the NSA did not meet that 72-hour reporting requirement. But in all of those [redacted] cases, the tasking itself was reasonable; it's just that they failed to comply with the reporting requirement.

We're tracking a number of other incidents, but with respect to those incidents, we're pretty much in the same posture that we were back in December: They've been reported to us; we don't have all the facts with respect to those incidents yet in order to be able to categorize them and say, okay, this is a true noncompliance incident, this is just a roaming incident, or this is just a tasking error.

THE COURT: Now, the [redacted] situations where you hadn't been notified within 72 hours, you picked it up in a review much later, or how did it come -- did they report it in 72 hours plus 10, or was it picked up when you went over and --

[redacted] No. They actually reported those to us.

THE COURT: Okay.

[redacted] It was just for a variety of reasons they could not comply with the 72 hours. Sometimes it's just because a final determination can take a little while simply to the extent that the information is somewhat ambiguous. I think NSA errs on the side of caution and probably sets the date of that determination sooner rather than later such that the 72-hour reporting requirement is triggered basically at the first instance or first indication as opposed to when a final determination is made.

Again, we've sort of refined the reporting requirement and have explained to NSA basically when that 72-hour reporting requirement kicks in such that we've, again, seen less and less of these incidents as time has gone on.

THE COURT: So you've taken steps to make sure that NSA, their people understand at least your view of the 72 hours in order to cut down on the situations where things aren't reported.

[redacted] Yes. That's one of the most, I think, valuable aspects of the oversight visits. It's not just to, you know, we sit there and we review and go over things with NSA, but then we sort of have -- at the end, we sort of have a roundup where we all talk about issues that have been identified and ways that we can either fix problems or correct things. And I think we've won the fruits of that, as I said, because the

number of incidents we've seen has been diminishing over time.

THE COURT: Okay. Now, what do you foresee under the FISA Amendments Act? Do you foresee the same procedures for your oversight being implemented? Are you planning on different procedures? What are your thoughts?

(b)(6); (b)(7)(C) I can't say for certain. I would anticipate that things would not change, simply because in my view they've been working very well. As I've said, we've seen improvement, I think, just the whole process as we've refined it over the last year. I think where we are right now is probably -- we're in a good spot with respect to oversight, in my view.

THE COURT: All right. Well, what about the non-U.S. person status, which of course is new under the FISA Amendments Act? Are you going to be changing anything in terms of focusing on that?

(b)(6); (b)(7)(C) We already sort of do with respect to -- the U.S. person status is so intertwined with the location of the target [redacted] to the extent that in the past NSA would actually affirmatively identify targeted U.S. persons to us on the sheets, because one of the additional fields that they put in the sheets is basically a blurb, an explanation and a description of the target.

Clearly, we're not allowed to target U.S. persons anymore, so I don't anticipate seeing any such descriptions on the

sheets. But again, since the status of the person, the determination of how that is made is so intertwined with the same information upon which NSA relies to make a foreignness determination, that it would be hard for us not to identify such information as we're conducting the reviews.

THE COURT: Has there been -- and maybe you've said this, but is there thought to be or are you planning to or have you already sat down with people or issued things so that they can now focus on the fact that we've got the non-U.S. person status, which is also something they need to be focusing on?

[redacted] I don't think we've had formal discussions about it. Again, this wasn't an issue that has cropped up out of nowhere where we sort of had to still deal with this issue in the context of the Protect America Act, because under the certifications, we were not allowed to target U.S. persons unless we had 2.5 authority.

THE COURT: Okay.

[redacted] So we always had this affirmative -- although it was not affirmatively stated in the targeting procedures, there was an implicit requirement to ensure that we're not inadvertently or intentionally targeting U.S. persons in the absence of such authority.

So the types of checks that we're doing now build upon checks that we were doing previously in order to satisfy that requirement or limitation.

THE COURT: (b)(6) did you want to follow up on that at all? I know you guys were here last time. Anything?

(b)(6); (b)(7)(C): I don't think I have anything.

THE COURT: Okay. Thank you on that.

My next issue has to do with departures from procedures, if I can phrase it that way. Let me find out where we're going.

Here we are. I know that -- at least I believe the staff talked with you about this before this hearing, and it's page 10 of the targeting procedures. Let me just get them out.

"If, in order to protect against immediate threat to the national security, the NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures," and I know that -- again, was it at the hearing perhaps? I'm not remembering whether it was at the hearing or not. In any event, I know in the past there has been a representation of the situations that you contemplate coming within this. I don't think you dealt with that in your response from yesterday.

(b)(6); (b)(7)(C) No, we didn't.

THE COURT: Okay. Could you just confirm for us -- I know you've already had discussions with staff, but tell me what you expect to be contemplated by this provision.

(b)(6); (b)(7)(C) First, I think the circumstances under which this provision would be triggered would be very extreme

circumstances: an imminent terrorist attack or a terrorist attack that has occurred or something of equal significance. With respect to the types of departures, I mean, in all cases we will continue to adhere to the limitations set forth in the statute.

We are anticipating that the types of departures would be on a more technical level such as perhaps because NSA personnel are devoted to addressing or countering this terrorist threat, they may not be able to devote the resources necessarily for us to conduct an oversight review within the allotted 60 days.

THE COURT: Has this been used? Has the PAA provision ever been used?

(b)(6); (b)(7)(C) [redacted] We've never invoked it.

THE COURT: Never invoked. Okay. Can you give me a little more meat on the bones on what you would contemplate?

[redacted].

[redacted] I think the other situation we thought of is an emergency, as (b)(6); (b)(7)(C) describes, and our actual system for recording things is down. So technically we can't get to the system where we'd record this. We'd still make a note of what we've done, so we would comply substantially with what's required, we wouldn't want the issue to arise and prevent us from doing what we need to do, are we complying in every detail.

So that's the kind of thing that I think we contemplate

that it could be used in, and again, my own expectation is it will never be used, but we did provide for it in the unlikely event.

THE COURT: Okay. All right. Let's talk for a little bit about these *about* communications.

What I would find very helpful -- can someone just briefly and with not a lot of technical but some technical aspects talk to me about how communications are acquired? Are they acquired in a different way than the *to*-or-*from* communications? I mean, as I understand it, you're not acquiring them from Internet service providers, like [redacted] (b)(1); (b)(3); (b)(7)(E)

[redacted]: Judge, if I may, I'm going to let [redacted] come to the table because he's one of the people who can explain this.

THE COURT: Oh, wonderful. Come on up, sir. This is [redacted]

[redacted]. Yes, typically for *about* communications, right now we do not acquire them from Internet service providers [redacted]

So what happens there is you pick up things like two unknown communicants to us and the *to-from* talking about one of

our targeted selectors. That's a very useful case to us because

(b)(1); (b)(3); (b)(7)(E)

That's one example.

Another example is (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

In other arenas as well, (b)(1); (b)(3); (b)(7)(E)

same kind of thing. We maybe find (b)(1); (b)(3); (b)(7)(E) of a known target that provides a unique insight into that foreign intel need.

And another example, just to flesh these out, a bit more is we would have a target who (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

THE COURT: (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E) How do you do it?

[redacted] (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

THE COURT: Yeah.

[redacted] -- that then ensures (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

THE COURT: Okay. Can we talk for a minute -- obviously, the issue for the Court and for the government, as you came up with all these procedures, is the reasonableness

standard, and the Court is looking at that as well as, obviously, compliance with the Fourth Amendment, which in itself is a reasonableness standard, I guess, as well.

Do the *abouts* present a different issue in terms of the reasonableness, do you think? Let me just expand a little bit on that and have some response to it.

What percentage of the acquisitions are *abouts*, as opposed to *to* and *from*? Is an *about* acquisition more or less likely to pick up communications that otherwise you wouldn't be allowed to pick up for whatever reason? Do they present harder issues for reasonableness?

Somebody want to start discussing that with me? Have you thought about that?

[redacted] As far as the percentage number, we don't have a number for that, because as I mentioned earlier, when we [redacted] we find *to's* and *froms* and [redacted] so we don't categorize those separately to be able to count those communication as *abouts*.

So we don't have any numbers. I can tell you as far as usefulness, they're very useful, and we see them routinely, but I don't have a number for you on that.

THE COURT: And in terms of the usefulness, their importance to what you're trying to accomplish, talk to me a little bit about that. As important as a *to* or *from*, less important? What role do they play in what you're doing?

[redacted] They're very useful in [redacted]

[redacted]

So, for example, in the [redacted] (b)(1); (b)(3); (b)(7)(E) [redacted] (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

[redacted]

[redacted]

THE COURT: Now, you're saying in your response, still on the *abouts*, "the operation of the Internet protocol address filters or [redacted] prevents the intentional acquisition of communications about the target as to which the senders and all intended recipients are known at the time of acquisition to be located in the U.S."

[redacted] What about the U.S. person status, how that is more difficult to account for or to --

(b)(6); (b)(7)(C) Well, first of all, it's our position that the target of an *abouts* communication is still the user of the targeted selector. It's not the sender or recipient of the e-mail or other communication that contains the targeted selector. I mean, that's where the foreign intelligence interests lie, in the user of the targeted selector.

To the extent that the IP filters and [redacted] ensure that at least one end of the communication is outside the United States, more often than not, I would suspect both ends of the communication are outside the United States. We're collecting *abouts* of purely transient communications such that it's less likely that there's U.S. persons involved or U.S.-person information involved.

But even to the extent that one of the communicants was a U.S. person or was located in the United States, to the extent that there's U.S.-person information in the *abouts* communication, that information will be subject to the minimization procedures.

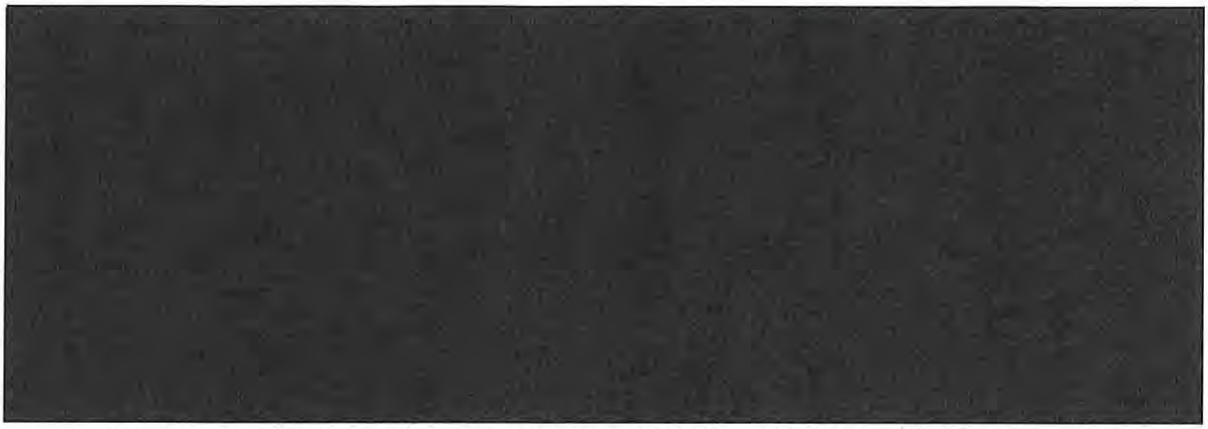
THE COURT: Okay. Anything from staff on the *abouts*? I'm going to talk some more about the filter issue but from a different perspective. Anybody?

[redacted] (b)(6) Judge, I think I do have a question.

THE COURT: Yes. Go ahead, Phil.

[redacted] (b)(6) When you describe how [redacted] these *about* communications, you described it in a way -- well, you said that [redacted] acquiring the *to-or-from* communications [redacted], if you wanted to for whatever reason, would it be technically feasible to -- in the same manner [redacted] would it be technically feasible to acquire only communications that are to or from the selector account and not those communications that otherwise contain a reference or name of a selector account?

[redacted] It is technically feasible. The problem with doing so is if you end up discarding a number of communications that are truly *to-froms* that you should be able to collect but [redacted]



So by trying to limit us to say no *abouts*, then we end up cutting out those kind of communications as well, truly *to-froms*. So it would be -- we're not surgical enough to take that out of the equation without impacting our ability to do *to-froms* effectively.

(b)(6) Okay.

Judge, may I offer --

THE COURT: Sure. This is right?

-- as to the reasonableness. I think you asked the question about reasonableness we haven't addressed. But one of the things the way we have this structured, we think it is akin to -- not exactly the same, but akin to finding a connection between a targeted e-mail address and a person outside the United States.

And for that communication only, we think it's reasonable to make that newly discovered person -- to acquire his communications. There's no automated tasking of that newly discovered person that takes place. Nothing happens as a matter of course. We only collect that single communication, and then

we assess it as to whether we want to make a new target there of the person overseas. But it's important, I think, to understand there's no follow-on automated, *now we found a new person, a new person, a new person*, and those are not automatically added to our task mode.

So it's a limited look with our target, the user of the e-mail address continuing to be our target, [redacted]

[redacted]

THE COURT: Yes. I'm glad you brought that up, [redacted] because what I understand, and I think you've just said it, is that when you're picking up the *about*, you're also getting information on the *to* and *from*. But if the *to* or *from* is now a person of interest, but if it's a U.S. person, for example, or something, you couldn't continue to just pick up that person, directed at the person, but then you'd have to come into court with an application or do whatever else. But you're not automatically then following that person.

[redacted] That's correct.

THE COURT: Now, on the IP -- this is getting to minimization, but because it relates to the filters, let's talk about it. And this is on page 5 of your written response from yesterday. The NSA minimization procedures, you're stating, "contain a provision for allowing retention of information

because of limitations on NSA's ability to filter communications." My question I had was is the filter discussed in targeting the same filtering. I just wanted to understand that, and apparently it is.

But talk to me a little bit, because there seemed to be some tension there. [redacted]

[redacted]

(b)(6); (b)(7)(C) I think the inclusion of that provision in the minimization procedures was intended to be prophylactic in the event that the filters don't necessarily work, and NSA has represented that it's been their experience with the filters and [redacted] that they have not captured purely domestic communications with respect to the *abouts*.

But to the extent that [redacted]

[redacted]

this provision basically captures instances where the filters may not work in every instance.

THE COURT: You did respond to this, but I guess maybe just a little bit more on how limited are they. I mean, what are the limitation of these filters?

[redacted] Limitations really come down to -- the

filter is basically [redacted]

[redacted]

[redacted]

THE COURT: (b)(6)

(b)(6) Thank you, Judge.

[redacted]

[redacted]

THE COURT: Okay.

(b)(6) With one other question. For example, with the filters, [redacted]

[redacted]

(b)(6) [redacted]

[redacted]

(b)(6) [redacted]:

MR. (b)(6) [redacted]

[redacted] (b)(6) [redacted]:

[redacted]

MR. (b)(6) [redacted]

[redacted]

(b)(6) [redacted]

[redacted]

MR. (b)(6) [redacted]

[redacted]

THE COURT: Okay. Again, going on or continuing with minimization procedures, let me see where I am here. Just a couple of things that I think the staff confirmed with you prior to the hearing when they raised various issues. And it wasn't in your memo from yesterday, so I'll just raise it here. But as I understand it, (b)(1); (b)(3); (b)(7)(E) [redacted]

(b)(6); (b)(7)(C) That's correct.

THE COURT: Okay. And on page 1, I guess it was, of (b)(1); (b)(3); (b)(7)(E) [redacted]

[redacted] (b)(6); (b)(7)(C) Yes.

THE COURT: All right. And then I wanted to go to 3(b)(1) of the minimization procedures, a paragraph I will tell you that I had some struggles with, but now I think I understand it.

(b)(6) [redacted] This will be the NSA minimizations --

THE COURT: I'm sorry, NSA.

All right. Now, first of all, as I understand it, I thought there was a "not" missing, and there was.

(b)(6); (b)(7)(C) [redacted] There is.

THE COURT: Okay, that's fine. I kept reading and thinking I was missing something, and it took me awhile. But let me just say to you what I understand this paragraph to mean, and then tell me if it -- that "NSA shall destroy inadvertently acquired U.S.-persons communications once they are identified as both clearly not relevant to the authorized purpose of the acquisition and not containing evidence of a crime." And also "inadvertently acquired U.S.-person communications includes these electronic communications acquired because of limitations of the ability to filter." That was the filter issue.

That's what will happen, and the time limit is a maximum of five years.

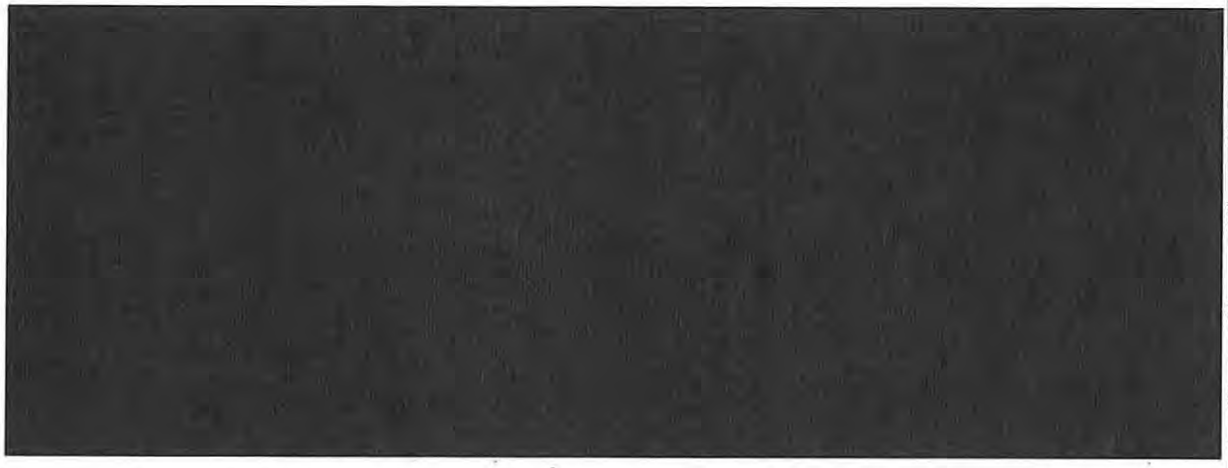
(b)(6); (b)(7) [redacted]: Correct.

THE COURT: It will be done at least with respect to the first part of 3(b)(1) at the earliest practical point, but at least five years --

(b)(6); (b)(7)(C) [redacted]: No later than five years.

THE COURT: No later than five years. And I understand that five years has been a time frame that has appeared in other procedures, but I think it probably would be helpful to just sort of talk a bit about where that comes from, why is that a number that's been selected.

(b)(6); (b)(7)(C) [redacted]: NSA can correct me if I'm wrong; the five years comes from the fact that [redacted]



That, I think, is the general thinking behind the five-year retention period. That's the potential analytical life cycle of a particular piece of information.

[redacted] Your Honor, this is [redacted] for the NSA.

THE COURT: Sure. Yes, sir.

[redacted] In a couple of other places in our minimization procedures, namely in Section 5 and Section 6, we talk about the five-year rule where in certain cases the intelligence director may extend that in the case of domestic communications or in the case of U.S.-person information if again it has foreign intelligence value or evidence of a crime.

So in 3(b)(1) we talk about five years, but there are a couple of other sections that might be invoked by our SID director where he could extend it.

THE COURT: Yes. Well, I think this makes clear that it's not talking about things that are not relevant -- it's only talking about things that are not relevant to the authorized

purpose of the acquisition and not containing evidence of a crime. So the implication is that if it does do that, the five years may not necessarily be -- fair enough.

All right. Number 13, page 11 of your response from yesterday. Now, I had a couple of questions with respect to the three minimization procedures and what they say about the director being able to do certain things, but (b)(6); (b)(7)(C), I understand that you alerted the staff before the hearing that there's another potential issue that you have thought of that could impact this issue.

(b)(6); (b)(7)(C) Correct. There's a provision in the FISA that was recently changed, 1806(i), which basically says -- the previous iteration of that provision of the statute said if you are unintentionally acquiring radio communications when the sender and all intended recipients are located in the United States, the attorney general has to determine whether or not that piece of information can be retained in very extreme circumstances, otherwise such circumstances have to be destroyed upon recognition.

The recent FISA Amendments Act struck "radio" out of that provision such that the provision appears to on its face apply to all types of acquisitions conducted under the act. Whether or not that particular provision applies to this type of collection such that it would require us to basically destroy domestic communications as they are recognized is an issue that

we're still trying to work through.

THE COURT: Okay. All right. And I'm sure we'll continue to talk on that as you work it through, and thank you for alerting us to that. Let me go forward, though, with the minimization procedures as they are, and let me ask a couple of questions about them, putting aside for the moment this issue with 1806.

We had one question for you, and now I don't know if we asked you this before, but the one question was the NSA and the CIA procedures had the directors doing things in writing. And the FBI provision didn't say "in writing," but as I understand it, the FBI, as you cite here, has represented that any such determination by the director would be made in writing even if not expressly required.

(b)(6); (b)(7)(C): Correct.

THE COURT: Okay. That answers that. Another similar kind of question. There may be no significance to the difference in language, but the NSA procedures at page 5 say, and I'm paraphrasing because I don't have the exact quote, that unless the director "specifically determines" something.

And then the FBI provisions simply say "unless the director determines," and I think the CIA also says "unless the director determines." Is there any meaning I'm supposed to take from "specifically?"

(b)(6); (b)(7)(C): No. I think "specifically" was just

intended to capture the notion that this would be on a case-by-case basis as opposed to just a broad-base, I'm going to exempt this particular gigantic class of communications.

THE COURT: But I take it the FBI and a CIA would also be on a case-by-case basis.

[redacted] Yes.

THE COURT: Yeah, I didn't think it had a lot of significance, but you never know, so I thought I'd ask.

You know, I may be at the end of my list. What I'd like to do is take a break. But since there's fewer of us than of you, we will step out, and then you can stay here and if -- because there's a lot of people here.

Obviously, use the time. If something was said here that you have an issue with because, you know, at least from your experience it doesn't work that way, please talk among yourselves and we can straighten that out. Or, if I had asked a question and you say, *Gee, I think the best answer is X and nobody said X*, please feel free to tell [redacted] and we can get that better answered on the record.

Okay. Thanks, everybody. Just give us a few minutes.

(Recess taken.)

THE COURT: Just a couple things. Going back to the *abouts*, if we can go back to them for a moment, you know the Court will have to do, obviously, a Fourth Amendment analysis in terms of the reasonableness -- of all the procedures, not just

of the *abouts*.

But I guess my question is, is there a different analysis for the *abouts* than for the *to* or *from*? Or to put it another way, could somebody articulate for me what you believe why the *abouts* don't present a different Fourth Amendment issue from the *to's* and the *froms*, that it's the same issue?

Again, to amplify even a little more, is the possibility of acquiring information that otherwise it would not be permissible to acquire in the *about* scenario different from the *to* or *from*?

In other words, is it incidental? Would you describe it in that way? If not, how would you describe it? Is it any less or more likely to happen with the *abouts* than with the *to* or *from*? Or any other aspect of the Fourth Amendment analysis that you think is relevant.

[redacted] I don't think that the Fourth Amendment analysis is any different with respect to an *abouts* communication or *to* or *from*. I mean, it's just as likely that one end of a *to* or *from* could be a U.S. person in communication with a target as an *about*.

In either case, the U.S.-person information contained in that communication would be subject to the minimization procedures, and it's not that U.S. person that is the target of the acquisition of that particular communication; it is the user of the targeted selector that appears in the body of that communication. So I think for Fourth Amendment purposes, with

respect to U.S. persons, I don't think the analysis is any different.

MR. OLSEN: We have given some thought to this, because *abouts* collections has been an issue in this collection as well as prior court orders. But I just would reiterate what [redacted] said in terms of our view of it in that it's essentially for the Fourth Amendment purposes an incidental collection where the target is the targeted account, and to the extent that a U.S. person's communication -- to or from a U.S. person, that would be deemed to be incidental to the collection.

And therefore under the analysis we put forward in, for example, the Yahoo litigation, that would be permissible and reasonable under the Fourth Amendment as long as minimization procedures are appropriately applied.

THE COURT: Is it more or less likely to pick up U.S.-person information in an *about* than a *to* or a *from*?

MR. OLSEN: I don't know the answer in practice. At least from my perspective in theory, I wouldn't see why it would be more likely than a targeted *to* or *from* collection where the target's outside the United States where there's similarly the possibility that that target would be in communication with someone in the United States, with a U.S. person in the United States.

So, just analytically, I think the same incidental collection subject to minimization procedures framework would

apply. And so under the Fourth Amendment applying, that we would submit would be reasonable under the Fourth Amendment.

(b)(6); (b)(7)(C) And I would note that in his opinion on the Yahoo litigation, Judge Walton recognized the reasonableness of a presumption that non-U.S. persons located overseas are more likely to communicate with other non-U.S. persons located overseas which may bear on the volume of potentially -- or *abouts* communications that potentially implicate U.S. persons versus non-U.S. persons. I think if you apply that presumption, it's more likely that an *about* will not implicate U.S.-person information.

THE COURT: Okay. Fair enough.

Well, that's really all that I --

(b)(6) Judge, I'm sorry.

THE COURT: Yes. Go ahead, (b)(6)

(b)(6) With regard to the *abouts*, it's occurred to me, just to be clear on the record, there were [redacted] sort of subcategories of such communications that were laid out in a footnote to Judge Kotelly's opinion in the PAA that in turn I think referred to an opinion issued or an order issued by Judge Vinson last year.

Do those [redacted] categories, as previously set out in those places, continue to be accurate and up to date and complete in terms of the communications that are obtained?

[redacted] I think so. If I recall correctly, and I

may not have all [redacted] categories off the top of my head, we have the instance where the selector is mentioned in the body of an e-mail sent between two communicants.

You have an instance where [redacted]

THE COURT: Well, there was [redacted]

[redacted] (b)(6); (b)(7)(C): Oh, [redacted] yes.

(b)(6) [redacted] And [redacted]

(b)(6); (b)(7)(C) [redacted]

(b)(6) [redacted]

[redacted] Yes.

THE COURT: Okay. Thank you, (b)(6), for that. Appreciate it. So I guess the only other outstanding issue at the moment is the 1806, I'll call it, issue, and what is your thinking in terms of timing? Obviously, at this point at least we have the September 4 deadline that we're looking at, but what are your thoughts on timing?

MR. OLSEN: We're going to turn to this immediately

following the hearing. This has been, as I think (b)(6); (b)(7)(C) mentioned, been an issue we identified yesterday or the day before in the evening.

So we have the right folks here to talk about it, and my expectation first would be that we would be able to communicate directly with the Court staff. I don't know how quickly we will have a definitive answer, but I would expect that we will have a definitive answer, understanding the timing of this overall, by tomorrow at some point and that what I expect to do is to have something in writing, perhaps not very formal, something along the lines of what we recently gave to the Court to address this issue.

It may be that that will be, in terms of our view, that we think we have a resolution to the issue and that no further action is necessary. It may be that we have other steps to propose to the Court, but we certainly understand the importance of moving quickly and turn to this right away.

THE COURT: Okay. Fair enough.

(b)(6); (b)(7)(C) And there were three other issues that we'd just like to clarify, statements that were made previously that we just want to provide maybe a fuller context to.

THE COURT: Sure.

(b)(6); (b)(7)(C) With respect to oversight and the number of compliance incidents that we've identified, just to give you some perspective on the relative nature of that number, since

the acquisition of the Protect America Act began, NSA has tasked over [redacted] selectors. So the fact that we've identified [redacted] or so actual compliance incidents is, relatively speaking, a very, very small number.

Another point that we'd just like to provide a little more clarification on is the point that [redacted] made with respect to extending the five-year retention period for particular communications, and maybe [redacted] can expand on this a little bit more.

We just want to make it clear that with respect to the determination by the SID director to extend that, that's not on a communication-by-communication or selector-by-selector basis. It can be a broader range of communications that the SID director may make that determination for and extend the retention period.

THE COURT: Are you focusing on a particular part of the procedures? Can we look at them? That will help me, I think. These are the NSA minimization procedures?

(b)(6) [redacted] It's section 6(b).

(b)(6); (b)(7)(C) [redacted] There's one in 6(b), and there's one in 5(3)(b).

(b)(6) [redacted]: May I ask a question?

THE COURT: Absolutely. Go ahead, (b)(6) [redacted]

(b)(6) [redacted] Has the SID director invoked this provision? Is there an extension currently in place?

[redacted]: There's not under PAA. [redacted]

[redacted]

[redacted]

(b)(6) [redacted]

[redacted]

[redacted]: [redacted].

(b)(6) [redacted]: Oh, I see.

[redacted]: [redacted]

[redacted] Our concern, we don't want to leave a misimpression, when you read this together, if we discover -- if we find that there are U.S.-person communications here, we will take this action.

If, however, we haven't discovered that and the SID director extends the period, it's possible it will be undiscovered U.S.-person communication during that seven-year period. So we don't want to give a misimpression by saying retained no longer than five years in any event.

I guess it should be read to say in any event -- I don't know where it is, but it allows the SID director to extend the retention period as invoked. In that case, undiscovered. We haven't realized it, but we have these kinds of communications. They would continue to be retained as well.

THE COURT: That's because they're undiscovered. If it's discovered, it's five years.

MR. [redacted]: That's correct. If it's discovered --

THE COURT: Yeah. If they're discovered.

[redacted] They would be destroyed at that time.

THE COURT: Obviously, if they're not -- okay.

(b)(6); (b)(7)(C), now that I've read them again, can you just repeat what you said you wanted to make clear, that this wasn't on a case-by-case basis?

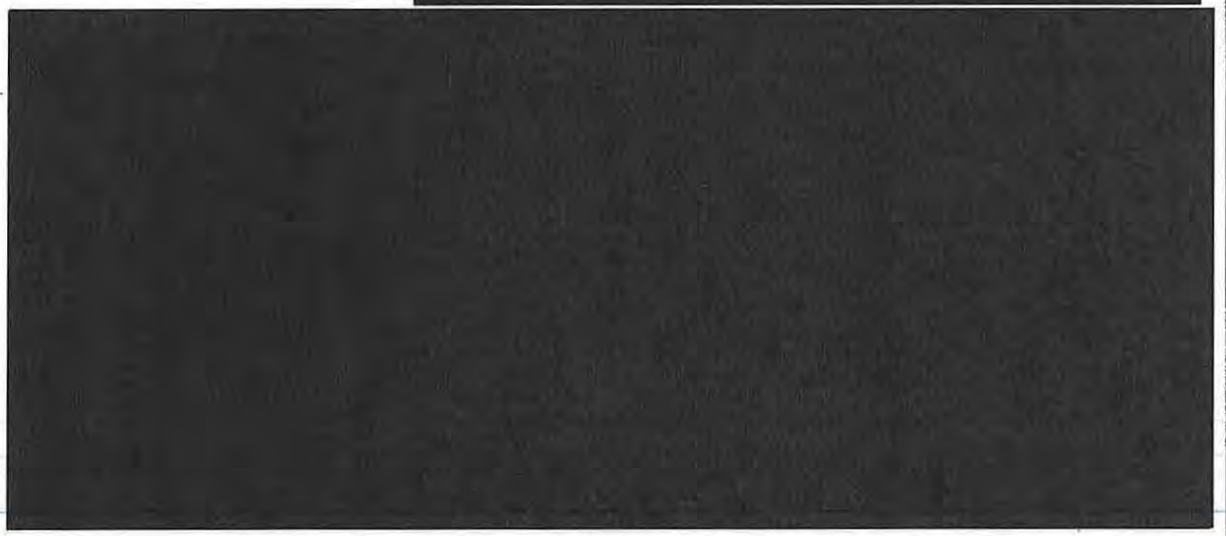
(b)(6); (b)(7)(C) It can apply to a broader range of communications. It's not, okay, the SID director determines that this --

THE COURT: Particular little thing right there.

(b)(6); (b)(7)(C) -- meets this standard, therefore I can extend the retention duration beyond the five years. It can be a range of communications.

THE COURT: Just give me an example. I think we just had one. Can somebody give me an example?

[redacted]



THE COURT: I see. Okay. Thank you.

(b)(6); (b)(7)(C) And one last clarification. With respect to the ongoing requirement that an analyst keep track of its targets and basically is responsible for ensuring the continuing foreign intelligence purpose of the collection, [redacted] said NSA imposes a [redacted] that the analyst has to make that determination.

We just want it to be clear that that is the outer limit of the requirement that that determination be made and that in practice that determination is made on a much more ongoing basis than just [redacted]

THE COURT: And I don't think I understood it to mean [redacted] but I appreciate that clarification.

All right. Anything else?

(b)(6); (b)(7)(C) That's all, Your Honor.

THE COURT: Okay. Thank you so much, everybody. I appreciate it. All right. We are adjourned.

(Proceedings adjourned at 11:02 a.m.)

(b)(6) Deputy Clerk
FISC, certify that this document is a true and correct copy of the original. (b)(6)

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix V

2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum

A Stream Reassembly mechanism based on DPI

Shuhui Chen
College of Computer Science
National University of Defense Technology
Changsha, China
Email: shchen@nudt.edu.cn

Yong Tang
College of Computer Science
National University of Defense Technology
Changsha, China
Email: ytang@nudt.edu.cn

***Abstract*—Stream Reassembly is an indispensable function of Deep Packet Inspection, which is an critical element of Network Intrusion System. However, since it need to heavily move packet payload from one block of memory to another block of memory, Stream Reassembly has a serious memory performance issue. In this paper, in order to improve the Stream Reassembly performance, a Stream Reassembly Card (SRC) is designed, which enables to manage and assemble streams through adding a level of buffer to adjust the sequence of packets by using the Multi-core NPU. Specifically, three optimistic techniques, namely Stream Table Dispatching, No-Locking Timeout, and Multi-channel Virtual Queue are introduced in SRC design. The experiments show that the reassembly can achieve more than 3 Gbps in terms of processing speed, triply outperforming over the traditional server based architecture.**

***Index Terms*—Network Security; Network Intrusion System; Network Forensics System; Multi-core NPU; Stream Reassembly;**

I. Introduction

DPI (Deep Packet Inspection) is a critical technique for Network Forensic System (NFS), where packet payloads need to be matched against pre-defined patterns to obtain the evidences with a 4-step process, namely preprocessing, header-matching, content-matching and outputting in NIDS and NFS. In general, in the event of a network with a low speed, server based approach (in which the stream reassembly, rule matching and warning are all conducted by one server) can satisfy the performance requirement. However, with the exponential increasing of bandwidth, the traditional server based approach (even for a server with high performance) no longer meets the performance requirement. To break up this bottleneck, many researches have been carried on to improve the overall performance by achieving efficient content-matching [1]–[6].

Many previously reported methods mainly focus on improving the rule matching algorithms, and/or using FPGA [1], [2] or GPU [3]–[6] for efficient content-matching, and the results show that the ratio of running time used for matching is decreasing with the enhancement of matching performance. Experiments from some other researchers [7] further indicated that when the ratio of the matching time to the overall decrease to 1%, Stream4 (which reassembles streams in previous Snort version) will take on the load of 80% when it is used to assemble the packets.

Currently, advanced progresses have been made in the network electron component area. For example, Raza Micro-electronics has developed XLR, XLS and XLP NPUs, while Cavium has launched OCTEON Series NPU. The emergence of these multi-core NPUs can largely improve the performance of the network devices and network security devices. In this paper, we present a new Stream Reassembly Card (SRC) design, which enables to manage and assemble streams through adding a level of buffer to adjust the sequence of packets by using the Multi-core NPU.

II. Related Work

There are two open source programs: Libnids [8] and Tcpflow [9] that fulfill TCP stream reassembly, but both of them cannot meet the performance requirements of the current network links. Researchs having relationship with stream are often focus on the measurements.

For example, [10] has used two data recorded from two different operational networks, and studied the flows in size, duration, rate and burst, and examined how they are correlated. [11] concerned on the problem of counting the distinct flows on a high speed network link. They proposed a new timestamp-vector algorithm that retains the fast estimation and small memory requirement of the bitmap-based algorithms while reducing the possibility of underestimating the number of active flows.

[12] has introduced a TCP reassembly model and a stream verification methodology that can be used to derive and compute reassembly errors. [13] has introduced an algorithm that solves the problem of TCP stream reassembling and matching performance problem for network forensics system and IDS. Instead of caching the total fragments, their methods stores each fragment with a two-tuple that is constant size data structure, thus the memory requirement involved in caching fragments is largely reduced.

[14] has introduced a hardware based reassembly system to solve both the efficiency and robust performance problems in the face of the adversaries to subvert it. They characterized the behavior of out-of-sequence packets seen in benign TCP traffic, and designed a system that addresses the most commonly observed packet-reordering case in which connections have at most a single sequence hole in only one direction of the stream.

III. Why Multi-core NPU is Selected

NIDS obtains copies of packets directly from the network media, regardless of their destination. Raw packets captured

978-0-7695-4676-6/12 $26.00 © 2012 IEEE
DOI 10.1109/IPDPSW.2012.152

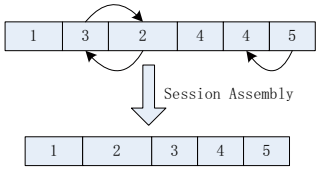


Fig. 1. An example of stream reassembly.

by the NIDS are confused and disordered messes, but DPI in NIDS needs these packets to be fabricated as integrated blocks according to their TCP stream belongings before they are sent to the matching engine.

Figure. 1 gives an instance, and the stream in the example is composed of 6 packets. But packet 2 and packet 3 are out of order, and packet 4 is repeated. The stream reassembly process needs to exchange the sequence of packet 2 and packet 3, and the unwanted second packet 4 should also be deleted. The process incurs 3 times packets movement: packet 2 moving ahead, packet 3 moving backwards, and packet 5 moving ahead. This is just an example of a single stream, and in the real network environment, one backbone link may contain a large number of streams. In other words, there may be too many packet movements in the reassembling process. Modern servers use DRAM (DDR2 or DDR3) as their main memory, one memory access may take a number of cycles to obtain a result because DRAM has a relatively long startup time.

However, multi-core NPU can improve the performance of this kind of operation, which is because:

(1) There are many hardware threads in one core and many cores in one NPU, which makes the total threads in a NPU, will be more than a dozen. The threads of this kind are hardware threads instead of software threads so the switching cost is very low. The large number of hardware contexts enables software to more effectively leverage the inherent parallelism exhibited by packet assembling applications. When one thread is waiting for the result of the memory accessing, the other thread could switch in and makes another memory accessing request, and if many threads use such a pipeline, the latency of the DRAM will be hidden and the effective bandwidths of the DRAM access would increase.

(2) A multi-core NPU is often with low electric power consumption, so it is easy to be manufactured as a card. When a NPU based card is used, an extra buffer is introduced to the processing flow, so the packets can be sorted as they are being transferred from the memory of the card to the memory of the host (server), which is a form of trading space for performance. In this way, when the packets have been received into the memory of the card, they are stored in the memory as their reaching order, but their sequence are maintained by the software running on the NPU.

(3) The architecture of NPU often has a favorable I/O features, and the packets could be imported from the interface to the memory with high throughput. As the dispatching component generally dispatch packet according to the selected bits from the packet head, stream reserved would not be a problem. Since many researches [15], [16] focus on how to accelerate the packets capturing performance, an approach combination packets capture and stream reassembly is cost-effective.

(4) NPU often has a well designed message-passing mechanism between different threads, which uses cross-bar structure or fast shared SRAM as its transferring medium, and makes the cooperation and synchronization between threads facile.

IV. System Architecture

A. Stream in TCP Transferring Level

We focus on three different critical actions, which are TCB creation (the point at which an IDS decides to instantiate a new TCB for a detected connection), Packet Reorder(the process an NIDS uses to reconstruct a stream associated with an open TCB), and TCB Termination (the point at which the IDS decides to close a TCB). Every TCP connection can be expressed as a four-element tuple (which includes source IP, source port, destination IP, and destination port). Once a packet is captured, its corresponding stream needs to be found and the TCB data structure needs to be updated. Basically, TCB is attached to a Hash Table indexed by hash algorithm using some bits from the four-element tuple as parameters. Collisions lead to several TCBs attached to one table entry.

B. Frameworks of SRC

The framework of SRC is depicted in Figure. 2. In SRC, packets are captured from the interfaces to the memory; for maintaining the TCP connection data, a hash table known as Stream Table is used. When the packets enter the memory, their locations are stored in the packet descriptions. Besides the points which point to the packets, packet descriptions also contain the packet length and the fields used to dispatch the packets to the threads.

Threads running on the NPU wait circularly, processing a received packet and then waiting for another packet. Once the data needs to be submitted, every thread is responsible for the task of submitting the packets from the memory of the NPU to the memory of the host. Both the softwares running on the NPU and CPU share a little memory space in the DDR of the NPU for message communication, and the memory space is used by the NPU to get the address of the DMA, the timeout of the host setting, the BlockSize, and the consuming states; CPU can also use the memory space to gain the running states of the NPU. As the packets are DMAed to the host memory, the transferring is conducted one packet after another, which is due to the packets are not stored consecutively in the memory of the NPU while we need them to be consecutive when they reach the memory of the CPU.

Software running on the NPU mainly executes three actions mentioned in Section. IV-A: TCB Creation, Packet Reordering, and TCB Termination. When a packet reaches one core, the related thread looks up the Stream Tables to determine whether there is a corresponding TCB exists. If not, the corresponding TCB is created, and the packet is appended to the TCB. Or else, the packet is appended to the corresponding TCB and its link position is determined; meanwhile, a judgment is made

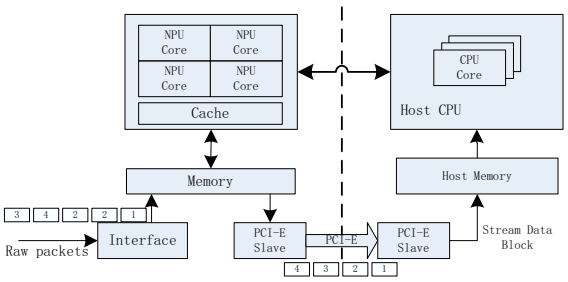


Fig. 2. Frameworks of SRC.

on whether the total packet size of the stream is equal or larger than BlockSize (Submitting Block Size). If the answer is positive, all the packets are submitted in the light of their sequence to the Host.

The total connection records are maintained in a hash table called Stream Table for efficient access. Note that the hash needs to be independent of the permutation of source and destination pairs, which could be achieved by comparison the source IP together with source port and destination IP together with the destination port, and always make the less one to be the first parameter or using some hash algorithms that are not sensitive to the sequence of parameters. Using such hash values as the indexes to the stream table, the corresponding connection can be located. Hash collisions can be resolved by chaining the colliding TCBs in a linked list.

Data submission procedure running by the packet processing threads needs to work cooperatively with the program running on the host CPU. A consecutive memory chunk needs to be allocated to storage the packets uploaded, and for the convenience of the packet organization, the chunk needs to be divided into fix-sized buffers which are organized as a ring. Software (IDS and NFS) running on host continually process the data block received.

C. The Procedures of Stream Reassembly

The two significant data structures in stream reassembly are stream table and TCB. Stream table is made up of many entries, each of which points to a list of TCBs that have the same hash value. In SRC, two types of threads are used to fulfill the stream reassembly: the packet processing thread and the timeout thread. The packet processing threads are responsible for packet receiving, stream reconstruction and data submission; moreover, stream reconstruction is divided into TCB Creation, Packet Reordering and TCB Termination. The timeout thread is a simple circular procedure; it accesses TCBs one by one ceaselessly, comparing the current time with the time of the last coming packet in every stream. If the gap between the two times is large than the appointed value, timeout thread deems that the corresponding stream may be asleep or dead, so it submits the remaining data and delete the TCB to give space to other streams.

The main purpose of *ReorderPacket* is to sort the one-stream-affiliated packets according to their TCP sequence number, and drop the repeated packets that have the same sequence number. Instead of being processed after a batch of packets belonging to a stream have been received, the packets are maintained their order upon being received. The reasons why it does in this way are as follows: (1) The batch processing could cause the computing burst, which is detrimental to the smooth process; (2) Disordered packets are rare actually, most of the arrived packets are ordinal and consecutive. As a result, processing packets one by one will save more computational resource.

As the data is submitted to the host, all the packets must be insured to be ordinal and consecutive. We use **ordering** to express the sequence of the packet and **continuity** to denote if there is any packet should reach but have not reached. When the packets reache, their ordering can be insured by sorting the sequence number and modifying the points of the list that attached packets, but the continuity cannot be ensured, it is due to the disordered arrival is available. To determine if the data can be submitted, a counter DisContinuity Number (DCN) is used to identify if the received packets is continuous or not. DCN is the counter of gaps between adjoining packets for a stream.

The larger the DCN is, the more the degree of discontinuity is. An example is given as follows: for one direction of a stream, if packets 1, 2, 3, 4, 5, and 7 have been received (the numbers are the order numbers of the packet been sent out, not the sequence numbers of the TCP level), the DCN of the stream is 1, because there is a gap between packet 5 and packet 7. If packets 1, 2, 3, 4, and 7 have been received, the DCN of the stream is still 1, because even through there are two packets between packet 4 and packet 7 as they look like, we do not know there is one packet or two packets can fill in this gap when we receive the packet 7, the only fact we know is that there is a gap between the sequence number of packet 4 and packet 7 from TCP level.

All the packets are linked up while the packets with smaller sequence number are in the front of the link and the packets with bigger sequence number are at the back of the link. Bidirectional links for the packets are needed, because packets needed to submitted from NPU to CPU according to the sequence number of the packets. But when a packet arrivals, locating the inserting point from the verse direction may gain better performance. That is because the gap exists scarcely; and even when it emerges, it will be filled up quickly.

When a stream ends, timeouts or its size exceeds the BlockSize, the packets belong the stream must be uploaded to the CPU. Under the circumstances of stream end or timeout, DCN will be zero if all is OK. If it is not zero for some packets have not been received, there is nothing can be done by the reassembly component. But if we are under the third circumstance, which shows that the size of the stream achieves the BlockSize, and the DCN is not zero, reassembly component needs to find the gap that causing the DCN to be not zero. We can look for the link of the stream, if the lost packets are far from the last packet (for example, 8 packets is an experiential value), the finding process is stopped and the packets are submitted, considering that packets will not arrive.

On the other hand, if the gap is among the last 8 packets, we will submit the integrated packets and maintain the remanent inconsecutive packets of the stream. To sum up, we try to upload the packets that are consecutive to the host.

V. Improvement

A. Stream Table Dispatching Technique

There are two techniques can be implemented to organize the TCB in the stream table: shared stream table and separated stream table. For the shared stream table, all the threads share a whole stream table, so all the threads need to access the stream table in the global memory. As a result, a lock must be added to the corresponding item of the stream table when one thread is processing the packet. The contest accessing by all means decrease the performance. And for the separated stream table, every thread uses its own stream table, and we must use more memory than the shared stream table to hold several tables to make the TCB list not too long.

So, if both high utilization and high performance are required, a new technique must be adopted. To solve this problem perfectly, a unified hash method for packet dispatching to the threads and obtaining the stream table index is applied, making all the TCBs have the same stream table index are dispatched to the same thread. Therefore, the items of the stream table need not to append locks because all the packets hashed to the special item will be processed by one special thread. In addition, if the stream table items assigned to every thread are consecutive and their size is aligned to the Cache blocks, then the Cache hit ratio will be high to improve the overall performance.

B. No-Locking Timeout

A large numbers of concurrent TCP streams are present in the network, so the states of a large number of TCBs attached to the stream table must be maintained. To release the memory space of the streams that are not active in the SRC, three submission schemas have been used: stream timeout, stream termination, and the size of packet buffered achieve a specified size.

Because the packets timed out have to be uploaded, a separated timeout thread is used to confirm whether there is any stream is time out. The timeout thread circularly obtains every item in the stream table and then gains every TCB in the link to determinate if there is a timeout. If a timeout occurs, submission the packets and deletion the TCB are conducted. The stream table and the TCBs become the critical resources and locks are required because that the packet processing threads need to process on the TCBs and their corresponding packets as same as the timeout thread does.

The lock operation should be removed as our experiences on the network device and network security devices because we have not so much time to process a packet. For example, we only have 300 ms to process a packet for a Gbps link [17]. For the multi-cored NPUs of RMI and OCTEON, they both have a fast messaging mechanism to implement the synchronization and information transformation among different threads. The messaging mechanism can be used to remove the locks by the timeout thread sending a message to the packet processing thread, and then the packet processing thread submitting the packets and deleting the TCBs.

C. Multi-channel Virtual Queue

The performance of the Packet capture is critical to the overall traffic analysis system [18], [19]; similarly, data block submission is critical to the overall system of stream reassembly. It is obvious that multi-core computers are the current dominant trend in computers; thus, how to avoid data coping and make the data block distributed to the several cores in the host evenly can bring distinct improvement to the overall performance.

Luca [16] exploits the feature of the Intel NIC, but he has overtaken that packets on different directions for one stream will be dispatched to different core (Matching Engineer), many attacking warnings will not be reported for this reason. We have ever amended this problem by allowing the driver to re-compute the hash value if the source address is bigger than destination address, and if the source address is less than destination address, hardware distributing mechanism is kept. But it impacts the performance, although it is stream based, the performance of the method is only 60% of the method [16] introduced. Furthermore, Intel NIC only has 4 fixed queues, but the latest CPU can support 8 cores, the packets in 4 queues cannot be dispatched to 8 cores.

The host creates several ringed buffers, and tells the program running on the embedded multi-core NPU the number of ringed buffers, ring descriptors, length, head and tail pointers of the ring through shared memory. NPU then calculate the corresponded queue that each stream data block will be dispatched according to the information given by the CPU.

VI. Implementation and Performance Evaluation

A. Implementation

A Stream Reassembly Card is developed using XLS416 produced by Raza Microelectronics, Inc (RMI). The RMI XLS416 is a multi-core, multi-thread MIPS64 processor with a rich set of integrated I/O. XLS 416 has 4 cores and every core has 4 threads, so the total thread number is 16. One thread (referred as timeout thread) is used to take charge of the timeout management, and the other threads (referred as packet processing threads) all execute the same routine, whose job is receiving packets, assembly, and submission, when the timeout thread find that any stream has been timed out, it will send a message to the corresponding thread to notify which stream has been timed out, then every packet processing thread circularly check if there is any timeout message after processing one packet.

XLS 416 has three frequency models: 800M, 1.0G and 1.2G; for the best of the performance, we used the XLS with 1.2G Hz. XLS 416 integrates eight Gigabit Ethernet or two Ten Gigabit Ethernet. To further save the PCB size and consider that the Ten Gigabit Ethernet may be the mainstream link of the campus network, 2 ten-Gigabit interfaces are adopted to

SRC. Our SRC has 4G DRAM with 533 MHz and 1 PCIe1.1 $\times$ 4 Bus used to connect to the host. The interface chip is VSC8486-11 that connect the fiber module and the XLS through XAUI. DIMM chips are used instead of DIMM strips, for it occupies less PCB space and the stability is better. The total chip's power consumption is under 26 watts.

In the software level, there are a stream reassembly program running on the SRC and a Driver running on the host. Program running on the SRC is bound to one Image with the RMI OS and is burned into the Flash, which is also used to boot the system. We provide an SRC_API extending from Libnids. In addition to the feature of the Libnids, our SRC_API can be used to obtain the statistics and set the number of the analyses threads running on the host, timeout of the stream, and the BlockSize. 2M space is used to share information by the CPU and NPU, and 64M byte space per capturing thread running on the CPU.

B. Evaluation

The test topology is depicted in Figure. 3. Dell PowerEdge R710 Server with an Xeon 2.13Ghz E5606 CPU, and total 16GB ECC DDR3 (4x4GB) is used to host the SRC. R710 Server has a PCIe $\times$ 8 Bus which can be used to hold the joint of the SRC. Red Hat Enterprise Server 64Bit with a 2.6.18-92.el5 kernel is used as the Operation System. An IXIA XM2 with an Xcellon-Ultra NP 10GbE Load Module is used to construct the evaluation environment. The application level test is carried out by IXIA XM2 [20].

The HTTP is used as the traffic load. Two XM2 ports are used to emulate the traffic between one server and multi-clients. To make use of the transferring bandwidth fully, 8 capture threads in the host are used. To gain the relationship between the NPU core number and stream reassembly performance, we test the performance under different core number circumstance. Since every core has 4 threads, when one core is tested, one thread is used as timeout thread and the other 3 threads are used to reorder the packets; and when two cores are tested, one thread is used as timeout thread and the other 7 threads are used to reorder the packets, and so forth. Because the traditional NIDS used Libnids [8] to conduct its stream reassembly, we tested its performance and the results are depicted in the last column of Table. I.

More cores lead to higher performance, and longer packets produce higher performance. It is also revealed that if all the cores are used, the performance is close to that of the packet capture. It means that when all the threads in the NPU are turned on to reassemble the packets, the performance is near to the PCI transferring ability, so it can be inferred that if the PCI multiplying factor is 8, the performance will be higher than the current implementation. As we know, the average packet length is between 300 and 400 bytes, so the performance of the real environment will be higher than 3Gbps. That is to say, while we formerly used three high performance server to conduct the stream reassembly, now one SRC can accomplish the same task.

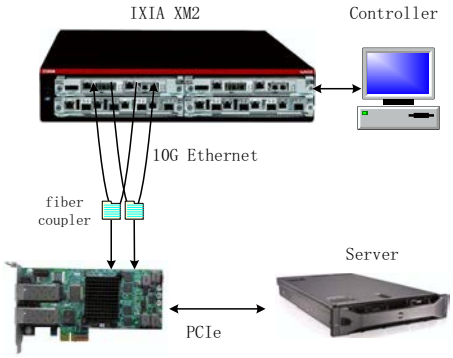


Fig. 3. Stream Reassembly Performance Test Environment.

TABLE I
THROUGHPUT OF SRC AND LIBNIDS.

Packet Length[1]	1 core	2 cores	3 cores	4 cores	Libnids
64	0.22	0.33	0.61	0.64	0.45
128	0.25	0.47	0.98	1.18	0.48
256	0.59	1.02	2.50	3.11	0.82
512	0.75	1.51	2.66	3.48	0.93
1024	1.30	2.73	3.12	3.70	0.99
1500	1.45	2.98	3.11	3.85	1.21

[1] Unit: Byte.

VII. CONCLUSION

The performance of TCP packet reassembly becomes the bottleneck as the matching performance is increasing. In this paper, a co-processing stream reassembly framework based on multi-core NPU has then been introduced as a card, so the packet capture and stream reassembly can be both solved by a card. And to heighten the performance, we brought forward Stream Table Dispatching, No-Locking Timeout, and Multi-channel Virtual Queue to improve the performance of the proposed SRC scheme. The solution adopted cannot hold much memory because the size and electricity limit, whereas the memory size is critical to the performance, we analyzed how much memory is need for a specified timeout, block size and throughput. Last, RMI XLS416 was used to implement a co-processing Stream Reassembly Card, The result showed that our scheme is about 3 times of Libnids used in the current predominant server.

VIII. ACKNOWLEDGMENT

This work has been supported by the National High-Tech Research and Development Plan of China under Grant No.2011AA01A103 .

REFERENCES

[1] N. Weaver, V. Paxson, and J. M. Gonzalez, "The shunt: an fpga-based accelerator for network intrusion prevention," in *Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays*, ser. FPGA '07. New York, USA: ACM, 2007, pp. 199–206.

[2] M. Labrecque and J. G. Steffan, "The case for hardware transactional memory in software packet processing," in *Proceedings of the 6th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, ser. ANCS '10, 2010, pp. 37–48.

[3] V. Giorgos, A. Spiros, P. Michalis, E. P. Markatos, and S. Ioannidis, "Gnort: High performance network intrusion detection using graphics processors." in *Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection.* USA: SpringerLink, 2008, pp. 116–134.

[4] G. Vasiliadis, M. Polychronakis, S. Antonatos, E. P. Markatos, and S. Ioannidis, "Regular expression matching on graphics hardware for intrusion detection," in *Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection*, ser. RAID '09, Berlin, Heidelberg, 2009, pp. 265–283.

[5] G. Vasiliadis, M. Polychronakis, and S. Ioannidis, "Midea: a multi-parallel intrusion detection architecture," in *Proceedings of the 18th ACM conference on Computer and communications security*, ser. CCS '11. New York, USA: ACM, 2011, pp. 297–308.

[6] C.-H. Lin, C.-H. Liu, and S.-C. Chang., "Accelerating regular expression matching using hierarchical parallel machines on gpu," in *IEEE Globecom 2011 proceedings*, HOUSTON, TEXAS, USA, pp. 1–5.

[7] S. Egorov and G. Savchuk, "Snortran: An optimizing compiler for snort rules," *Fidelis Security Systems*, 2002.

[8] Libnids, http://libnids.sourceforge.net/.

[9] Tcpflow, http://afflib.org/software/tcpflow.

[10] K. chan Lan and J. Heidemann., "A measurement study of correlation of Internet flow characteristics," *Computer Networks*, vol. 50, no. 1, pp. 46–62, 2006.

[11] H.-A. Kim and D. O'Hallaron, "Counting network flows in real time," in *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, vol. 7. IEEE, dec. 2003, pp. 3888–3893.

[12] G. Wagener, A. Dulaunoy, and T. Engel, "Towards an estimation of the accuracy of tcp reassembly in network forensics," in *Future Generation Communication and Networking, 2008. FGCN '08. Second International Conference on*, vol. 2. IEEE, dec. 2008, pp. 273–278.

[13] M. Zhang and J. Ju, "Space-economical reassembly for intrusion detection system." *Information and Communications Security*, pp. 393–404, 2003.

[14] S. Dharmapurikar and V. Paxson, "Robust tcp stream reassembly in the presence of adversaries," in *Proceedings of the 14th conference on USENIX Security Symposium - Volume 14*, Berkeley, CA, USA, 2005.

[15] E. M. L. Gorka Aguirre Cascallana, "Collecting packet traces at high speed," 2006.

[16] L. Deri, N. S. P. A, V. D. B. Km, and L. L. Figuretta, "Improving passive packet capture: Beyond device polling," in *Proceedings of SANE*, vol. 2004, pp. 85–93.

[17] J. V. Lunteren, T. Engbersen, and S. Member, "Fast and scalable packet classification," *IEEE Journal on Selected Areas in Communications*, vol. 21, pp. 560–571, 2003.

[18] L. Deri, "ncap: Wire-speed packet capture and transmission," in *End-to-End Monitoring Techniques and Services, 2005. Workshop on*. IEEE, 2005, pp. 47–55.

[19] M. Smith and D. Loguinov, "Enabling high-performance internet-wide measurements on windows," in *PAM*, 2010, pp. 121–130.

[20] IXIA, http://www.ixiacom.com/.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix W

US008813221B1

(12) **United States Patent**
Dubrovsky et al.

(10) **Patent No.: US 8,813,221 B1**
(45) **Date of Patent: *Aug. 19, 2014**

(54) **REASSEMBLY-FREE DEEP PACKET INSPECTION ON MULTI-CORE HARDWARE**

(75) Inventors: **Aleksandr Dubrovsky**, San Mateo, CA (US); **John E. Gmuender**, Sunnyvale, CA (US); **Huy Minh Nguyen**, Fountain Valley, CA (US); **Ilya Minkin**, Los Altos, CA (US); **Justin M. Brady**, San Jose, CA (US); **Boris Yanovsky**, Saratoga, CA (US)

(73) Assignee: **SonicWALL, Inc.**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1015 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/238,205**

(22) Filed: **Sep. 25, 2008**

(51) **Int. Cl.**
G06F 11/00 (2006.01)

(52) **U.S. Cl.**
USPC **726/22**; 726/23

(58) **Field of Classification Search**
CPC H04L 47/34; H04L 63/14; H04L 63/1416; H04L 63/145; H04L 45/00; H04I 63/1408; G06F 21/00
USPC 726/22, 23
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,796,942	A	8/1998	Esbensen	
5,945,933	A	8/1999	Kalkstein	
6,088,803	A	7/2000	Tso et al.	
6,108,782	A	8/2000	Fletcher et al.	
6,119,236	A	9/2000	Shipley	
6,178,448	B1	1/2001	Gray et al.	
6,219,706	B1	4/2001	Fan et al.	
6,449,723	B1	9/2002	Elgressy et al.	
6,851,061	B1	2/2005	Holland et al.	
7,134,143	B2	11/2006	Stellenberg et al.	
7,185,368	B2	2/2007	Copeland, III	
7,304,996	B1	12/2007	Swenson et al.	
2002/0083331	A1	6/2002	Krumel	
2003/0084328	A1	5/2003	Tarquini et al.	
2003/0110208	A1 *	6/2003	Wyschogrod et al.	709/202
2003/0145228	A1	7/2003	Suuronen et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

EP	1 122 932	8/2001
EP	1 528 743	5/2005
WO	WO 97/39399	10/1997

OTHER PUBLICATIONS

Villa (Feb. 2008). IBM Research Report: Too many words, too little time: Accelerating real-time keyword scanning with multi-core processors. Retrieved from http://domino.research.ibm.com/library/cyberdig.nsf/papers/9EB4740B4B0739CF852573F5005A6311/$File/rc24488.pdf. Retrieval data Mar. 5, 2012.*

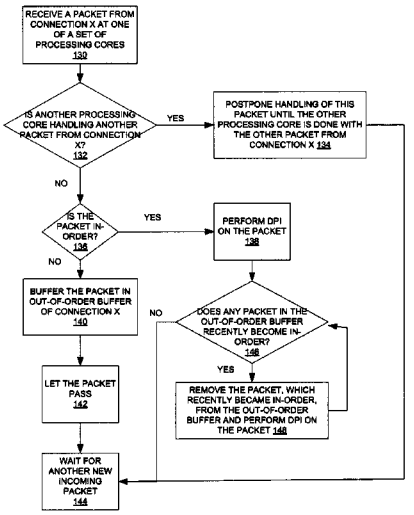
(Continued)

Primary Examiner — Brian Shaw
(74) *Attorney, Agent, or Firm* — Lewis Roca Rothgerber LLP

(57) **ABSTRACT**

Some embodiments of reassembly-free deep packet inspection (DPI) on multi-core hardware have been presented. In one embodiment, a set of packets of one or more files is received at a networked device from one or more connections. Each packet is scanned using one of a set of processing cores in the networked device without buffering the one or more files in the networked device. Furthermore, the set of processing cores may scan the packets substantially concurrently.

16 Claims, 7 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

2004/0093513	A1	5/2004	Cantrell et al.	
2004/0123155	A1	6/2004	Etoh et al.	
2004/0255163	A1	12/2004	Swimmer et al.	
2005/0120243	A1	6/2005	Palmer et al.	
2005/0216770	A1	9/2005	Rowett et al.	
2005/0262556	A1	11/2005	Waisman et al.	
2006/0020595	A1	1/2006	Norton et al.	
2006/0069787	A1	3/2006	Sinclair	
2006/0077979	A1 *	4/2006	Dubrovsky et al.	370/394
2007/0058551	A1	3/2007	Brusotti et al.	

OTHER PUBLICATIONS

"The Ultimate Internet Sharing Solution, WinProxy, User Manual," Copyright 1996-2002 Osistis Software, Inc., dated Feb. 2002 (290 pgs).

Roesch, Martin and Green, Chris, "Snort Users Manual," Snort Release 2.0.0, M. Roesch, C. Green, Copyright 1998-2003 M. Roesch, Copyright 2001-2003 C. Green, Copyright 2003 Sourcefire, Inc. dated Dec. 8, 2003 (53 pgs).

Bellovin, S., "Firewall-Friendly FTP," Network Working Group, RFC No. 1579, AT&T Bell Laboratories, Feb. 1994 , http://www.ietf.org/rfc1579.txt?number=1579, downloaded Jul. 15, 2002, 4 pages.

European Search Report, Application No. EP 04 02 5579, May 23, 2005, 3 pages.

Office Action for U.S. Appl. No. 10/697,846 mailed Jan. 5, 2007, 16 pages.

Kruegal, Christopher, et al. "Using Decision Trees to Improve Signature-Based Intrusion Detection", Sep. 8, 2003, RAID 2003: recent Advance in Intrusion Detection, 20 pages.

Branch, Joel, et al., "Denial of Service Intrusion Detection Using Time Dependent Deterministic Finite Automata", RPI Graduate Research Conference 2002, Oct. 17, 2002, 7 pages.

Juniper Networks, "Attack Prevention," www.juniper.net/products/intrusion/prevention.html, downloaded Jun. 11, 2004, 2 pages.

Juniper Networks, "Attack Detection," www.juniper.net/products/intrusion/detection.html, downloaded Jun. 11, 2004, 7 pages.

Juniper Networks, "Intrusion Detection and Prevention," www.juniper.net/products/intrusion/downloaded Jun. 11, 2004, 2 pages.

Juniper Networks, "Architecture," www.juniper.net/products/intrusion/architecture.html, downloaded Jun. 11, 2004, 3 pages.

Juniper Networks, "Juniper Networks NetScreen-IDP 10/100/500/1000," Intrusion Detection and Prevention, Spec Sheet, Apr. 2004, 2 pages.

Roberts, Paul, "NetScreen Announces Deep Inspection Firewall," IDG News Service, Oct. 20, 2003, http://www.nwfusion.com/news/2003/1020netscannou.html, downloaded Jun. 11, 2004, 5 pages.

Snort.org, "The Open Source Network Intrusion Detection System", www.snort.org/about.html, 2 pages.

Blyth, Andrew, "Detecting Intrusion", School of Computing, University of Glamorgan, 14 pages.

Office Action mailed Mar. 1, 2010 for U.S. Appl. No. 11/112,252, filed Apr. 21, 2005., 40 pages.

Final Office Action mailed Oct. 19, 2009 for U.S. Appl. No. 11/112,252, filed Apr. 21, 2005., 32 pages.

Office Action mailed Mar. 31, 2009 for U.S. Appl. No. 11/112,252, filed Apr. 21, 2005., 35 pages.

Office Action mailed Apr. 29, 2008 of U.S. Appl. No. 11/112,252, filed Apr. 21, 2005. 25 pages.

Office Action mailed Nov. 14, 2008 of U.S. Appl. No. 11/112,252, filed Apr. 21, 2005. 26 pages.

Office Action mailed Oct. 2, 2007 of U.S. Appl. No. 10/964,871, filed Oct. 13, 2004. 19 pages.

Final Office Action mailed Mar. 20, 2008 of U.S. Appl. No. 10/964,871, Oct. 13, 2004. 19 pages.

Office Action mailed Jul. 16, 2008 of U.S. Appl. No. 10/964,871, Oct. 13, 2004. 21 pages.

Office Action mailed Jan. 9, 2009 of U.S. Appl. No. 10/964,871, Oct. 13, 2004. 21 pages.

"SonicWALL Content Filtering Service," Comprehensive Internet Security™, © 2005, 2pp.

SonicW ALL Internet Security Appliances, "Content Security Manager Integrated Solutions Guide", Version 3.0, © 2007, 160 pp.

SonicW ALL Internet Security Appliances, "SonicOS 3.8 Standard Administrator's Guide", © 2007, 362 pp.

"SonicOS Standard 3.8.0.2 Release Notes, SonicWALL Secure Anti-Virus Router 80 Series," SonicW ALL, Inc., Software Release: Apr. II, 2007, 13 pp.

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Unified Threat Management, Intelligent Real-time Protection, © 2005 , 2 pp.

"SonicWALL Endpoint Security: Anti-Virus, Automated and Enforced Anti-Virus and Anti-Spyware Protection," © 2007, Mar. 2007, 2 pp.

"SonicWaLL Content Security Manager Series, Easy-to-use, Affordable, Content Security and Internet Threat Protection," © 2006, Dec. 2006, 4 pp.

"SonicWALL Complete Anti-Virus, Automated and Enforced Anti-Virus Protection," © 2005, 2 pp.

Aggarwal, N., "Improving the Efficiency of Network Intrusion Detection Systems", Indian Institue of Technology, May 3, 2006, pp. 1-40.

Van Engelen, R., "Constucting Finite State Automata for High-Performance XML Web Services," International Symposium on Web Services and Applications, 2004, pp. 1-7.

Lucas, Simon M., et al., "Learning Deterministic Finite Automata with a Smart State Labeling Evolutionary Algorithm," IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 27, No. 7, Jul. 2005, pp. 1063-1074.

Office Action mailed Jul. 7, 2010 of U.S. Appl. No. 11/778,546, Jul. 16, 2007. 15 pages.

Office Action mailed May 14, 2009 of U.S. Appl. No. 11/772,723, Jul. 2, 2007. 7 pages.

Office Action mailed Oct. 23, 2009 of U.S. Appl. No. 11/772,723, Jul. 2, 2007. 8 pages.

* cited by examiner

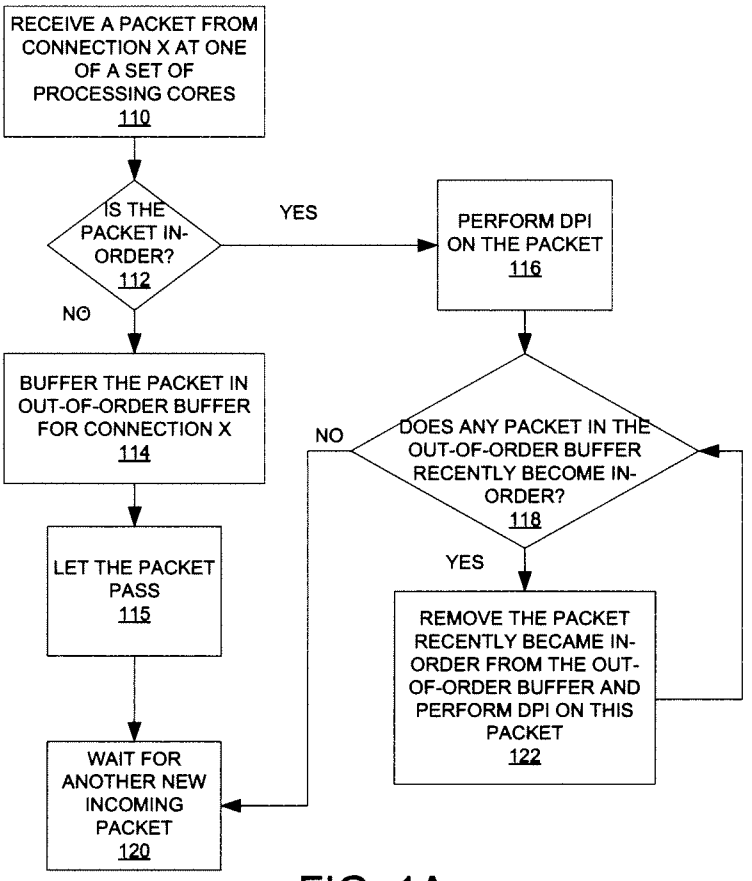

RECEIVE A PACKET FROM CONNECTION X AT ONE OF A SET OF PROCESSING CORES
110
IS THE PACKET IN-ORDER?
112
YES
NO
PERFORM DPI ON THE PACKET
116
BUFFER THE PACKET IN OUT-OF-ORDER BUFFER FOR CONNECTION X
114
DOES ANY PACKET IN THE OUT-OF-ORDER BUFFER RECENTLY BECOME IN-ORDER?
118
NO
YES
LET THE PACKET PASS
115
REMOVE THE PACKET RECENTLY BECAME IN-ORDER FROM THE OUT-OF-ORDER BUFFER AND PERFORM DPI ON THIS PACKET
122
WAIT FOR ANOTHER NEW INCOMING PACKET
120

FIG. 1A

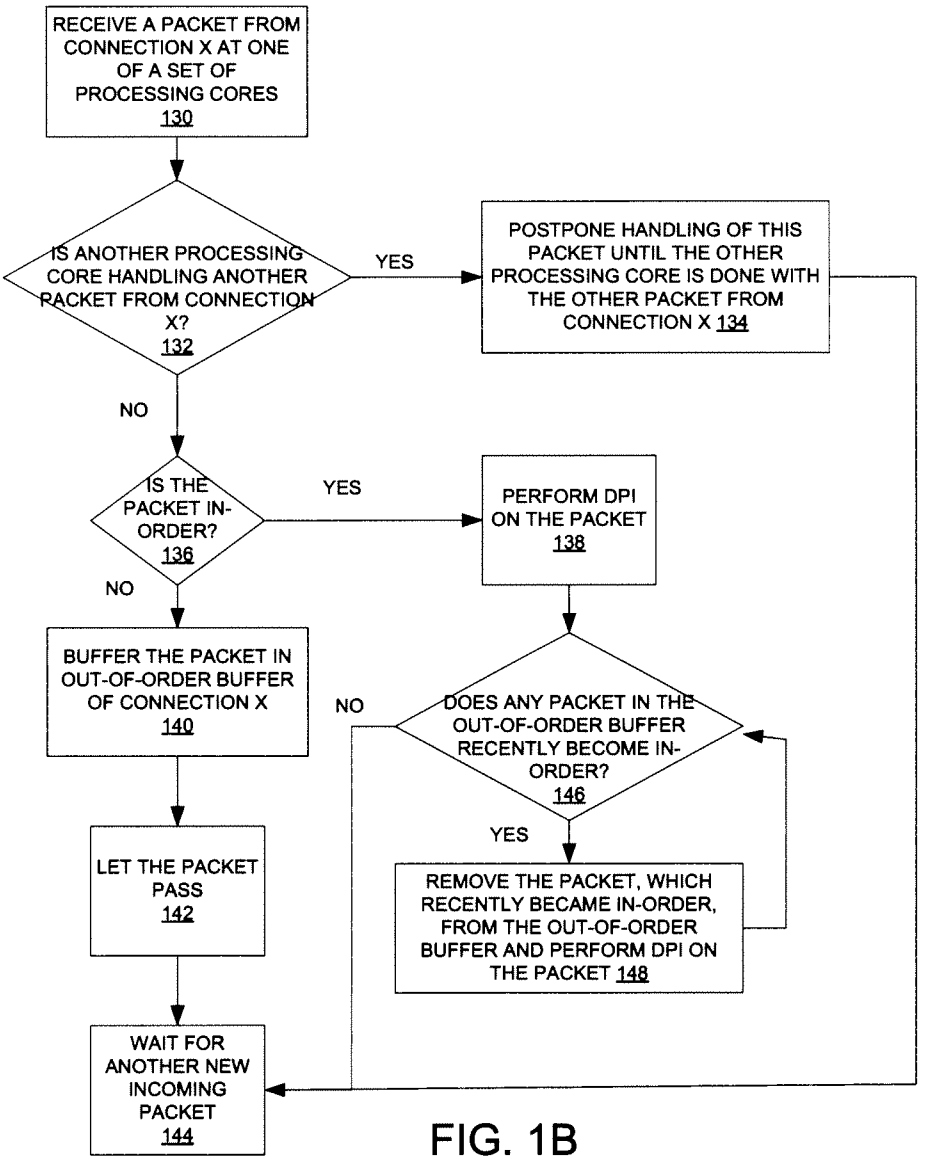

RECEIVE A PACKET FROM CONNECTION X AT ONE OF A SET OF PROCESSING CORES 130
IS ANOTHER PROCESSING CORE HANDLING ANOTHER PACKET FROM CONNECTION X? 132
YES
POSTPONE HANDLING OF THIS PACKET UNTIL THE OTHER PROCESSING CORE IS DONE WITH THE OTHER PACKET FROM CONNECTION X 134
NO
IS THE PACKET IN-ORDER? 136
YES
PERFORM DPI ON THE PACKET 138
NO
BUFFER THE PACKET IN OUT-OF-ORDER BUFFER OF CONNECTION X 140
NO
DOES ANY PACKET IN THE OUT-OF-ORDER BUFFER RECENTLY BECOME IN-ORDER? 146
YES
REMOVE THE PACKET, WHICH RECENTLY BECAME IN-ORDER, FROM THE OUT-OF-ORDER BUFFER AND PERFORM DPI ON THE PACKET 148
LET THE PACKET PASS 142
WAIT FOR ANOTHER NEW INCOMING PACKET 144

FIG. 1B

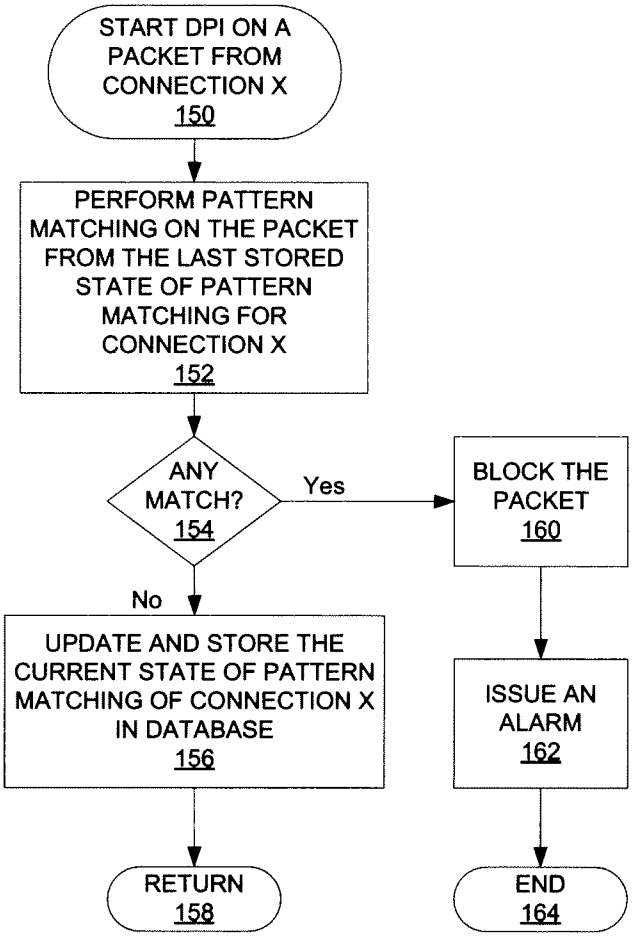

START DPI ON A PACKET FROM CONNECTION X
150
PERFORM PATTERN MATCHING ON THE PACKET FROM THE LAST STORED STATE OF PATTERN MATCHING FOR CONNECTION X
152
ANY MATCH?
154
Yes
BLOCK THE PACKET
160
No
UPDATE AND STORE THE CURRENT STATE OF PATTERN MATCHING OF CONNECTION X IN DATABASE
156
ISSUE AN ALARM
162
RETURN
158
END
164

Figure 1C

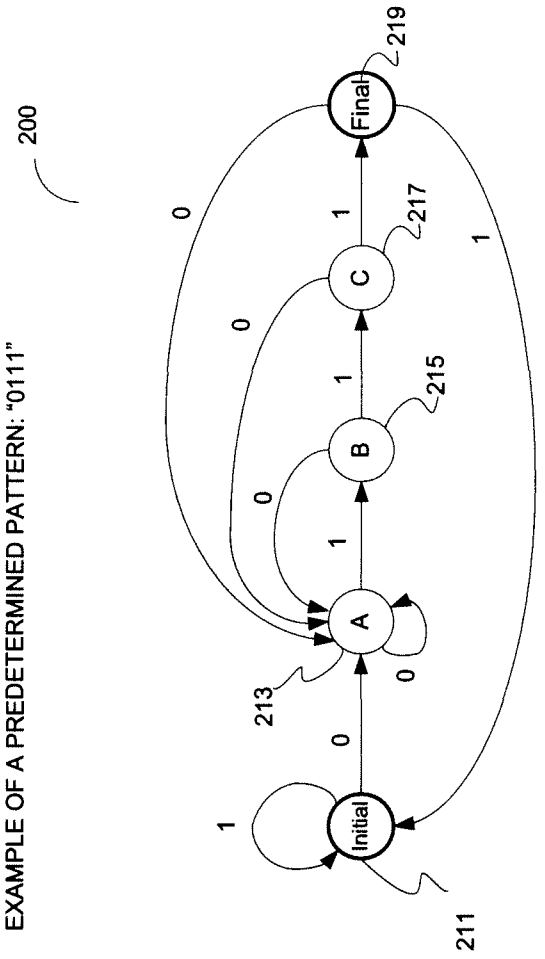

200
EXAMPLE OF A PREDETERMINED PATTERN: "0111"
Initial
A
B
C
Final
211
213
215
217
219
0
1
0
1
0
1
0
1
0
1

Figure 2

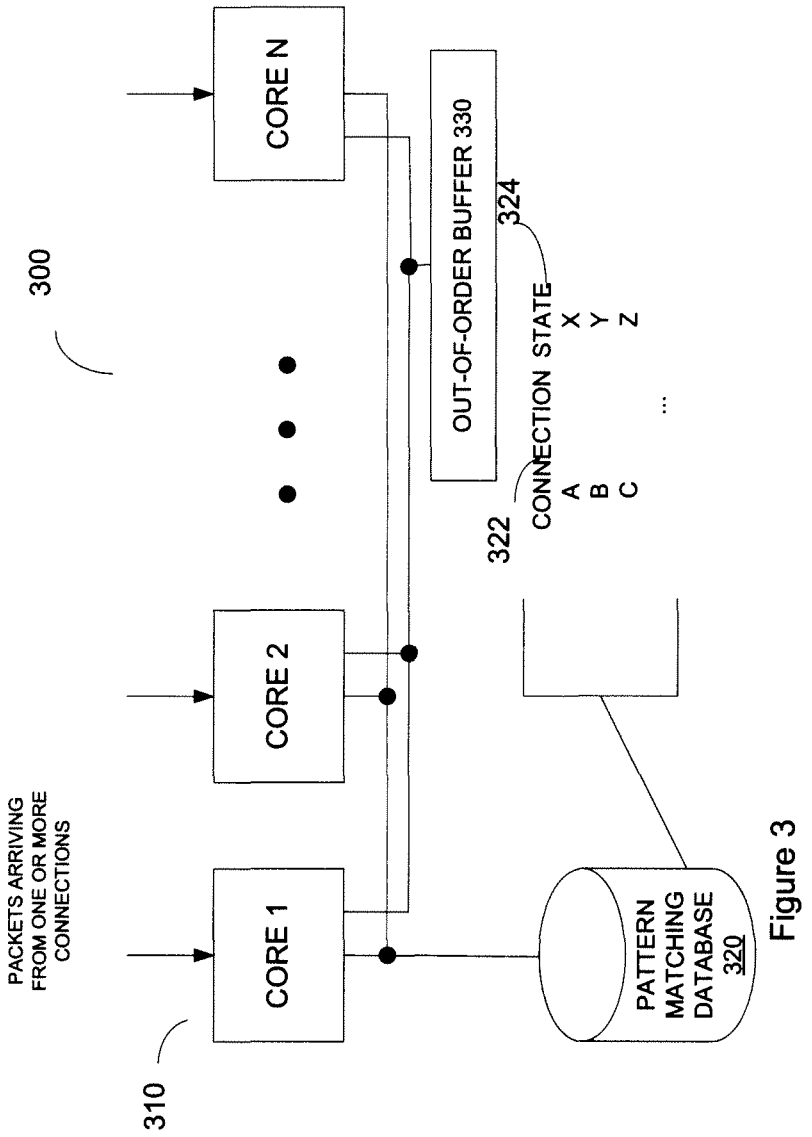

300
CORE N
CORE 2
CORE 1
310
PACKETS ARRIVING FROM ONE OR MORE CONNECTIONS
OUT-OF-ORDER BUFFER 330
324
322
CONNECTION STATE
X
Y
Z
A
B
C
...
PATTERN MATCHING DATABASE 320

Figure 3

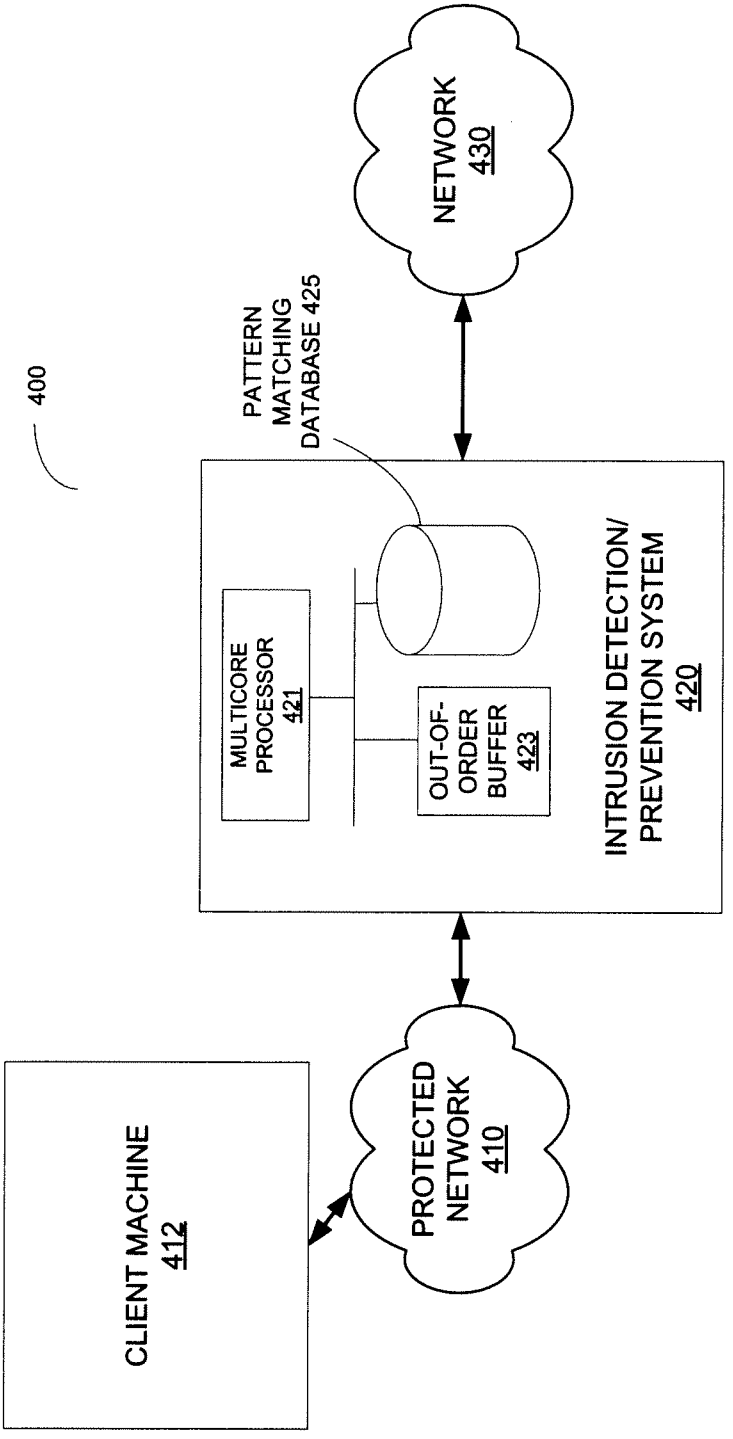

400
NETWORK
430
PATTERN
MATCHING
DATABASE 425
MULTICORE
PROCESSOR
421
OUT-OF-
ORDER
BUFFER
423
INTRUSION DETECTION/
PREVENTION SYSTEM
420
PROTECTED
NETWORK
410
CLIENT MACHINE
412

Figure 4

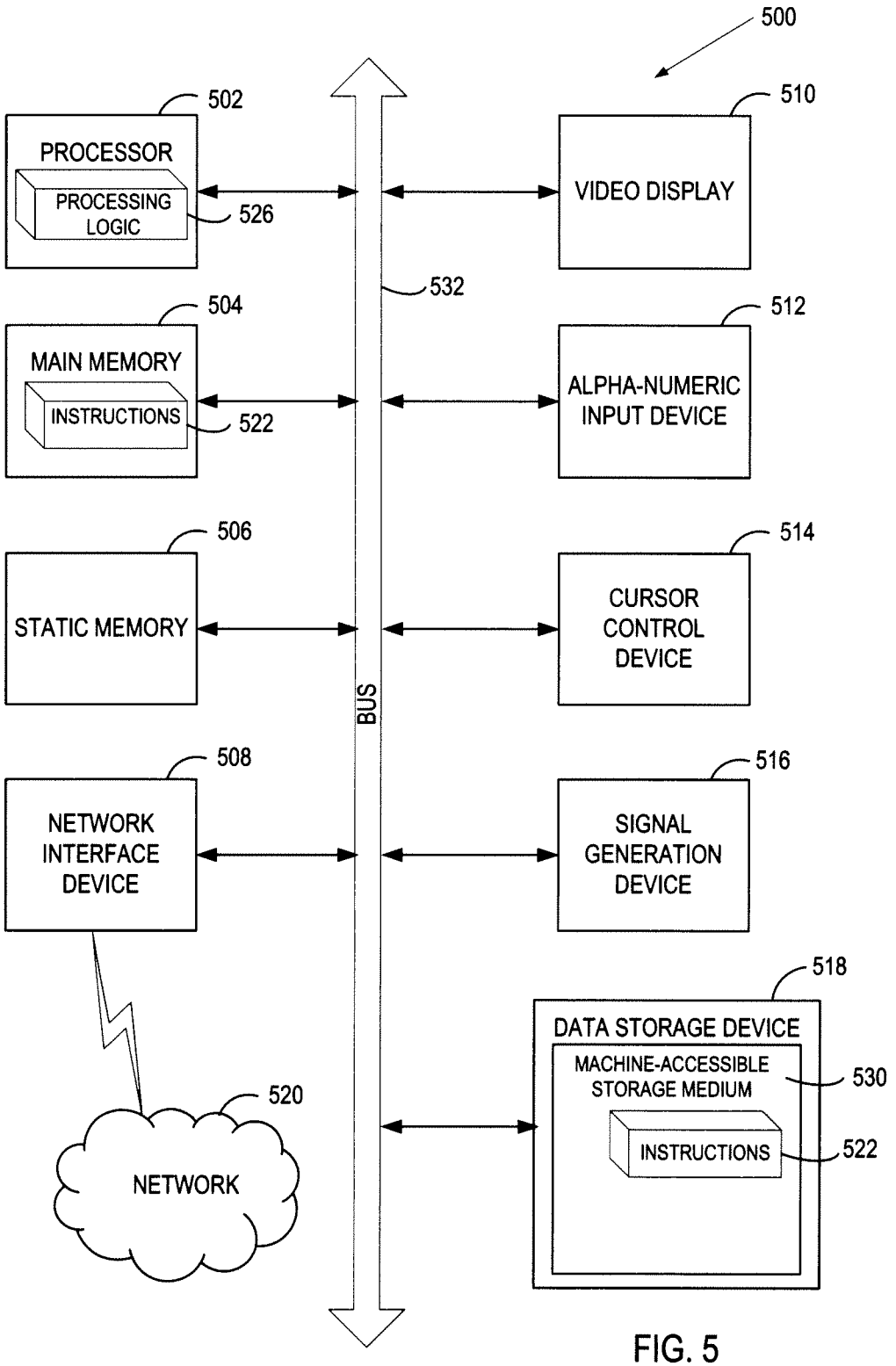

500
502
PROCESSOR
PROCESSING LOGIC
526
504
MAIN MEMORY
INSTRUCTIONS
522
506
STATIC MEMORY
508
NETWORK INTERFACE DEVICE
520
NETWORK
BUS
532
510
VIDEO DISPLAY
512
ALPHA-NUMERIC INPUT DEVICE
514
CURSOR CONTROL DEVICE
516
SIGNAL GENERATION DEVICE
518
DATA STORAGE DEVICE
MACHINE-ACCESSIBLE STORAGE MEDIUM
530
INSTRUCTIONS
522

FIG. 5

REASSEMBLY-FREE DEEP PACKET INSPECTION ON MULTI-CORE HARDWARE

TECHNICAL FIELD

The present invention relates to intrusion detection and prevention in a networked system, and more particularly, to performing multiple packet payloads analysis on multi-core hardware.

BACKGROUND

Today, in many security products, scanning by pattern matching is used to prevent many types of security attacks. For example, some existing desktop virus scanning may include scanning files against certain recognizable patterns. These files may come from mail attachments or website downloads. These desktop applications are simpler in that by the time the pattern matching is performed, the input has been all accumulated in the correct order. The situation is more complicated for gateway products, such as firewalls, attempting to match patterns for other purposes. Some of these products scan for patterns over Transport Control Protocol (TCP) packets. Since TCP usually breaks down application data into chunks called TCP segments, the full pattern may reside in several TCP segments. One conventional approach is to reassemble all TCP packets together into one large chunk and perform pattern matching on this chunk, similar to scanning files. The disadvantage of this approach is that this approach requires processing to reassemble, and it further requires memory to buffer the intermediate result before pattern matching can take place.

To further complicate the problem, many security attacks exhibit more than one pattern, and thus, multiple pattern matching has to be performed in order to successfully screen out these attacks. Such a collection of patterns is called a signature. For example, an attack signature may contain a recognizable header and a particular phrase in the body. To detect such an attack, the detection mechanism has to match all the patterns in the signature. If only part of the signature is matched, false positives may occur. As such, the term "attack pattern" is used to refer to a single pattern or a signature.

When such attacks are transported over TCP, the contents, and therefore the recognizable patterns, may exist in different TCP segments. In fact, even a single pattern is often split over several segments. Therefore, two problems have to be solved at the same time. On one hand, the detection mechanism has to scan each pattern across multiple segments, and on the other hand, the detection mechanism also has to scan across patterns. One existing approach is to reassemble all packets and scan for each pattern in sequence. This approach is inefficient in terms of processing time and memory usage because scanning cannot start until all packets are received and reassembled and extra memory is needed to store the packets received.

Another problem in pattern matching is that the packets may arrive out of order. Again, using TCP as an example, the application data is broken into what TCP considers the best sized chunks to send, called a TCP segment or a TCP packet. When TCP sends a segment, it maintains a timer and waits for the other end to acknowledge the receipt of the segment. The acknowledgement is commonly called an ACK. If an ACK is not received for a particular segment within a predetermined period of time, the segment is retransmitted. Since the IP layer transmits the TCP segments as IP datagrams and the IP datagrams can arrive out of order, the TCP segments can arrive out of order as well. Currently, one receiver of the TCP segments reassembles the data so that the application layer receives data in the correct order.

An existing Intrusion Detection/Prevention System (IPS) typically resides between the two ends of TCP communication, inspecting the packets as the packets arrive at the IPS. The IPS looks for predetermined patterns in the payloads of the packets. These patterns are typically application layer patterns. For example, the pattern might be to look for the word "windows." However, the word may be broken into two TCP segments, e.g., "win" in one segment and "dows" in another segment. If these two segments arrive in the correct order, then IPS can detect the word. However, if the segments arrive out of order, which happens relatively often, then the IPS may first receive the segment containing "dows", and have to hold this segment and wait for the other segment. A typical approach is for the IPS to force the sender to retransmit all the segments from the last missing one, hoping that the segments may arrive in order the second time. One disadvantage of this approach is the additional traffic in between and the additional processing on both ends of the TCP communication.

To take advantage of the introduction of multi-core processors (e.g., Intel® Core™2 Quad Processors from Intel Corporation of Santa Clara, Calif.), some conventional ISPs use multi-core processors to scan incoming segments to speed up the process. In general, each multi-core processor has two or more processing cores. According to one conventional approach, one of the processing cores is used to completely reassemble the file while the remaining processing cores perform scanning or pattern matching in the background after the file has been completely reassembled. However, this approach does not scale in terms of having enough memory to store all files. Also, background scanning by multiple processing cores is less efficient due to extra memory copying overhead and extra scheduling processing overhead.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which:

FIG. **1**A illustrates one embodiment of a method to perform multiple packet analysis on multi-core hardware.

FIG. **1**B illustrates an alternate embodiment of a method to perform multiple packet analysis on multi-core hardware.

FIG. **1**C illustrates one embodiment of a method to perform deep packet inspection.

FIG. **2** illustrates an exemplary Deterministic Finite Automaton (DFA) according to one embodiment of the invention.

FIG. **3** illustrates a functional block diagram of one embodiment of multi-core hardware usable to perform multiple packet analysis.

FIG. **4** illustrates one embodiment of a system in which embodiments of the present invention may be implemented.

FIG. **5** illustrates a block diagram of an exemplary computer system, in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION

Described herein are some embodiments of reassembly-free deep packet inspection on multi-core hardware. In one embodiment, a set of packets of one or more files is received at a networked device from one or more connections. Each packet is scanned using one of a set of processing cores in the

networked device without buffering the one or more files in the networked device. Furthermore, the set of processing cores may scan the packets substantially concurrently.

In the following description, numerous details are set forth. It will be apparent, however, to one skilled in the art, that the present invention may be practiced without these specific details. In some instances, well-known structures and devices are shown in block diagram form, rather than in detail, in order to avoid obscuring the present invention.

Some portions of the detailed descriptions below are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present invention also relates to apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer-readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, flash memory, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein.

FIG. **1**A illustrates one embodiment of a method to perform multiple packet analysis on multi-core hardware, where

multiple processing cores of a set of processing cores are allowed to handle packets from the same connection (hereinafter, "connection X"). In some embodiments, the set of processing cores includes processing cores of a multi-core processor. The method may be performed by processing logic that may comprise hardware (e.g., circuitry, dedicated logic, programmable logic, processing cores, etc.), software (such as instructions run on a processing core), firmware, or a combination thereof.

Initially, one of a set of processing cores receives a packet from connection X (processing block **110**). The packet is part of a file, which may be re-constructed by re-assembling the packet with other packets of the file. Then the processing core determines if the packet is in-order (processing block **112**). For example, the processing core may check a sequence number in a header of the packet against a next packet sequence number of connection X, which may be stored in a database commonly accessible by the processing cores.

If the packet is not in-order, i.e., out-of-order, then the processing core may buffer the packet in an out-of-order buffer associated with connection X (processing block **114**). The processing core may allow the packet to pass (processing block **115**). Then the processing core waits for another new incoming packet (processing block **120**).

If the packet is in-order, then the processing core performs deep packet inspection (DPI) on the packet (processing block **116**). Details of some embodiments of DPI are discussed below. Then the processing core checks if there is any packet in the out-of-order buffer associated with connection X that recently became in-order (processing block **118**). If there is no packet in the out-of-order buffer associated with connection X that is next in sequence (in-order), the processing core transitions to processing block **120** to wait for another new incoming packet. Otherwise, if there is a packet in the out-of-order buffer associated with connection X that is now in-order, then the processing core removes this packet and performs DPI on this packet (processing block **122**). When the processing core completes DPI on this packet, the processing core returns to processing block **118** to check if there is another packet in the out-of-order buffer associated with connection X that is in-order.

Note that the incoming packets are scanned without buffering the file for reassembly because the packets can be inspected for the predetermined pattern without being reassembled into the file. Thus, the above technique is well suited for IPSs that have limited capacity for buffering or storage. Furthermore, the above technique allows the set of processing cores to scan incoming packets substantially concurrently. Therefore, the speed of the scanning may be improved over conventional approaches.

FIG. **1**B illustrates one embodiment of a method to perform multiple payload analysis on multi-core hardware, where only a single core in a set of processing cores is allowed to handle packets from a particular connection (hereinafter, "connection X") at a time. In some embodiments, the set of processing cores includes processing cores of a multi-core processor. The method may be performed by processing logic that may comprise hardware (e.g., circuitry, dedicated logic, programmable logic, processing cores, etc.), software (such as instructions run on a processing core), firmware, or a combination thereof.

Initially, one processing core of the set of processing cores receives a packet from connection X (processing block **130**). Then the processing core checks if there is another processing core in the set of processing cores handling another packet from connection X (processing block **132**). If there is another processing core handling another packet from connection X

currently, then the processing core postpones handling of this packet until the other processing core is done with the other packet from connection X (processing block **134**). The processing core may transition to processing block **144** to wait for another new incoming packet.

If the processing core determines that there is no other processing core in the set of processing cores handling another packet from connection X, then the processing core checks if this packet is in-order (processing block **136**). If this packet is not in-order, i.e., out-of-order, then the processing core buffers this packet in an out-of-order buffer associated with connection X (processing block **140**). The processing core may allow this packet to pass (processing block **142**). Then the processing core waits for another new incoming packet (processing block **144**).

If the processing core determines that this packet is in-order, then the processing core performs DPI on this packet (processing block **138**). Details of some embodiments of DPI are discussed below. After performing DPI on the packet, the processing core checks if there is any packet in the out-of-order buffer associated with connection X, which is now in-order (processing block **146**). If there is a packet in the out-of-order buffer that is now in-order, then the processing core removes the packet that recently became in-order from the out-of-order buffer and performs DPI on this packet (processing block **148**). Then the processing core returns to processing block **146** to repeat the above process. If there is no packet in the out-of-order buffer that is in-order, then the processing core transitions to processing block **144** to wait for another new incoming packet.

Like the technique illustrated in FIG. **1**A, the technique illustrated in FIG. **1**B also allows scanning of the incoming packets without buffering the file for reassembly because the packets can be scanned for the predetermined pattern, without reassembling the packets into the file, by DPI.

FIG. **1**C illustrates one embodiment of a method to perform deep packet inspection (DPI) using one of a set of processing cores. In some embodiments, the set of processing cores includes processing cores of a multi-core processor. The method may be performed by processing logic that may comprise hardware (e.g., circuitry, dedicated logic, programmable logic, processing cores, etc.), software (such as instructions run on a processing core), firmware, or a combination thereof.

Initially, the processing core starts DPI on a packet from connection X at block **150**. This packet is hereinafter referred to as the current packet. The processing core performs pattern matching on the current packet from the last stored state of pattern matching for connection X (processing block **152**). Specifically, the processing core is trying to look for a predetermined pattern or signature in the incoming packets, which may be associated with a computer virus or malicious code. By identifying such pattern or signature in the incoming packets and blocking at least one of the packets containing part of the predetermined pattern or signature, the set of processing cores can protect a system from computer viral attack. In some embodiments, the last stored state of pattern matching for connection X is stored in a database commonly accessible by the set of processing cores. As such, each of the set of processing cores can handle packets from connection X, even though some of the packets may be inspected by different processing cores.

In some embodiments, if there is a match between a predetermined pattern and the data pattern in the incoming packets inspected so far (which includes the current packet), then the processing core blocks the current packet (processing block **160**). Then the processing core may issue an alarm to warn a system administrator of detection of potentially malicious code or virus in the incoming packets (processing block **162**), and the process ends at block **164**.

If there is no match between the predetermined pattern and the data pattern in the incoming packets inspected so far, then the processing core may update and store the current state of pattern matching of connection X in the database (processing block **156**). The method then ends at block **158**.

In some embodiments, pattern matching performed in DPI is accomplished using Deterministic Finite Automaton (DFA). An exemplary DFA is shown in FIG. **2** to illustrate the concept.

FIG. **2** illustrates an exemplary DFA according to one embodiment of the invention. In this example, an IPS is programmed to detect and to prevent a pattern of "0111" to pass through. The DFA **200** shown in FIG. **2** corresponds to this pattern. A set of processing cores may use the DFA **200** to perform pattern matching on a number of packets to determine whether the packets contain the pattern "0111". Furthermore, to simplify the illustration, it is assumed in this example that each packet contains only one digit. However, it should be appreciated that the concept is applicable to scenarios where a packet contains more than one digits and/or alphabetic letters.

Referring to FIG. **2**, the DFA **200** includes 5 states **211**-**219**. The states **211**-**219** in the DFA **200** may be referred to as nodes. A processing core in the set of processing cores begins pattern matching at the initial state **211**. If a packet received contains a "1", the processing core remains in the initial state **211**. If the packet contains a "0", which corresponds to the first digit in the predetermined pattern, the processing core transitions to the A state **213**.

If the processing core receives a "0" subsequently, the processing core remains in the A state **213**. If the processing core receives a "1", which corresponds to the second digit in the predetermined pattern, then the processing core transitions into the B state **215**. From the B state **215**, the processing core may transition back to the A state **213** if the next packet received contains a "0". If the next packet received contains a "1", which corresponds to the third digit in the predetermined pattern, then the processing core transitions to the C state **217**. However, note that another processing core in the set of processing cores may receive and process the next packet in some embodiments.

From the C state **217**, the processing core may transition back to the A state **213** if the next packet received contains a "0". If the next packet received contains a "1", which corresponds to the last digit in the predetermined pattern, then the processing core transitions to the final state **219**. When the processing core reaches the final state **219**, the processing core knows that the packets received so far contain the predetermined pattern. Hence, the processing core may perform the appropriate operations in response to receiving the predetermined pattern, such as blocking the packet of the predetermined pattern last received and issuing an alarm to alert system administrators. To keep track of which state of the DFA is in currently, the processing core stores the current state of the DFA in a database commonly accessible by the set of processing cores. As such, another processing core may continue pattern matching on the next packet from the current state if the other processing core receives the next packet. Furthermore, the current state of the DFA may be associated with a connection from which the packet is received so that the set of processing cores may inspect packets from multiple connections using the information from the database.

One advantage of using the DFA to perform pattern matching on packets is to eliminate the need to reassemble the

packets because the processing cores can walk through the DFA as each packet is received and examined. Because a pattern is typically broken up into a number of segments and each segment is transmitted using a packet, it is necessary to inspect multiple packets in order to identify the pattern. Using the DFA, the processing cores may not have to reassemble the packets in order to find out what the pattern contained in the packets is in order to match the pattern against a predetermined pattern. The processing cores may perform pattern matching on a packet-by-packet basis as each of the packets is received without reassembling the packets by walking through the DFA. If a processing core reaches a final state, there is a match between the pattern contained in the packets received so far and the predetermined pattern. There is no need to store the packets for reassembling the packets. Instead, the processing cores may simply store the current state of the DFA in a database commonly accessible by the processing cores.

The concept described above may be expanded to signature detection. A signature is a collection of multiple patterns. To keep track of which pattern within a signature is being matched, processing logic may use a tree structure, where each node within the tree structure corresponds to a pattern and each pattern is represented using a DFA. Alternatively, a single DFA may represent multiple patterns.

FIG. **3** illustrates a functional block diagram of one embodiment of multi-core hardware usable to perform multiple payload analysis in an IPS. The IPS may be implemented within a set-top box coupled to a protected network. The multi-core hardware **300** includes a set of processing cores **310**, a pattern matching database **320**, and an out-of-order buffer **330**. In some embodiments, the set of processing cores **310** includes processing cores in a multi-core processor. The processing cores **310** are communicably coupled to the database **320** so that each of the processing cores **310** may retrieve and update information in the database **320**. Likewise, the processing cores **310** are also communicably coupled to the out-of-order buffer **330** so that each of the processing cores **310** may access the out-of-order buffer **330**.

In some embodiments, the processing cores **310** receive packets from one or more connections. To prevent harmful virus or malicious code from reaching the protected network, the processing cores **310** performs reassembly-free DPI on the packets. When one of the processing cores **310** receives a packet, the processing core may determine if the packet is in-order or out-of-order. An out-of-order packet may be temporarily stored in the out-of-order buffer **330** and be associated with the connection from which the out-of-order packet is received. In-order packets are examined by the processing cores **310** and are allowed to pass to the protected network if no pattern of harmful virus or malicious code is detected. The processing cores **310** update and store the current pattern matching state of each connection in the database **320**. As such, any one of the processing cores **310** can continue with the on-going pattern matching from the current state of a connection that sends the current packet. In some embodiments, the database **320** includes a relational database that stores the current pattern matching states **324** with their corresponding connections **322** as shown in FIG. **2**. Details of some embodiments of the method to perform reassembly-free DPI have been discussed above.

FIG. **4** illustrates one embodiment of a system in which embodiments of the present invention may be implemented. The system **400** includes a client machine **412** within a protected network **410**, an IPS **420**, and a network **430**. The protected network **410** is communicably coupled to the network **430** via the IPS **420**. Thus, packets transmitting between the protected network **410** and the network **430** have to pass through the IPS **420**. In some embodiments, there may be more than one client machines coupled to the protected network **410**. The network **430** may include a variety of networks, such as local area network (LAN), wide area network (WAN), etc. Furthermore, the network **430** may be publicly accessible, and therefore, computer virus and malicious code targeting the protected network **410** may be sent from the network **430**. As such, the IPS **420** scans the incoming packets to prevent computer virus and malicious code from entering the protected network **410**.

In some embodiments, the IPS **420** includes a multi-core processor **421**, an out-of-order buffer **423**, and a pattern matching database **425**. The multi-core processor **421** includes a set of processing cores, such as the processing cores **310** shown in FIG. **3**.

In some embodiments, each of the processing cores receives packets from the network **430** through different connections. Furthermore, the packets may arrive out-of-order, and if so, the out-of-order packets may be temporarily stored in the out-of-order buffer **423** to be inspected later. The processing cores of the multi-core processor **421** perform DPI on the in-order packets and store the current pattern matching states of the connections in the pattern matching database **425**. If a pattern associated with computer virus or malicious code is identified in the incoming packets inspected so far, the multi-core processor **421** blocks the packet currently being inspected and may further issue a warning to a system administrator. If no pattern associated with computer virus or malicious code is identified in the incoming packets inspected so far, then the multi-core processor **421** allows the packet currently being inspected to pass to the protected network **410**, which may be further transmitted to the client machine **412**. By blocking the packet currently being inspected if the pattern is identified in the packets received so far, the computer virus or malicious code cannot be completely passed into the protected network **410**, and hence, the computer virus or malicious code cannot be completely reassembled on the client machine **412**. The incomplete computer virus or malicious code typically cannot harm the client machine **412** coupled thereto. Details of some embodiments of a method to perform reassembly-free DPI have been discussed above.

FIG. **5** illustrates a diagrammatic representation of a machine in the exemplary form of a computer system **500** within which a set of instructions, for causing the machine to perform any one or more of the methodologies discussed herein, may be executed. In alternative embodiments, the machine may be connected (e.g., networked) to other machines in a LAN, an intranet, an extranet, and/or the Internet. The machine may operate in the capacity of a server or a client machine in client-server network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The machine may be a personal computer (PC), a tablet PC, a set-top box (STB), a Personal Digital Assistant (PDA), a cellular telephone, a web appliance, a server, a network router, a switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

The exemplary computer system **500** includes a processing device **502**, a main memory **504** (e.g., read-only memory (ROM), flash memory, dynamic random access memory (DRAM) such as synchronous DRAM (SDRAM) or Rambus

DRAM (RDRAM), etc.), a static memory **506** (e.g., flash memory, static random access memory (SRAM), etc.), and a data storage device **518**, which communicate with each other via a bus **532**.

Processing device **502** represents one or more general-purpose processing devices such as a microprocessor, a central processing unit, or the like. More particularly, the processing device may be complex instruction set computing (CISC) microprocessor, reduced instruction set computing (RISC) microprocessor, very long instruction word (VLIW) microprocessor, or processor implementing other instruction sets, or processors implementing a combination of instruction sets. Processing device **502** may also be one or more special-purpose processing devices such as an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), a digital signal processor (DSP), network processor, or the like. The processing device **502** is configured to execute the processing logic **526** for performing the operations and steps discussed herein.

The computer system **500** may further include a network interface device **508**. The computer system **500** also may include a video display unit **510** (e.g., a liquid crystal display (LCD) or a cathode ray tube (CRT)), an alphanumeric input device **512** (e.g., a keyboard), a cursor control device **514** (e.g., a mouse), and a signal generation device **516** (e.g., a speaker).

The data storage device **518** may include a machine-accessible storage medium **530** (also known as a machine-readable storage medium or a computer-readable medium) on which is stored one or more sets of instructions (e.g., software **522**) embodying any one or more of the methodologies or functions described herein. The software **522** may also reside, completely or at least partially, within the main memory **404** and/or within the processing device **502** during execution thereof by the computer system **500**, the main memory **504** and the processing device **502** also constituting machine-accessible storage media. The software **522** may further be transmitted or received over a network **520** via the network interface device **508**.

While the machine-accessible storage medium **530** is shown in an exemplary embodiment to be a single medium, the term "machine-accessible storage medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "machine-accessible storage medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by the machine and that cause the machine to perform any one or more of the methodologies of the present invention. The term "machine-accessible storage medium" shall accordingly be taken to include, but not be limited to, solid-state memories, optical and magnetic media, etc. In some embodiments, machine-accessible storage medium may also be referred to as computer-readable storage medium.

Thus, some embodiments of reassembly-free DPI on multi-core hardware have been described. It is to be understood that the above description is intended to be illustrative, and not restrictive. Many other embodiments will be apparent to those of skill in the art upon reading and understanding the above description. The scope of the invention should, therefore, be determined with reference to the appended claims, along with the full scope of equivalents to which such claims are entitled.

What is claimed is:

1. A method comprising:

receiving a plurality of packets of one or more files at a networked device comprising a plurality of processing cores, the packets from a plurality of connections;

processing each of the received packets, wherein processing each received packet comprises:

determining from which of the plurality of connections the packet came, and

postponing processing one of the received packets based on a determination that another processing core is currently processing a packet from a same connection, and

continuing to process the one of the received packets based on a determination that no other processing core is currently processing a packet from the same connection;

storing a current state of pattern matching in a database in memory accessible to each of the plurality of processing cores, wherein the current state of pattern matching corresponds to packets received from the determined corresponding connection, and wherein a plurality of other current states of pattern matching are stored for other connections from the plurality of connections;

scanning each of the plurality of packets using one of the plurality of processing cores in the networked device without buffering the one or more files in the networked device, such that the plurality of processing cores scan the plurality of packets substantially concurrently, wherein when the plurality of packets are from one of the plurality of connections, a first processing core of the plurality of processing core receives an in-order packet and scans the in-order packet, a second processing core of the plurality of processing core receives an out-of-order packet and temporarily buffers the out-of-order packet in an out-of-order buffer without scanning the out-of-order packet, wherein the first processing core retrieves a next in order packet from the out-of-order buffer to scan after scanning the in-order packet; and

updating the current state of pattern matching based on a plurality of scan results from the plurality of processing cores, the updated current state of pattern matching stored with the determined corresponding connection.

2. The method of claim **1**, further comprising: resolving conflicts between out-of-order packets among the plurality of packets.

3. The method of claim **2**, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order or out-of order;

the first processing core scanning the packet if the first packet is in-order; and

the first processing core temporarily buffering the first packet in an out-of order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

4. The method of claim **3**, wherein resolving conflicts between out-of-order packets further comprises:

the second processing core of the plurality of processing cores receiving a second packet from the first connection while the first processing core is still processing the first packet; and

the second processing core re-scheduling scanning of the second packet to a later time.

5. The method of claim 1, wherein storing the current state of pattern matching further comprises storing a plurality of current states in the database, each current state associated with one of the plurality of connections.

6. An apparatus comprising:

a network interface to receive a plurality of packets of one or more files from a plurality of connections;

a plurality of processing cores to perform reassembly-free deep packet inspection on the plurality of packets without buffering the one or more files such that the plurality of processing cores scan the plurality of packets substantially concurrently, wherein each processing core processes each received packet by:

determining from which of the plurality of connections the packet came,

postponing processing one of the received packets based on a determination that another processing core is currently processing a packet from a same connection, and

continuing to process the one of the received packets based on a determination that no other processing core is currently processing a packet from the same connection, wherein when the plurality of packets are from one of the plurality of connections, a first processing core of the plurality of processing core receives an in-order packet and scans the in-order packet, a second processing core of the plurality of processing core receives an out-of-order packet and temporarily buffers the out-of-order packet in an out-of-order buffer without scanning the out-of-order packet, wherein the first processing core retrieves a next in order packet from the out-of-order buffer to scan after scanning the in-order packet; and

memory accessible to each of the plurality of processing cores, the memory associated with a database for storing a current state of pattern matching, the current state of pattern matching corresponding to packets from the determined corresponding connection, wherein a plurality of other current states of pattern matching are stored for other connections from the plurality of connections, wherein the current state of pattern matching is updated based on a plurality of scan results from the plurality of processing cores, the updated current state of pattern matching stored with the determined corresponding connection.

7. The apparatus of claim 6, wherein the plurality of processing cores resolve conflicts between out-of-order packets among the plurality of packets.

8. The apparatus of claim 6, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection and scans the packet if the first packet is in-order, and temporarily buffers the first packet in an out-of-order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

9. The apparatus of claim 6, wherein the second processing core to receive a second packet from a first connection while the first processing core is still processing the first packet, and to re-schedule scanning of the second packet to a later time.

10. The apparatus of claim 6, wherein the database further stores a plurality of current states, each current state associated with one of the plurality of connections.

11. A system comprising the apparatus of claim 6, further comprising: one or more client devices coupled to receive the plurality of packets after the plurality of packets have been scanned without identifying any prohibited content.

12. A non-transitory computer-readable medium embodying instructions that, when executed by a processor, will cause the processor to perform operations comprising:

receiving a plurality of packets of one or more files at a networked device comprising a plurality of processing cores, the packets from plurality of connections;

processing each of the received packets, wherein processing each received packet comprises:

determining from which of the plurality of connections the packet came,

postponing processing one of the received packets based on a determination that another processing core is currently processing a packet from a same connection, and

continuing to process the one of the received packets based on a determination that no other processing core is currently processing a packet from the same connection;

storing a current state of pattern matching in a database accessible to each of the plurality of processing cores, wherein the current state of pattern matching corresponds to packets from the determined corresponding connection, and wherein a plurality of other current states of pattern matching are stored for other connections from the plurality of connections;

scanning each of the plurality of packets using one of the plurality of processing cores in the networked device without buffering the one or more files in the networked device, such that the plurality of processing cores scan the plurality of packets substantially concurrently, wherein when the plurality of packets are from one of the plurality of connections, a first processing core of the plurality of processing core receives an in-order packet and scans the in-order packet, a second processing core of the plurality of processing core receives an out-of-order packet and temporarily buffers the out-of-order packet in an out-of-order buffer without scanning the out-of-order packet, wherein the first processing core retrieves a next in order packet from the out-of-order buffer to scan after scanning the in-order packet; and

updating the current state of pattern matching based on a plurality of scan results from the plurality of processing cores, the updated current state of pattern matching stored with the determined corresponding connection.

13. The non-transitory computer-readable medium of claim 12, wherein the operations further comprise: resolving conflicts between out-of-order packets among the plurality of packets.

14. The non-transitory computer-readable medium of claim 12, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order or out-of order;

the first processing core scanning the packet if the first packet is in-order; and

the first processing core temporarily buffering the first packet in an out-of order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

15. The non-transitory computer-readable medium of claim 14, wherein resolving conflicts between out-of-order packets further comprises:

the second processing core of the plurality of processing cores receiving a second packet from the first connection while the first processing core is still processing the first packet; and

the second processing core re-scheduling scanning of the second packet to a later time.

16. The non-transitory computer-readable medium of claim **12**, wherein storing the current state of pattern matching further comprises: storing a plurality of current states in the database, each current state associated with one of the plurality of connections.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 8,813,221 B1
APPLICATION NO. : 12/238205
DATED : August 19, 2014
INVENTOR(S) : Dubrovsky et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Column 10, Lines 44-46 should read:

2. The method of claim 1, further comprising[[:]] resolving conflicts between out-of-order packets among the plurality of packets.

Column 10, Lines 47-59 should read:

3. The method of claim 2, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order; and

the first processing core scanning the packet if the first packet is in-order.

Column 11, Lines 49-56 should read:

8. The apparatus of claim 6, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection and scans the packet if the first packet is in-order.

Column 11, Lines 64-67 should read:

11. A system comprising the apparatus of claim 6, further comprising [[:]] one or more client devices coupled to receive the plurality of packets after the plurality of packets have been scanned without identifying any prohibited content.

Column 12, Lines 47-50 should read:

Signed and Sealed this
Eighteenth Day of August, 2015

Michelle K. Lee

Michelle K. Lee
Director of the United States Patent and Trademark Office

13. The non-transitory computer-readable medium of claim 12, wherein the operations further comprise [[:]] resolving conflicts between out-of-order packets among the plurality of packets.

Column 12, Lines 51-64 should read:

14. The non-transitory computer-readable medium of claim [[12]] 13, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order; and

the first processing core scanning the packet if the first packet is in-order.

Column 13, Lines 7-11 should read:

16. The non-transitory computer-readable medium of claim 12, wherein storing the current state of pattern matching further comprises [[:]] storing a plurality of current states in the database, each current state associated with one of the plurality of connections.

Column 13, Lines 12-19 should read:

17. The method of claim 2, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is out-of-order; and

the first processing core temporarily buffering the first packet in an out-of-order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

Column 13, Lines 20-24 should read:

18. The apparatus of claim 6, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection and temporarily buffers the first packet in an out-of-order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

Column 13, Lines 25-32 should read:

19. The non-transitory computer-readable medium of claim 13, wherein when the plurality of packets

are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is out-of order; and

the first processing core temporarily buffering the first packet in an out-of order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix X

IMMEDIATE RELEASE

NSA Stops Certain Section 702 "Upstream" Activities

Press Operations

Release No: PA-014-18
April 28, 2017

Since 2008, the National Security Agency (NSA) and other members of the U.S. Intelligence Community have relied on Section 702 of the Foreign Intelligence Surveillance Act (FISA) to conduct surveillance on specific foreign targets located outside the United States to acquire critical intelligence on issues ranging from international terrorism to cybersecurity. After a comprehensive review of mission needs, current technological constraints, United States person privacy interests, and certain difficulties in implementation, NSA has decided to stop some of its activities conducted under Section 702.

While the Foreign Intelligence Surveillance Court (FISC) was considering the government's annual application to renew the Section 702 certifications, NSA reported several earlier, inadvertent compliance incidents related to queries involving U.S. person information in 702 "upstream" internet collection. Although the incidents were not willful, NSA was required to, and did, report them to both Congress and the FISC. The court issued two extensions of the government's renewal application in order to receive additional information from the government about this issue and the government's plan to resolve it. The previous year's certifications remained in effect during these extension periods.

During the extension period, NSA undertook a broad review of its Section 702 program. Under Section 702, NSA collects internet communications in two ways: "downstream" (previously referred to as PRISM) and "upstream." Under downstream collection, NSA acquires communications "to or from" a Section 702 selector (such as an email address). Under upstream collection, NSA acquires communications "to, from, or about" a Section 702 selector. An example of an "about" email communication is one that includes the targeted email address in the text or body of the email, even though the email is between two persons who are not themselves targets. The independent Privacy and Civil Liberties Oversight Board described these collection methods in an exhaustive report published in 2014.

After considerable evaluation of the program and available technology, NSA has decided that its Section 702 foreign intelligence surveillance activities will no longer

include any upstream internet communications that are solely about a foreign intelligence target. Instead, this surveillance will now be limited to only those communications that are directly "to" or "from" a foreign intelligence target. These changes are designed to retain the upstream collection that provides the greatest value to national security while reducing the likelihood that NSA will acquire communications of U.S. persons or others who are not in direct contact with one of the Agency's foreign intelligence targets.

In addition, as part of this curtailment, NSA will delete the vast majority of previously acquired upstream internet communications as soon as practicable.

NSA previously reported that, because of the limits of its current technology, it is unable to completely eliminate "about" communications from its upstream 702 collection without also excluding some of the relevant communications directly "to or from" its foreign intelligence targets. That limitation remains even today. Nonetheless, NSA has determined that in light of the factors noted, this change is a responsible and careful approach at this time.

After reviewing amended Section 702 certifications and NSA procedures that implement these changes, the FISC recently issued an opinion and order, approving the renewal certifications and use of procedures, which authorize this narrowed form of Section 702 upstream internet collection. A declassification review of the FISC's opinion and order, and the related targeting and minimization procedures, is underway.

The National Security Agency works tirelessly around the world to help keep the nation safe. We have a solemn responsibility and commitment to do this work exactly right. When incidents occur, we immediately report them to oversight bodies and develop appropriate solutions. We never stop putting improvements in place while carrying out our critical mission.

IMMEDIATE RELEASE

NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702

Press Operations

Release No: PA-044-18
April 28, 2017

The National Security Agency is instituting several changes in the way it collects information under Section 702 of the Foreign Intelligence Surveillance Act.

Section 702, set to expire at the end of this year, allows the Intelligence Community to conduct surveillance on only specific foreign targets located outside the United States to collect foreign intelligence, including intelligence needed in the fight against international terrorism and cyber threats.

NSA will no longer collect certain internet communications that merely mention a foreign intelligence target. This information is referred to in the Intelligence Community as "about" communications in Section 702 "upstream" internet surveillance. Instead, NSA will limit such collection to internet communications that are sent directly to or from a foreign target.

Even though NSA does not have the ability at this time to stop collecting "about" information without losing some other important data, the Agency will stop the practice to reduce the chance that it would acquire communications of U.S. persons or others who are not in direct contact with a foreign intelligence target.

Finally, even though the Agency was legally allowed to retain such "about" information previously collected under Section 702, the NSA will delete the vast majority of its upstream internet data to further protect the privacy of U.S. person communications.

The changes in policy followed an in-house review of Section 702 activities in which NSA discovered several inadvertent compliance lapses.

NSA self-reported the incidents to both Congress and the FISC, as it is required to do. Following these reports, the FISC issued two extensions as NSA worked to fix the problems before the government submitted a new application for continued Section 702 certification. The FISC recently approved the changes after an extensive review.

The Agency's efforts are part of its commitment to continuous improvement as we work to keep the nation safe. NSA has a solemn responsibility and duty to do our

work exactly right while carrying out our critical mission."

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix Y

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

STATISTICAL TRANSPARENCY REPORT

Regarding Use of National Security Authorities

~ Calendar Year 2017 ~

LEADING INTELLIGENCE INTEGRATION

Office of Civil Liberties, Privacy, and Transparency

April 2018

STATISTICAL TRANSPARENCY REPORT

Regarding Use of National Security Authorities

~ Calendar Year 2017 ~

Table of Contents

Introduction

Today, consistent with the USA FREEDOM Act and the FISA Amendments Reauthorization Act of 2017 (the reauthorized FAA) requirements to release certain statistics (codified in 50 U.S.C. § 1873(b)) and the Intelligence Community's (IC) Principles of Intelligence Transparency, we are releasing our **fifth** annual *Statistical Transparency Report Regarding Use of National Security Authorities* presenting statistics on how often the government uses certain national security authorities. Providing these statistics allows for an additional way to track the use of Foreign Intelligence Surveillance Act (FISA) authorities and gives further context to the IC's rigorous and multi-layered oversight framework that safeguards the privacy of United States person information acquired pursuant to FISA. The report goes beyond its statutory duty of providing statistics and further provides the public with detailed explanation as to how the IC uses these national security authorities.

Additional public information on national security authorities is available at the Office of the Director of National Intelligence's (ODNI) website, www.dni.gov, and ODNI's public tumblr site, *IC on the Record*. Furthermore, since the release of the previous report, ODNI has created the new website, www.intelligence.gov, that contains additional public information on the IC's activities.

A. Background.

In June 2014, the Director of National Intelligence (DNI) began releasing statistics relating to the use of critical national security authorities, including the FISA, in an annual report called the *Statistical Transparency Report Regarding Use of National Security Authorities* (hereafter the *Annual Statistical Transparency Report*). Subsequent *Annual Statistical Transparency Reports* were released in 2015, 2016, and 2017.

On June 2, 2015, the USA FREEDOM Act was enacted, codifying a requirement to publicly report many of the statistics already reported in the *Annual Statistical Transparency Report.* The Act also expanded the scope of the information included in the reports by requiring the DNI to report information concerning United States person (U.S. person or USP) search terms and queries of certain FISA-acquired information, as well as specific statistics concerning call detail records. *See* 50 U.S.C. § 1873(b). On January 19, 2018, the reauthorized FAA was signed. *See* 50 U.S.C. § 1881a. The reauthorized FAA (also referred to as the Section 702 Reauthorization Act of 2017) codified additional statistics that must be publicly released, including many statistics that the government previously reported pursuant to its commitment to transparency.

B. Areas Covered in this Report.

This report provides statistics in the following areas (the terms used below are defined and explained later in this report):

- **FISA Probable Cause Authorities.** The number of orders—and the number of targets under those orders—for the use of FISA authorities that require probable cause determinations by the Foreign Intelligence Surveillance Court (FISC), under Titles I and III, and Section 703 and 704, of FISA.

- **FISA Section 702.**
  - The number of orders—and the number of targets under those orders—issued pursuant to Section 702 of FISA.
  - The number of U.S. person queries of Section 702-acquired content and metadata.
  - The number of instances in which the Federal Bureau of Investigation (FBI) personnel received and reviewed Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence.
  - The number of instances in which the FBI opened, under the Criminal Investigative Division, an investigation of a U.S. person (who is not considered a threat to national security) based wholly or in part on Section 702-acquired information.
  - The number of National Security Agency (NSA)-disseminated Section 702 reports containing U.S. person identities (various statistics relating to reports where the U.S. person identity was openly named or originally masked and subsequently unmasked).

- **Use in Criminal Proceedings.** The number of criminal proceedings in which the United States or a State or political subdivision provided notice under FISA of the government's intent to enter into evidence or otherwise use or disclose any information derived from electronic surveillance, physical search, or Section 702 acquisition.

- **Pen Register and Trap and Trace Devices.** The number of orders—and the number of targets under those orders—for the use of FISA's pen register/trap and trace devices, and the number of unique identifiers used to communicate information collected pursuant to those orders.

- **Business Records.** The number of orders—and the number of targets under those orders—issued pursuant to FISA's business records authority, and the number of unique identifiers used to communicate information collected pursuant to those orders. In

addition, the number of orders—and the number of targets under those orders—issued pursuant to FISA's business record authority for the production of call detail records, and the number of call detail records received from providers and stored in NSA repositories.

- **National Security Letters**. The number of national security letters issued, and the number of requests for information within those national security letters.

C. Context and Clarity.

Consistent with the IC's *Principles of Intelligence Transparency*, this report seeks to enhance public understanding by including explanations and charts for context and clarity. For example, the report provides charts that place the statistics in this report in context with the statistics in prior reports. While these statistics provide an important point of reference for understanding the use of these authorities, it is important to keep in mind the statistics' limitations. The statistics fluctuate from year to year for a variety of reasons (e.g., operational priorities, world events, technical capabilities), some of which cannot be explored in an unclassified setting. Moreover, there may be no relationship between a decrease in the use of one authority and an increase in another. Nonetheless, we believe this report provides helpful information about how the IC uses these vital national security authorities.

D. Key Terms.

Certain terms used throughout this report are described below. Other terms are described in the sections in which they are most directly relevant.

- **U.S. Person**. As defined by Title I of FISA, a U.S. person is "a citizen of the United States , an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)]." 50 U.S.C. § 1801(i). Section 602 of the USA FREEDOM Act, however, uses a narrower definition. Since the broader Title I definition governs how U.S. person queries are conducted pursuant to the relevant minimization procedures, it will be used throughout this report.

- **Target.** Within the IC, the term "target" has multiple meanings. With respect to the statistics provided in this report, the term "target" is defined as the individual person, group, entity composed of multiple individuals, or foreign power that uses the selector such as a telephone number or email address.

- **Orders.** There are different types of orders that the FISC may issue in connection with FISA cases, for example: orders granting or modifying the government's authority to conduct foreign intelligence collection; orders directing electronic communication service providers to provide any technical assistance necessary to implement the authorized foreign intelligence collection; and supplemental orders and briefing orders requiring the government to take a particular action or provide the court with specific information. The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. This report *does not count such amendments* separately. The FISC may renew some orders multiple times during the calendar year. Each authority permitted under FISA has specific time limits for the FISA authority to continue (e.g., a Section 704 order against a U.S. person target outside of the United States may last no longer than 90 days but FISA permits the order to be renewed, *see* 50 U.S.C. § 1881c(c)(4)). Each renewal requires a separate application submitted by the government to the FISC and a finding by the FISC that the application meets the requirements of FISA. Thus, unlike amendments, this report *does count each such renewal* as a separate order. These terms will be used consistently throughout this report.

- **"Estimated Number."** Throughout this report, when numbers are *estimated,* the estimate comports with the statutory requirements to provide a "good faith estimate" of a particular number.

- **Dissemination.** In the most basic sense, dissemination refers to the sharing of minimized information. As it pertains to FISA (including Section 702), if an agency (in this instance NSA) lawfully collects information pursuant to FISA and wants to disseminate that information, the agency must first apply its minimization procedures to that information.

FISA Probable Cause Authorities

A. FISA Titles I and III

FISA Title I, Title III, and Title VII Section 703 and 704

→ *All of these authorities require individual court orders based on probable cause.*

→ *Titles I and III apply to FISA activities directed against persons within the United States.*

→ *Sections 703 and 704 apply to FISA activities directed against U.S. persons outside the United States.*

To conduct electronic surveillance or physical search under FISA Title I or FISA Title III, a probable cause court order is required regardless of U.S. person status. Under FISA, Title I permits electronic surveillance and Title III permits physical search in the United States of foreign powers or agents of a foreign power for the purpose of collecting foreign intelligence information. *See* 50 U.S.C. §§ 1804 and 1823. Title I (electronic surveillance) and Title III (physical search) are commonly referred to as "Traditional FISA." Both require that the FISC make a probable cause finding, based upon a factual statement in the government's application, that (i) the target is a foreign power or an agent of a foreign power, as defined by FISA and (ii) the facility being targeted for electronic surveillance is used by or about to be used, or the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power. In addition to meeting the probable cause standard, the government's application must meet the other requirements of FISA. *See* 50 U.S.C. §§ 1804(a) and 1823(a).

B. FISA Title VII, Sections 703 and 704

FISA Title VII Sections 703 and 704 similarly require a court order based on a finding of probable cause for the government to undertake FISA activities targeting U.S. persons located outside the United States. Section 703 applies when the government seeks to conduct electronic surveillance or to acquire stored electronic communications or stored electronic data, in a manner that otherwise requires an order pursuant to FISA, of a U.S. person who is reasonably believed to be located outside the United States. Section 704 applies when the government seeks to conduct collection overseas targeting a U.S. person reasonably believed to be located outside the United States under circumstances in which the U.S. person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States. Both Sections 703 and 704 require that the FISC make a

probable cause finding, based upon a factual statement in the government's application, that the target is a U.S. person reasonably believed to be (i) located outside the United States and (ii) a foreign power, agent of a foreign power, or officer or employee of a foreign power. Additionally, the government's application must meet the other requirements of FISA. *See* 50 U.S.C. §§ 1881b(b) and 1881c(b).

C. Statistics

How targets are counted. If the IC received authorization to conduct electronic surveillance and/or physical search against the same target in four separate applications, the IC would count one target, not four. Alternatively, if the IC received authorization to conduct electronic surveillance and/or physical search against four targets in the same application, the IC would count four targets. Duplicate targets across authorities are not counted.

Figure 1a: Table of FISA "Probable Cause" Court Orders and Targets

Titles I and III and Sections 703 and 704 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of orders	1,767	1,519	1,585	1,559	**1,437**
Estimated number of targets of such orders*	1,144	1,562	1,695	1,687	**1,337**

See 50 U.S.C. §§ 1873(b)(1) and 1873(b)(1)(A).

* Although providing this statistic was first required by the USA FREEDOM Act, the reauthorized FAA of 2017 enumerated this requirement at 50 U.S.C. § 1873(b)(1)(A).

Figure 1b: Chart of FISA "Probable Cause" Court Orders and Targets

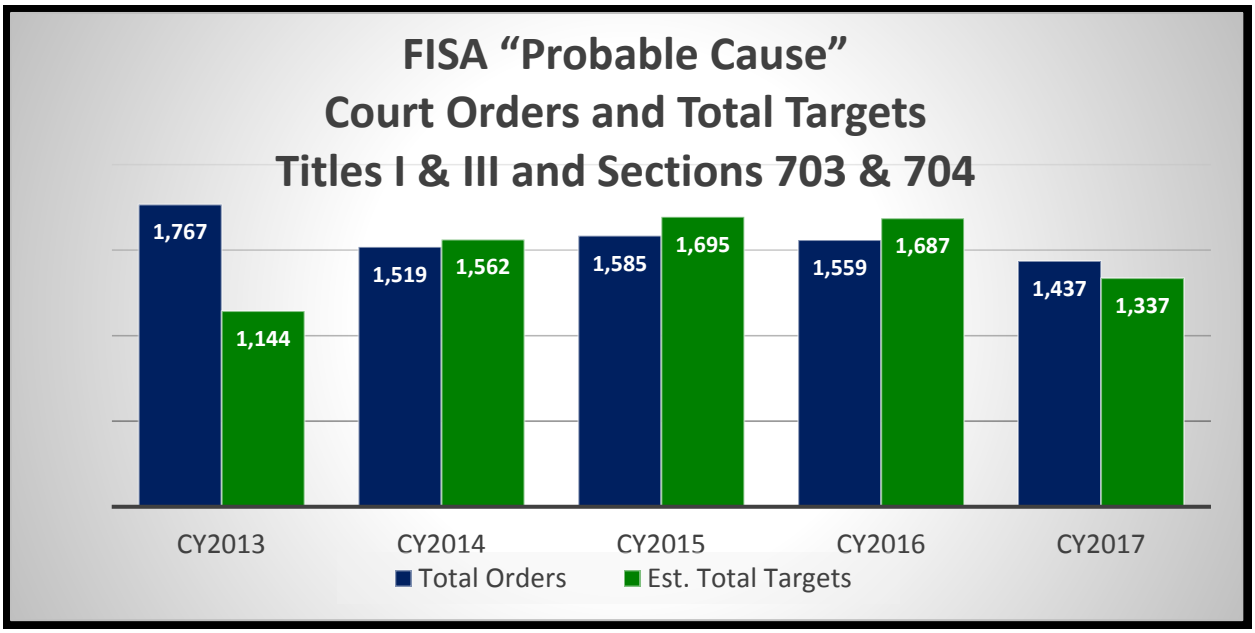


Figure 2: Table of FISA "Probable Cause" Targets – U.S. Persons

Titles I and III and Sections 703 and 704 -- Targets	CY2016	CY2017
Estimated number of targets who are *non*-U.S. persons*	1,351	**1,038**
Estimated number of targets who are U.S. persons*	336	**299**
Estimated percentage of targets who are U.S. persons	19.9%	**22.4%**

See 50 U.S.C. §§1873(b)(1)(B) and 1873(b)(1)(C) for rows one and two, respectively.

* Previously the IC was not statutorily required to publicly provide these statistics but provided them consistent with transparency principles. The reauthorized FAA of 2017 codified this requirement at 50 U.S.C. §§ 1873(b)(1)(B) and 1873(b)(1)(C).

FISA Section 702

A. Section 702

Title VII - FISA Amendments Act (FAA) Section 702

→ *Commonly referred to as "Section 702."*

→ *Requires individual targeting determinations that the target (1) is a non-U.S. person (2) who is reasonably believed to be located outside the United States and (3) who has or is expected to communicate or receive foreign intelligence information.*

Title VII of FISA includes Section 702, which permits the Attorney General and the DNI to jointly authorize the targeting of (i) non-U.S. persons (ii) reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. *See* 50 U.S.C. § 1881a. All three elements must be met. Additionally, Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting procedures, minimization procedures, and querying procedures that they attest satisfy the statutory requirements and are consistent with the Fourth Amendment. Additional information on how the government uses Section 702 is posted on *IC on the Record*.

Section 702 Targets and "Tasking." Under Section 702, the government "targets" a particular non-U.S. person, group, or entity reasonably believed to be located outside the United States and who possesses, or who is likely to communicate or receive, foreign intelligence information, by directing an acquisition at – i.e., "*tasking*" – selectors (e.g., telephone numbers and email addresses) that are assessed to be used by such non-U.S. person, group, or entity, pursuant to targeting procedures approved by the FISC. Before "tasking" a selector for collection under Section 702, the government must apply its targeting procedures to ensure that the IC appropriately tasks a selector used by a non-U.S. person who is reasonably believed to be located outside the United States and who will likely possess, communicate, or receive foreign intelligence information.

NSA and FBI task selectors pursuant to their respective Section 702 targeting procedures, which are discussed below. All agencies that receive unminimized (i.e., "raw") Section 702 data – NSA, FBI, Central Intelligence Agency (CIA), and National Counterterrorism Center (NCTC) – handle the Section 702-acquired data in accordance with minimization procedures, which are explained below.

The FISC's role. Under Section 702, the FISC determines whether *certifications* provided jointly by the Attorney General and the DNI meet all the requirements of Section 702. If the FISC determines that the government's certifications its targeting, minimization, and, as described below, querying procedures meet the statutory requirements of Section 702 and are consistent with the Fourth Amendment, then the FISC issues an order and supporting statement approving the certifications. The 2016 FISC order and statement approving certifications was publicly released in May 2017 and posted on *IC on the Record*.

Certifications. The certifications are jointly executed by the Attorney General and DNI and authorize the government to acquire foreign intelligence information under Section 702. Each annual certification application package must be submitted to the FISC for approval. The package includes the Attorney General and DNI's certifications, affidavits by certain heads of intelligence agencies, targeting procedures, minimization procedures, and, as described below, querying procedures. Samples of certification application packages have been publicly released on *IC on the Record*, most recently in May 2017. The certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information, through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The certifications have included information concerning international terrorism and other topics, such as the acquisition of information concerning weapons of mass destruction.

Targeting procedures. The targeting procedures detail the steps that the government must take before tasking a selector, as well as verification steps after tasking, to ensure that the user of the tasked selector is being targeted appropriately – specifically, that the user is a non-U.S. person, located outside the United States, who is being tasked to acquire foreign intelligence information. The IC must make individual determinations that each tasked selector meets the requirements of the targeting procedures. Each agency's Section 702 targeting procedures are approved by the Attorney General and then reviewed, as part of the certification package, by the FISC, which reviews the sufficiency of each agency's targeting procedures including assessing the IC's compliance with the procedures. NSA's targeting procedures (signed in 2017) for the 2016 certification package have been publicly released *IC on the Record*.

Minimization procedures. The minimization procedures detail requirements the government must meet to use, retain, and disseminate Section 702 data, which include specific restrictions on how the IC handles non-publicly available U.S. person information acquired from Section 702 collection of non-U.S. person targets, consistent with the needs of the government to obtain, produce, and disseminate foreign intelligence information. Each agency's Section 702 minimization procedures are approved by the Attorney General and then reviewed, as part of the certification package, by the FISC, which reviews the sufficiency of each agency's

minimization procedures, including assessing the IC's compliance with past procedures. The 2016 certification minimization procedures have been released on *IC on the Record*.

Querying procedures. With the reauthorized FAA of 2017, Congress amended Section 702 to require that querying procedures be adopted by the Attorney General, in consultation with the DNI. Section 702(f) requires that a record of each U.S. person query term be kept. Similar to the other procedures, the querying procedures are required to be reviewed by the FISC as part of the certification package for consistency with the statute and the Fourth Amendment. Congress added other requirements in 702(f), which pertain to the access of certain results of queries conducted by FBI; those requirements will be discussed later in this report.

To date, each agency's court-approved minimization procedures have provided the rules under which the agency may query their databases containing previously acquired Section 702 data (content and metadata) using a U.S. person query term. As described above, with the reauthorized FAA of 2017, Congress amended Section 702 to require that, going forward, querying procedures must be adopted by the Attorney General. Query terms may be date-bound, and may include alphanumeric strings, such as telephone numbers, email addresses, or terms, such as a name, that can be used individually or in combination with one another. Pursuant to court-approved procedures, an agency can only query Section 702 information if the query is reasonably likely to return foreign intelligence information or, in the case of the FBI, evidence of a crime. Additional information about U.S. person queries is posted on *IC on the Record*.

Compliance. The IC's adherence to the targeting and minimization procedures, including query requirements, is subject to robust internal agency oversight and to rigorous external oversight by the Department of Justice (DOJ), ODNI, Congress, and the FISC. Every identified incidence of non-compliance is reported to the FISC (through individual notices or in reports) and to Congress in semiannual reports. DOJ and ODNI also submit semiannual reports to Congress that assess the IC's overall compliance efforts. Past assessments have been publicly released.

B. Statistics—Orders and Targets

Counting Section 702 orders. As explained above, the FISC may issue a single order to approve more than one Section 702 certification to acquire foreign intelligence information. Note that, in its own transparency report, which is required pursuant to 50 U.S.C. § 1873(a), the Director of the Administrative Office of the United States Courts (AOUSC) counted each of the Section 702 certifications associated with the FISC's order. Because the number of the government's Section 702 certifications remains a classified fact, the government requested that the AOUSC redact the number of certifications from its transparency report prior to publicly releasing it.

In 2016, the government submitted a certification application package to the FISC. Pursuant to 50 U.S.C. § 1881a(j)(2), the FISC extended its review of the 2016 certification package. The FISC may extend its review of the certifications "as necessary for good cause in a manner consistent with national security." *See* 50 U.S.C. § 1881a(j)(2) (note that with the reauthorized FAA of 2017, this section has been updated to § 1881a(k)(2)). Thus, because the FISC did not complete its review of the 2016 certifications during calendar year 2016, the FISC did not issue an order concerning those certifications in calendar year 2016. The 2015 order remained in effect during the extension period. On April 26, 2017, the FISC issued an order authorizing the 2016 certifications.

Figure 3: Table of Section 702 Orders

Section 702 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of orders issued	1	1	1	0	**1**

See 50 U.S.C. § 1873(b)(2).

Estimating Section 702 targets. The number of 702 "targets," provided below, reflects an estimate of the number of non-U.S. persons who are the users of tasked selectors. This estimate is based on information readily available to the IC. Unless and until the IC has information that links multiple selectors to a single foreign intelligence target, each individual selector is counted as a separate target for purposes of this report. On the other hand, where the IC is aware that multiple selectors are used by the same target, the IC counts the user of those selectors as a single target. This counting methodology reduces the risk that the IC might inadvertently understate the number of discrete persons targeted pursuant to Section 702.

Figure 4: Table of Section 702 Targets (recall that only non-USPs are targeted)

Section 702 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017
Estimated number of targets of such orders*	89,138	92,707	94,368	106,469	**129,080**

See 50 U.S.C. § 1873(b)(2)(A).

* Previously the IC was not statutorily required to publicly provide this statistic, but provided it consistent with transparency principles. The reauthorized FAA of 2017 codified this requirement at 50 U.S.C. § 1873(b)(2)(A).

C. Statistics—U.S. Person Queries

In July 2014, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) issued a report on Section 702 entitled, "*Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*" (*PCLOB's Section 702 Report*), which reported U.S. person query statistics for calendar year 2013. *See PCLOB's Section 702 Report,* at 57-58. The USA FREEDOM Act, enacted in 2015, required the public reporting of statistics regarding the number of U.S. person queries of Section 702. Specifically, the Act required the "number of search terms concerning a known United States person used to retrieve the unminimized contents […]" – referred as *query terms of content* – and "the number of queries concerning a known United States person of unminimized noncontents information […]" – referred as *queries of metadata*. *See* 50 U.S.C. § 1873(b)(2)(B) and (b)(2)(C), respectively. Thus, ODNI began reporting on these statistics in the *Annual Statistical Transparency Report* covering calendar year 2015.

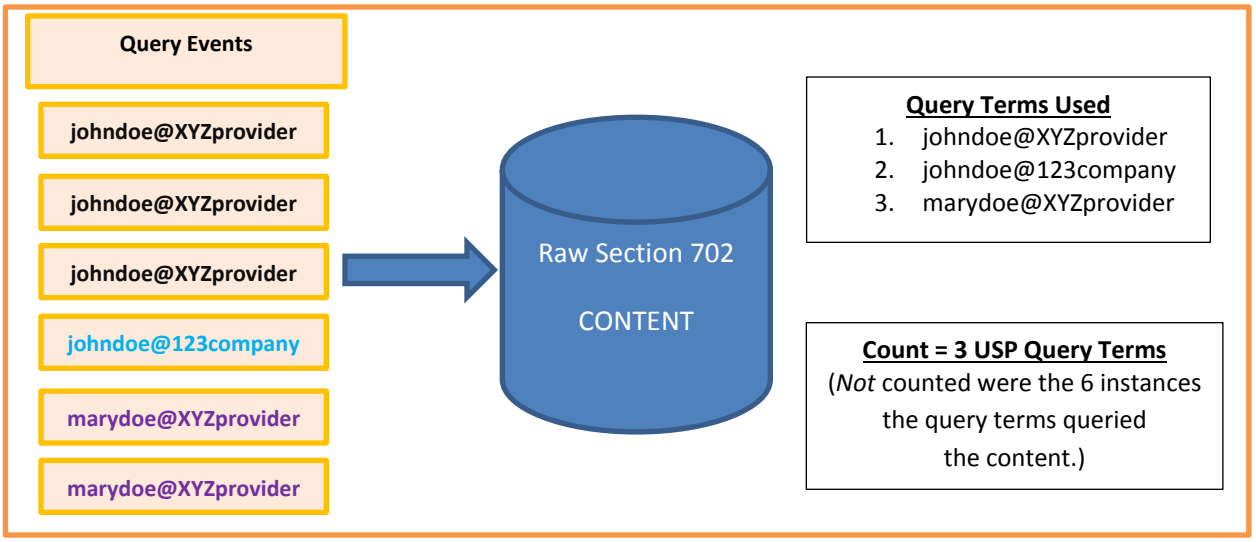
Below are statistics for U.S. person queries of raw, unminimized Section 702-acquired data.[1] The U.S. person statistics are based on (a) approved U.S. person *query terms* used to query

[1] With the reauthorization of FAA in 2017, Congress codified new requirements regarding the access of results of certain queries conducted by the FBI. Specifically under Section 702(f)(2)(A), an order from the FISC is now required before the FBI can review the contents of a query using a U.S. person query term when the query was not designed to find and extract foreign intelligence information and was performed in connection with a predicated criminal investigation that does not relate to national security. Before the FISC may issue such an order based on a finding of probable cause, an FBI officer must apply in writing, to include the officer's justification that the query results would provide evidence of criminal activity, and the application must be approved by the Attorney General.

Section 702 *content* and (b) U.S. person *queries* conducted of Section 702 *noncontents* (i.e., metadata). It is important to understand that these two very different numbers cannot be combined because they use *different counting methodologies* (approved query terms versus queries conducted) and *different data types* (content versus noncontents).

Counting approved U.S. person *query terms* used to query Section 702 *content*. The NSA counts the number of U.S. person identifiers it approved to query the content of unminimized Section 702-acquired information. For example, if the NSA used U.S. person identifier "johndoe@XYZprovider" to query the content of Section 702-acquired information, the NSA would count it as one regardless of how many times the NSA used "johndoe@XYZprovider" to query its 702-acquired information. The CIA started using this model in 2016 for counting query terms and those statistics were included in the *Annual Statistical Transparency Report* covering CY2016. When the NCTC began receiving raw Section 702 information, NCTC followed a similar approach of counting U.S. person query terms that were used to query Section 702 content.

Figure 5: Illustration of how the IC counts approved U.S. person query terms used to query Section 702 content



50 U.S.C. Section 1873(b)(2)(A) requires annual reporting of the number of times the FBI received an order pursuant to 702(f)(2)(A); this statistic will be provided in future transparency reports.

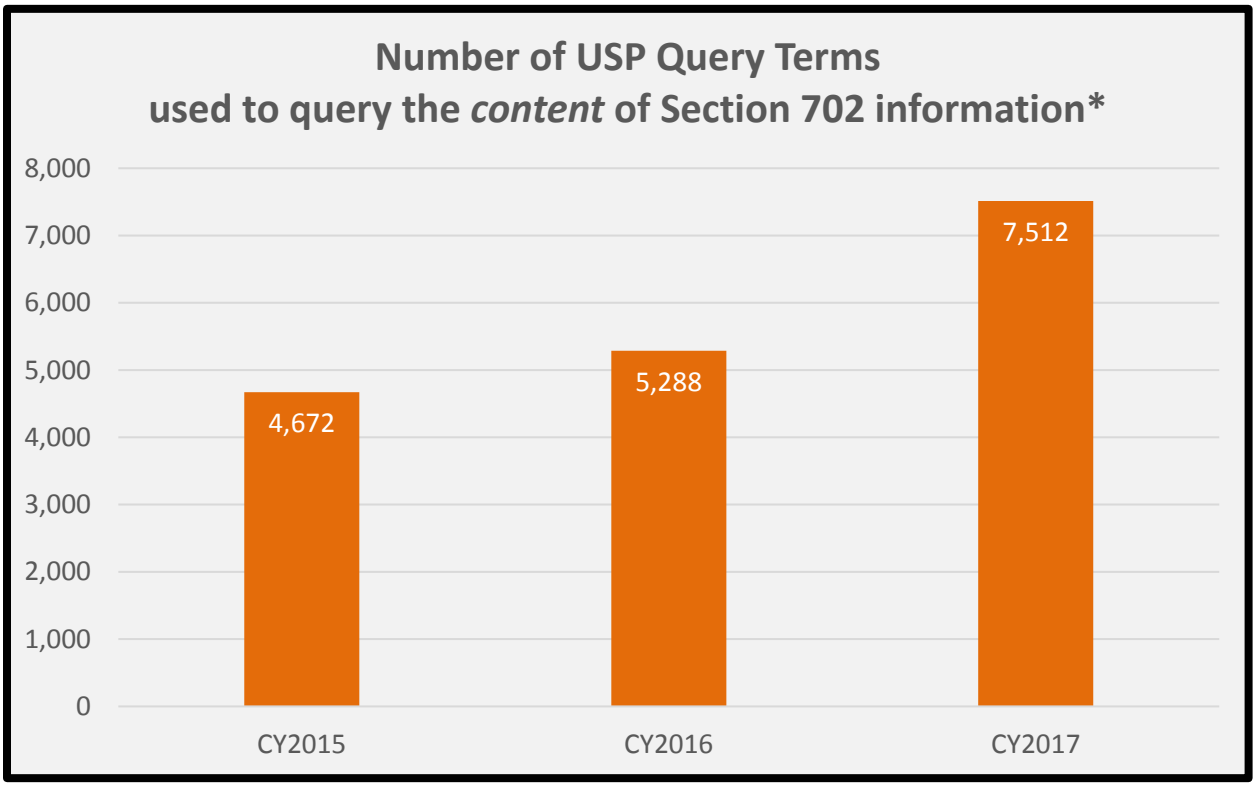
Figure 6a: Table of U.S. Person Query Terms Used to Query Section 702 Content

Section 702 of FISA	CY2015	CY2016	CY2017
Estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702 (excluding search terms used to prevent the return of U.S. person information)*	4,672	5,288	**7,512**

See 50 U.S.C. § 1873(b)(2)(B).

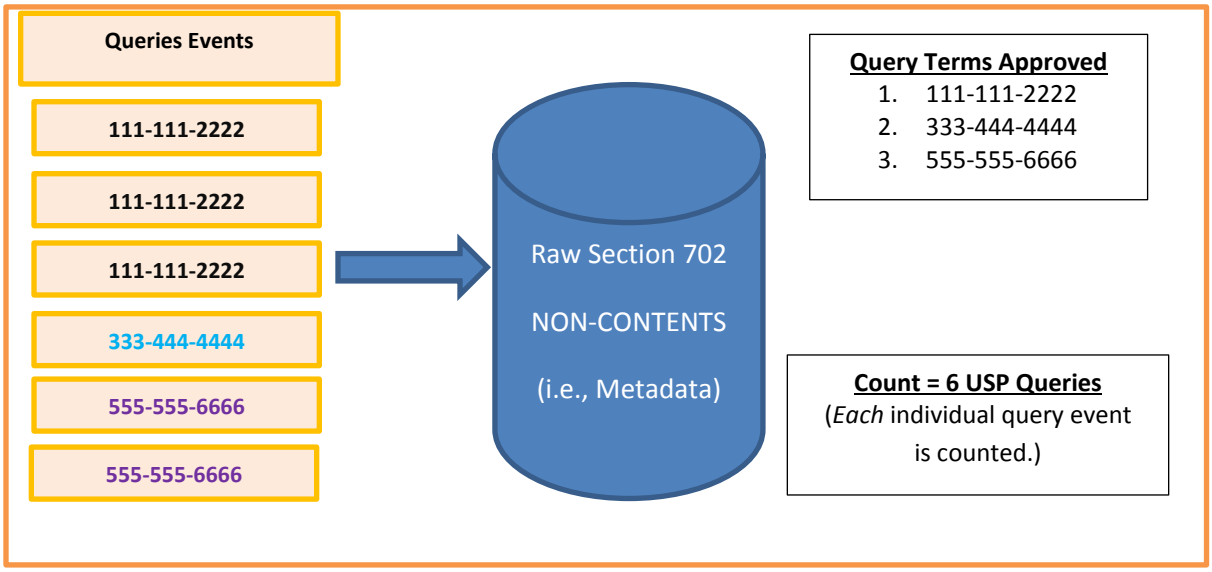
* Consistent with 50 U.S.C. § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI. However, the reauthorized FAA of 2017 codified a new reporting requirement for the FBI under 50 U.S.C. § 1873(b)(2)(D), which is addressed later in this report.

Figure 6b: Chart of U.S. Person Query Terms Used to Query Section 702 Content



Counting *queries* using U.S. person identifiers of noncontents collected under Section 702. This estimate represents the number of times a U.S. person identifier is used to query the noncontents (i.e., metadata) of unminimized Section 702-acquired information. For example, if the U.S. person identifier telephone number "111-111-2222" was used 15 times to query the noncontents of Section 702-acquired information, the number of queries counted would be 15.

Figure 7: Illustration of how the IC counts U.S. person queries of Section 702 noncontents



As with last year's transparency report, one IC element, the CIA, remains currently unable to provide the number of queries using U.S. person identifiers of unminimized Section 702 noncontents information for CY2017. Under 50 U.S.C. § 1873(d)(3)(A), if the DNI concludes that this good-faith estimate cannot be determined accurately because not all of the relevant elements of the IC are able to provide this good faith estimate, then the DNI is required to (i) certify that conclusion in writing to the relevant Congressional committees; (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate; (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and (iv) make such certification publicly available on an Internet web site. Because the CIA remained unable to provide such information for calendar year 2017, the DNI made a certification, pursuant to 50 U.S.C. § 1873(d)(3)(A) to the relevant Congressional committees. As required by statute, this certification is being made publicly available as an attached appendix to this current report (see Appendix A). As described in Appendix A, CIA will be able to provide a good faith estimate of these queries for calendar year 2018; such information will be included in the 2019 annual transparency report.

Figure 8: Table of U.S. Person Queries of Noncontents of Section 702

Section 702 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017
Estimated number of queries concerning a known U.S. person of unminimized noncontents information obtained under Section 702 (excluding queries containing information used to prevent the return of U.S. person information)*	9,500	17,500	23,800	30,355	**16,924**

See 50 U.S.C. § 1873(b)(2)(C).

* Consistent with 50 U.S.C. § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI. However, the reauthorized FAA of 2017 codified a new reporting requirement for the FBI under 50 U.S.C. § 1873(b)(2)(D), which was addressed earlier in this report.

FISC Order Requiring Certain Section 702 Query Reporting by FBI. On November 6, 2015, the FISC granted the government's application for renewal of the 2015 certifications and, among other things, concluded that the FBI's U.S. person querying provisions in its minimization procedures, "strike a reasonable balance between the privacy interests of the United States persons and persons in the United States, on the one hand, and the government's national security interests, on the other." *Memorandum Opinion and Order* dated November 6, 2015, at 44 (released on *IC on the Record* on April 19, 2016). The FISC further stated that the FBI conducting queries, "designed to return evidence of crimes unrelated to foreign intelligence does not preclude the Court from concluding that taken together, the targeting and minimization procedures submitted with the 2015 Certifications are consistent with the requirements of the Fourth Amendment." *Id*.

Nevertheless, the FISC ordered the government to report in writing, "each instance after December 4, 2015, in which FBI personnel *receive and review* Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information." (Emphasis added). *Id*. at 44 and 78. The FISC directed that the report contain details of the query terms, the basis for conducting the query, the manner in which the query will be or has been used, and other details. *Id.* at 78. In keeping with the IC's *Principles of Transparency*, the DNI declassified the number of each such query reported to the FISC in calendar year 2016. This year, the DNI has again declassified the number reported for calendar year 2017, as noted in Figure 10.

Figure 9: Table Regarding Required Section 702 Query Reporting to the FISC

Section 702 of FISA	CY2016	CY2017
Per the FISC Memorandum Opinion and Order dated November 6, 2015: Each reported instance in which FBI personnel *received and reviewed* Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence.	1	**0**

D. Section 702 and FBI Investigations.

The reauthorized FAA of 2017 now requires that the FBI report on the number of instances in which the FBI opened a criminal investigation of a U.S. person, who is not considered a threat to national security, based wholly or in part on Section 702-acquired information. *See* 50 U.S.C. § 1873(b)(2)(D). This statistic will provide transparency with regard to how often Section 702 collection is used for non-national security investigations conducted by the FBI. Figure 10 provides the required statistic.

Figure 10: Table Regarding Number of FBI Investigations Opened on USPs Based on Section 702 Acquisition

Section 702 of FISA	CY2017
The number of instances in which the FBI opened, under the Criminal Investigative Division or any successor division, an investigation of a U.S. person (who is not considered a threat to national security) based wholly or in part on an acquisition authorized under Section 702.	**0**

See 50 U.S.C. § 1873(b)(2)(D).

NSA Dissemination of U.S. Person Information under FISA Section 702

A. Section 702

In July 2014, the *PCLOB's Section 702 Report* contained 10 recommendations. Recommendation 9 focused on "accountability and transparency," noting that the government should implement measures, "to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program." *PCLOB's Section 702 Report* at 145-146. Specifically, the PCLOB recommended that "the NSA should implement processes to annually count […] (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers, such as telephone numbers or e-mail addresses, potentially associated with individuals." *Id.* at 146. This recommendation is commonly referred to as Recommendation 9(5). In response to the PCLOB's July 2014 Recommendation 9(5), NSA previously publicly provided (in the *Annual Statistical Transparency Report* for calendar year 2015) and continues to provide the following additional information regarding the dissemination of Section 702 intelligence reports that contain U.S. person information. Because the PCLOB issued its recommendation in 2014, these statistics were not included in *Annual Statistical Transparency Report* for calendar years 2013 or 2014.

NSA has been providing similar information to Congress since 2009, in classified form, per FISA reporting requirements. For example, FISA Section 702(m)(3) requires that NSA annually submit a report to applicable Congressional committees regarding certain numbers pertaining to the acquisition of Section 702-acquired information, including the number of "disseminated intelligence reports containing a reference to a United States person identity." *See* 50 U.S.C. § 1881a(m)(A)(3)(i) (prior to the reauthorized FAA of 2017under § 1881a(l)(3)(A)(i)). Section 702a(m)(A)(3) also requires that the number of "United States-person identities subsequently disseminated by [NSA] in response to request for identities that were not referred to by name or title in the original reporting." *See* 50 U.S.C. § 1881a(m)(3)(A)(ii). This second requirement refers to NSA providing the number of approved unmasking requests, which is explained below. Additionally, NSA provides the number of NSA's disseminated intelligence reports containing a U.S. person reference to Congress as part of the Attorney General and the DNI's joint assessment of compliance. *See* 50 U.S.C. § 1881a(m)(1) (prior to the reauthorized FAA of 2017under § 1881a(l)(1)).

Prior to the PCLOB issuing its *Section 702 Report*, NSA's Director of the Civil Liberties, Privacy, and Transparency Office published "*NSA's Implementation of Foreign Intelligence Surveillance Act Section 702,"* on April 16, 2014, (hereinafter "NSA DCLPO Report"), in which it explained

NSA's dissemination processes. *NSA DCLPO Report* at 7-8. NSA "only generates classified intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information." *NSA DCLPO Report* at 7.

Section 702 only permits the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. Such targets, however, may communicate information to, from, or about U.S. persons. NSA minimization procedures (publicly released on May 11, 2017) permit the NSA to disseminate U.S person information if the NSA masks the information that could identify the U.S. person. The minimization procedures also permit NSA to disseminate the U.S. person identity only if doing so meets one of the specified reasons listed in NSA's minimization procedures, including that the U.S. person consented to the dissemination, the U.S. person information was already publicly available, the U.S. person identity was necessary to understand foreign intelligence information, or the communication contained evidence of a crime and is being disseminated to law enforcement authorities. Even if one these conditions applies, as a matter of policy, NSA may still mask the U.S. person information and will include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. *Id.* In certain instances, however, NSA makes a determination prior to releasing its original classified report that the U.S. person's identity is appropriate to disseminate in the first instance using the same standards discussed above.

Masked U.S. Person Information. Agency minimization procedures generally provide for the substitution of a U.S. person identity with a generic phrase or term if the identity otherwise does not meet the dissemination criteria; this is informally referred to as "masking" the identity of the U.S. person. Information about a U.S. person is masked when the identifying information about the person is not included in a report. For example, instead of reporting that Section 702-acquired information revealed that non-U.S. person "Bad Guy" communicated with U.S. person "John Doe" (i.e., the actual name of the U.S. person), the report would mask "John Doe's" identity, and would state that "Bad Guy" communicated with "an identified U.S. person," "a named U.S. person," or "a U.S. person."

Unmasking U.S. Person Information. Recipients of NSA's classified reports, such as other federal agencies, may request that NSA provide the U.S. person identity that was masked in an intelligence report. The requested identity information is released only if the requesting recipient has a "need to know" the identity of the U.S. person and if the dissemination of the U.S. person's identity would be consistent with NSA's minimization procedures (e.g., the identity is necessary to understand foreign intelligence information or assess its importance), and additional approval has been provided by a designated NSA official.

As part of their regular oversight reviews, DOJ and ODNI review disseminations of information about U.S. persons that NSA obtained pursuant to Section 702 to ensure that the disseminations were performed in compliance with the minimization procedures.

Additional information describing how the IC protects U.S. person information obtained pursuant to FISA provisions is provided in recent reports by the civil liberties and privacy officers for the ODNI (including NCTC), NSA, FBI, and CIA. The reports collectively documented the rigorous and multi-layered framework that safeguards the privacy of U.S. person information in FISA disseminations. *See ODNI Report on Protecting U.S. Person Identities in Disseminations under FISA* and annexes containing agency specific reports.

B. Statistics

Below are statistics and charts to further explain how NSA disseminates U.S. person information incidentally acquired from Section 702 in classified intelligence reports. NSA may:

i. openly name (i.e., originally reveal) the U.S. person in the report,
ii. initially mask (i.e., not reveal) the U.S. person identity in the report, or
iii. in the instances where the U.S. person identity was initially masked, upon a specific request, later reveal and unmask the U.S. person identity but only to the requestor.

This year's report presents the dissemination numbers in a different format from the previous report to facilitate understanding and to provide consistency with NSA's classified FISA Section 702(m)(3) reports to Congress. This report separates the number of reports (in Figure 11) from the statistics relating to the U.S. person identities later disseminated (in Figure 12).

NSA applies its minimization procedures in preparing its classified intelligence reports, and then disseminates the reports to authorized recipients with a need to know the information in order to perform their official duties. Very few of NSA's intelligence reports from Section 702 collection contain references to U.S. person identities (whether masked or openly named).

The first row of Figure 11 provides "an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity." *See* 50 U.S.C. § 1881a(m)(3)(A)(i). Note that a single report could contain multiple U.S. person identities, masked and/or openly named. NSA's counting methodology is to include any disseminated intelligence report that contains a reference to one or more U.S. person identities, whether masked or openly named, even if the report includes information from other sources. NSA does not maintain records that allow it to readily determine, in the case of an intelligence report that includes information from several sources, from which source a reference to a U.S. person identity was derived. Accordingly, the references to U.S. person identities may have resulted

from Section 702 authorized collection or from other authorized signals intelligence activity conducted by NSA. This counting methodology was used in the previous report and is used in NSA's FISA Section 702(m)(3) report. As noted above, a U.S. person is "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)]." *See* 50 U.S.C. § 1801(i).

The second row of Figure 11 provides the *number of reports* containing U.S. person identities *where the U.S. person identity was masked* in the report. The third row provides the *number of reports* containing U.S. person *identities where the U.S. person was openly named* in the report.

Figure 11: Table of Section 702 *Reports* Containing USP information unmasked by NSA

Section 702 Reports Containing U.S. person (USP) information disseminated by NSA	CY2016	CY2017
Reports – Total number of NSA disseminated §702 reports containing USP identities *regardless of whether the identity was openly named or masked*.	3,914	**4,065**
Reports – Total number of NSA disseminated §702 reports containing USP identities *where the USP identity was masked.*	2,964	**3,034**
Reports – Total number of NSA disseminated §702 reports containing USP identities *where the USP was openly named*.	1,200	**1,341**

As explained above, rows 2 and 3 will not total row 1 because one report may contain both masked and openly namely identities.

Figure 12 provides statistics relating to the numbers of U.S. person identities that were originally masked in those reports counted in Figure 11 but which NSA later provided to authorized requestors (i.e., unmasked) during CY2017. This statistic is the number required to be reported to Congress in NSA's FISA Section 702(m)(3) report. In other words, Figure 12 provides "an accounting of the number of United States-person identities subsequently disseminated by [NSA] in response to requests for identities that were not referred to by name or title in the original reporting." *See* 50 U.S.C. § 1881a(m)(3)(A)(ii). This number is different than numbers provided in either CY2015 or the CY2016 *Annual Statistical Transparency Report*. NSA has decided to declassify the total number of U.S. person identities unmasked in response to a request. The U.S. person identities include individuals as well as non-individual entities

whose identities NSA masks pursuant to law or policy. These non-individual entities, include, for example, U.S. IP addresses and artificial "persons" such as corporations.

Previously, the *Annual Statistical Transparency Report* focused on responding to the PCLOB's report recommendation 9(5) by counting only those U.S. person identities where the proper name or title of an individual was unmasked; it did not count any other unmasking such as email addresses or telephone numbers or U.S. IP addresses or U.S. corporations. Rather than distinguishing between the different ways a U.S. person might be named in an intelligence report, NSA will provide the total number of U.S. person identities unmasked in response to a specific request from another agency whether it is a title of an individual, an identifier such as an email address, an IP address or a corporation. Thus, this current *Annual Statistical Transparency Report*, in Figure 12, reports that same metric that is reported in NSA's FISA Section 702(m)(3). However, because NSA's FISA Section 702(m)(3) reports have a time period of September through August, comparing the two reporting years is not an exact comparison.

Figure 12: Table of Section 702 USP Identities disseminated by NSA

Section 702 – U.S. person (USP) identities unmasked by NSA	12 month period Sep 2015-Aug 2016	CY2017
The number of U.S. person identities that NSA unmasked in response to a specific request from another agency.	9,217	**9,529**

Beginning with next year's transparency report (due April 2019), ODNI will report statistics pertaining to how the IC disseminates U.S. person information regardless of the legal authority under which the information was collected (not only FISA Section 702). *See* ICPG 107.1. Specifically, ODNI will report (1) the total number of requests to identify U.S. persons, whose identity was originally omitted, in disseminated intelligence reports, (2) the total number of those requests approved, and (3) the total number of those requests denied.

FISA Criminal Use and Notice Provisions

A. FISA Sections 106 and 305

FISA Sections 106 and 305
– Criminal Use and Notice Provisions –

→ *Commonly referred to as the "criminal use provision."*

→ *Section 106 applies to information acquired from Title I electronic surveillance; Section 305 applies to information acquired from Title III physical search.*

→ *Attorney General advance authorization is required before such information may be used in a criminal proceeding; if such information is used or intended to be used against an aggrieved person, that person must be given notice of the information and have a chance to suppress the information.*

→ *The reauthorized FAA of 2017 codified that statistics must be provided to the public as it pertained to Section 106, Section 305, as well as Section 702 acquired information.*

FISA Section 106 requires advance authorization from the Attorney General before any information acquired through Title I electronic surveillance may be used in a criminal proceeding. This authorization from the Attorney General is defined to include authorization by the Acting Attorney General, Deputy Attorney General, or, upon designation by the Attorney General, the Assistant Attorney General for National Security. Section 106 also requires that if a government entity intends to introduce into evidence in any trial, hearing, or other proceeding, against an aggrieved person, information obtained or derived from electronic surveillance, it must notify the aggrieved person and the court. The aggrieved person is then entitled to seek suppression of the information. FISA Section 706 requires that any information acquired pursuant to Section 702 be treated as electronic surveillance under Title I, including for purposes of the use, notice, and suppression requirements under Section 106.

FISA Section 305 provides the same requirements for information acquired through Title III physical search (i.e., advance authorization, notice, and opportunity to suppress).

B. Statistics

The reauthorized FAA of 2017codified that certain statistics concerning criminal proceedings must be provided to the public pertaining to Sections 106 and 305, including Section 702-acquired information. Specifically, figure 13 provides that, in 2017, the Government filed notice of intent to use FISA-acquired information, pursuant to Section 106 or 305, in seven (7) separate criminal proceedings.

Figure 13: Table Regarding Number of Criminal Proceedings in which the Government Provided Notice of Its Intent to Use Cert FISA Information

FISA Sections 106 and 305	CY2017
The number of criminal proceedings in which the United States or a State or political subdivision thereof provided notice pursuant to Section 106 (including with respect to Section 702-acquired information) or Section 305 of the government's intent to enter into evidence or otherwise use or disclose any information obtained or derived from electronic surveillance, physical search, or Section 702 acquisition.	**7**

FISA Title IV – Use of Pen Register and Trap and Trace (PR/TT) Devices

A. FISA PR/TT Authority

FISA Title IV

→ *Commonly referred to as the "PR/TT" provision.*

→ *Bulk collection is prohibited.*

→ *Requires individual FISC order to use PR/TT device to capture dialing, routing, addressing, or signaling (DRAS) information.*

→ *Government request to use a PR/TT device on U.S. person target must be based on an investigation to protect against terrorism or clandestine intelligence activities and that investigation must not be based solely on the basis of activities protected by the First Amendment to the Constitution.*

Title IV of FISA authorizes the use of pen register and trap and trace (PR/TT) devices for foreign intelligence purposes. Title IV authorizes the government to use a PR/TT device to seek and capture dialing, routing, addressing or signaling (DRAS) information. The government may submit an application to the FISC for an order approving the use of a PR/TT device (i.e., PR/TT order) for (i) "any investigation to obtain foreign intelligence information not concerning a United States person or" (ii) "to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution." 50 U.S.C. § 1842(a). If the FISC finds that the government's application sufficiently meets the requirements of FISA, the FISC must issue an order for the installation and use of a PR/TT device.

B. Statistics

Counting orders. Similar to how orders were counted for Titles I and III and Sections 703 and 704, this report only counts the orders *granting authority to conduct intelligence collection* -- the order for the installation and use of a PR/TT device. Thus, renewal orders are counted as a separate order; modification orders and amendments are not counted.

Estimating the number of targets. The government's methodology for counting PR/TT targets is similar to the methodology described above for counting targets of electronic surveillance and/or physical search. If the IC received authorization for the installation and use of a PR/TT device against the same target in four separate applications, the IC would count one target, not

four. Alternatively, if the IC received authorization for the installation and use of a PR/TT device against four targets in the same application, the IC would count four targets.

Estimating the number of unique identifiers. This statistic counts (1) the targeted identifiers and (2) the non-targeted identifiers (e.g., telephone numbers and e-mail addresses) that were in contact with the targeted identifiers. Specifically, the House Report on the USA FREEDOM Act states that "[t]he phrase 'unique identifiers used to communicate information collected pursuant to such orders' means the total number of, for example, email addresses or phone numbers that have been collected as a result of these particular types of FISA orders--not just the number of target email addresses or phone numbers." [H.R. Rept. 114-109 Part I, p. 26], with certain exceptions noted.

Figure 14: Table of PR/TT Orders, Targets, and Unique Identifiers Collected

Title IV of FISA ***PR/TT FISA***	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of orders	131	135	90	60	**33**
Estimated number of targets of such orders	319	516	456	41	**27**
Estimated number of unique identifiers used to communicate information collected pursuant to such orders*	-	-	134,987#	81,035#†	**56,064#**

See 50 U.S.C. §§ 1873(b)(3), 1873(b)(3)(A), and 1873(b)(3)(B).

* Pursuant to §1873(d)(2)(B), this statistic does not apply to orders resulting in the acquisition of information by the FBI that does not include electronic mail addresses or telephone numbers.

This number represents information the government received from provider(s) electronically for the entire calendar year. The government does not have a process for capturing unique identifiers received by other means (such as hard-copy or portable media).

† Last year, the FBI mistakenly interchanged the number of unique identifiers for business records and PR/TT orders, reporting the number of business records unique identifiers as PR/TT unique identifiers and vice versa. This report corrects the error and accurately identifies the legal authority under which the FBI obtained the unique identifiers.

Figure 15: Table of FISA PR/TT Targets – U.S. Persons and Non-U.S. Persons*

PR/TT Targets	CY2016	CY2017
Estimated number of targets who are *non*-U.S. persons	23	**16**
Estimated number of targets who are U.S. persons	18	**11**
Estimated percentage of targets who are U.S. persons	43.9%	**40.7%**

See 50 U.S.C. §§1873(b)(3)(A)(i) and 1873(b)(3)(A)(ii) for rows one and two, respectively.

* Previously the IC was not statutorily required to publicly provide these statistics, but provided them consistent with transparency principles. The reauthorized FAA of 2017 codified this requirement at 50 U.S.C. §§ 1873(b)(3)(A)(i) and 1873(b)(3)(A)(ii).

FISA Title V – Business Records

A. Business Records FISA

Under FISA, Title V authorizes the government to submit an application for an order requiring the production of any tangible things for (i) "an investigation to obtain foreign intelligence information not concerning a United States person or" (ii) "to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution." 50 U.S.C. § 1861. Title V is commonly referred to as the *"Business Records"* provision of FISA.

FISA Title V

→ *Commonly referred to as "Business Records" provision.*

→ *Bulk collection is prohibited.*

→ *Call Detail Records (CDRs) may be obtained from a telephone company if the FISC issues an individual court order for target's records.*

→ *Request for records in an investigation of a U.S. person must be based on an investigation to protect against terrorism or clandestine intelligence activities and provided that the investigation is not conducted solely upon activities protected by the First Amendment to the Constitution.*

In June 2015, the USA FREEDOM Act was signed into law and, among other things, it amended Title V, including by prohibiting bulk collection. *See* 50 U.S.C. §§ 1861(b), 1861(k)(4). The DNI is required to report various statistics about two Title V provisions – traditional business records and call detail records (discussed further below). On November 28, 2015, in compliance with amendments enacted by the USA FREEDOM Act, the IC terminated collection of bulk telephony metadata under Title V of the FISA (the "Section 215 Program"). Solely due to legal obligations to preserve records in certain pending civil litigation, including *First Unitarian Church of Los Angeles, et al. v. National Security Agency, et al.*, No. C 13-03287-JSW (N.D. Cal.) and *Jewel, et al. v. National Security Agency, et al.*, No. C 08-04373-JSW (N.D. Cal.), the IC continues to preserve previously collected bulk telephony metadata. Under the terms of a FISC order dated November 24, 2015, the bulk telephony metadata cannot be used or accessed for any purpose other than compliance with preservation obligations. Once the government's preservation obligations are lifted, the government is required to promptly destroy all bulk metadata produced by telecommunications providers under the Section 215 Program.

As noted in last year's *Annual Statistical Transparency Report*, on November 30, 2015, the IC implemented certain provisions of the USA FREEDOM Act, including the call detail records provision and the requirement to use a specific selection term. Accordingly, only one month's worth of data for calendar year 2015 was available with respect to those provisions. Any statistical information relating to a particular FISA authority for a particular month remains classified. Therefore, the Title V data specifically associated with December 2015 was only released in a classified annex provided to Congress as part of the report for CY2015. For the CY 2016 report, statistical information was collected for an entire year under the USA FREEDOM Act Title V provisions. As a result, those statistics were included in that report. For the CY 2017 report, statistical information was collected for an entire year under the USA FREEDOM Act Title V provisions. As a result, those statistics are included in this report.

Statistics related to *traditional business records* under Title V Section 501(b)(2)(B) are provided first pursuant to 50 U.S.C. § 1873(b)(5). Statistics related to *call detail records* under Title V Section 501(b)(2)(C) are provided second pursuant to 50 U.S.C. § 1873(b)(6).

B. Statistics – "Traditional" Business Records Statistics Orders, Targets & Identifiers

Business Record (BR) requests for tangible things include books, records, papers, documents, and other items pursuant to 50 U.S.C. §1861(b)(2)(B), also referred to as Section 501(b)(2)(B) . These are commonly referred to as "Traditional" Business Records.

Estimating the number of unique identifiers. This is an estimate of the number of (1) targeted identifiers (e.g., telephone numbers and email addresses) and (2) non-targeted identifiers that were in contact with the targeted identifiers. This metric represents unique identifiers received electronically from the provider(s). The government does not have a process for capturing unique identifiers received by other means (i.e., hard-copy or portable media).

Explaining how we count BR statistics. As an example of the government's methodology, assume that in 2017, the government submitted a BR request targeting "John Doe" with email addresses john.doe@serviceproviderX, john.doe@serviceproviderY, and john.doe@serviceproviderZ. The FISC found that the application met the requirements of Title V and issued orders granting the application and directing service providers X, Y, and Z to produce business records pursuant to Section 501(b)(2)(B). Provider X returned 10 non-targeted email addresses that were in contact with the target; provider Y returned 10 non-targeted email addresses that were in contact with the target; and provider Z returned 10 non-targeted email addresses that were in contact with the target. Based on this scenario, we would report the following statistics: A) one order by the FISC for the production of tangible things, B)

one target of said orders, and C) 33 unique identifiers, representing three targeted email addresses plus 30 non-targeted email addresses.

Figure 16: Table of "Traditional" Business Records Orders, Targets, and Unique Identifiers Collected

Business Records "BR" – Section 501(b)(2)(B)	CY2016	CY2017
Total number of orders issued pursuant to applications under Section 501(b)(2)(B)	84	**77**
Estimated number of targets of such orders	88	**74**
Estimated number of unique identifiers used to communicate information collected pursuant to such orders	125,354†	**87,834**

See 50 U.S.C. §§ 1873(b)(5), 1873(b)(5)(A), and 1873(b)(5)(B).

† Last year, the FBI mistakenly interchanged the number of unique identifiers for business records and PR/TT orders, reporting the number of business records unique identifiers as PR/TT unique identifiers and vice versa. This report corrects the error and accurately identifies the legal authority under which the FBI obtained the unique identifiers.

C. Statistics – Call Detail Record (CDR) Orders, Targets & Identifiers

Call Detail Records (CDRs) – commonly referred to as "call event metadata" – may be obtained from traditional telecommunications providers pursuant to 50 U.S.C. §1861(b)(2)(C). A CDR is defined as session identifying information (such as originating or terminating telephone number, an International Mobile Subscriber Identity (IMSI) number, or an International Mobile Station Equipment Identity (IMEI) number), a telephone calling card number, or the time or duration of a call. *See* 50 U.S.C. §1861(k)(3)(A). CDRs provided to the government do not include the content of any communication, the name, address, or financial information of a subscriber or customer, or cell site location or global positioning system information. *See* 50 U.S.C. §1861(k)(3)(B). CDRs are stored and queried by the service providers. *See* 50 U.S.C. §1861(c)(2).

Estimating the number of targets of CDR orders. A "target" is the person using the selector. For example, if a target uses four selectors that have been approved, the number counted for purposes of this report would be one target, not four. Alternatively, if two targets are using one selector that has been approved, the number counted would be two targets.

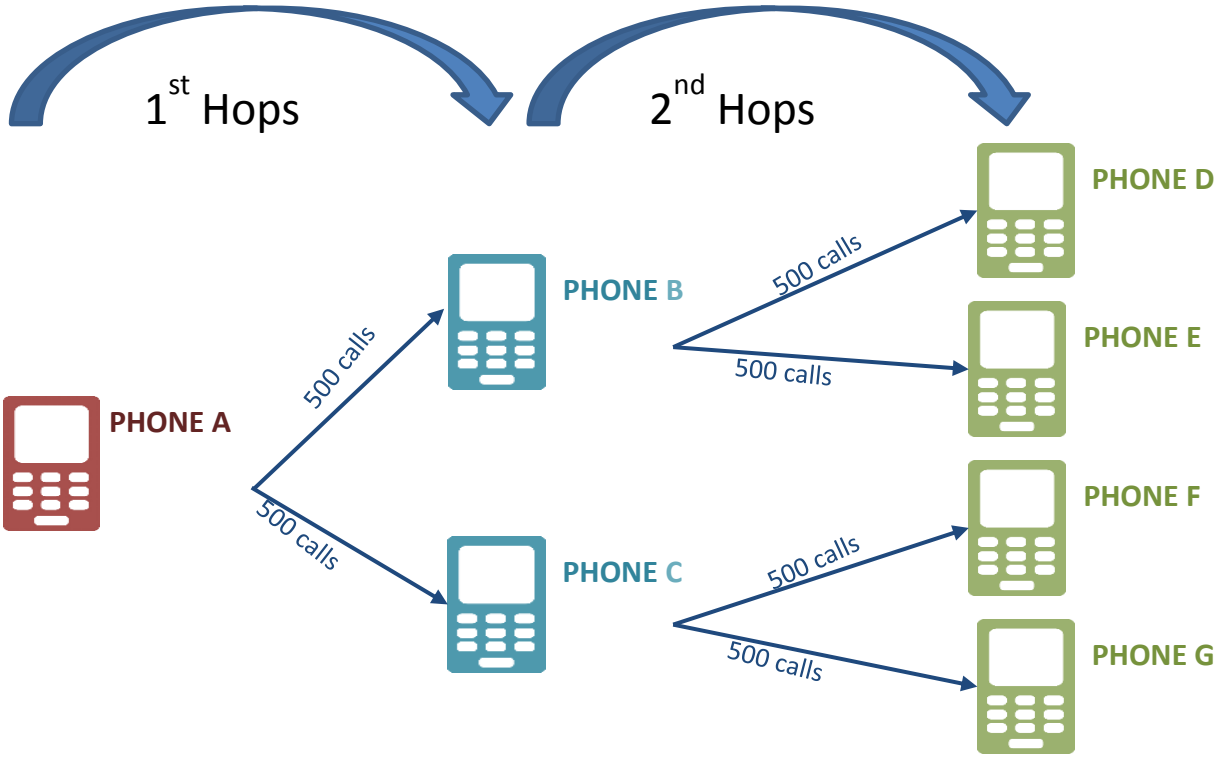
Figure 17: Table of CDR Orders and Targets

Call Detail Records "CDRs" – Section 501(b)(2)(C)	CY2016	CY2017
Total number of orders issued pursuant to applications under Section 501(b)(2)(C)	40	**40**
Estimated number of targets of such orders	42	**40**

See 50 U.S.C. §§ 1873(b)(6) and 1873(b)(6)(A).

The estimated number of Call Detail Records received from providers. This metric represents the number of *records received* from the provider(s) and stored in NSA repositories (records that fail at any of a variety of validation steps are not included in this number). CDRs covered by § 501(b)(2)(C) include call detail records created before, on, or after the date of the application relating to an authorized investigation. While the USA FREEDOM Act directs the government to provide a good faith estimate of "the number of unique identifiers used to communicate information collected pursuant to" orders issued in response to CDR applications (*see* 50 U.S.C. § 1873(b)(5)(B)), the statistic below does *not* reflect the number of unique identifiers contained within the call detail records received from the providers. As of the date of this report, the government does not have the technical ability to isolate the number of unique identifiers within records received from the providers. As explained in the 2016 NSA public report on the USA FREEDOM Act, the metric provided is over-inclusive because the government counts each record *separately even if the government receives the same record multiple times* (whether from one provider or multiple providers). Additionally, this metric includes duplicates of unique identifiers – i.e., because the government lacks the technical ability to isolate unique identifiers, the statistic counts the number of records even if unique identifiers are repeated. For example, if one unique identifier is associated with multiple calls to a second unique identifier, it will be counted multiple times. Similarly, if two different providers submit records showing the same two unique identifiers in contact, then those would also be counted. This statistic includes records that were received from the providers in CY2017 for all orders active for any portion of the year, which includes orders that the FISC approved in 2016. Furthermore, while the records are received from domestic communications service providers, the records received are for domestic and foreign numbers. More information on how NSA implements this authority can be found in the DCLPO report, in particular *see* page 5 for a description and illustration of the USA FREEDOM Implementation Architecture.

Figure 18: Illustration of a hop scenario and counting



Target uses Phone A which is the FISC-approved selector in the FISC order. This would count as **1 order, 1 target**, **7 unique identifiers** (phones A, B, C, D, E, F, G) and, assuming 500 calls between parties, **6000 CDRs** (*produced for both sides of a call event).

Assume an NSA intelligence analyst learns that phone number (**Phone A**) is being used by a suspected international terrorist (target). **Phone A** is the "specific selection term" or "selector" that will be submitted to the FISC (or the Attorney General in an emergency) for approval using the "reasonable articulable suspicion" (RAS) standard. Assume that one provider (provider X) submits a record showing **Phone A** called unique identifier **Phone B** – what is referred to as a "call event." This is the **"first hop."** In turn, assume that NSA submits the "first-hop" Phone B to the provider X, and finds that unique identifier was used to call another unique identifier **Phone D**. This is the **"second-hop."** If the unique identifiers call one another multiple times, then multiple CDRs are produced and duplication occurs. Additionally, the government may receive multiple CDRs for a single call event. NSA may also submit the specific selection Phone A number to another provider (provider Y) who may have CDRs of the same call events.

Not all CDRs provided to the government will be domestic numbers. The targeted "specific selection term" could be a foreign number, could have called a foreign number or the "first-

hop" number could have called a foreign number; thus, these CDRs statistics contain both domestic and foreign number results.

Figure 19: Table of CDRs Received Arising from Such Targets

Call Detail Records "CDRs" – Section 501(b)(2)(C)	CY2016	CY2017
Estimated number of call detail records arising from such targets that NSA received from providers pursuant to Section 501(b)(2)(C) and stored in its repositories*	151,230,968	**534,396,285**

* While the statute directs the government to count the unique identifiers, the government is not technically able to isolate the number of unique identifiers; thus, this number includes duplicate records. Additionally, the number of records contains both domestic and foreign numbers.

D. Statistics – Call Detail Record Queries

The number of search terms associated with a U.S. person used to query the CDR data. Each unique query is counted only once. The same term queried 10 times counts as one query term. A single query with 20 terms counts as 20 query terms.

Figure 20: Table of CDRs -- U.S. person query terms

Call Detail Records "CDRs" – Section 501(b)(2)(C)	CY2016	CY2017
Estimated number of search terms that included information concerning a U.S. person that were used to query any database of call detail records obtained through the use of such orders*	22,360	**31,196**

See 50 U.S.C. § 1873(b)(6)(C).

* Consistent with § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

National Security Letters (NSLs)

A. National Security Letters

In addition to statistics relating to FISA authorities, we are reporting information on the government's use of National Security Letters (NSLs). The FBI is statutorily authorized to issue NSLs for specific records (as specified below) only if the information being sought is relevant to a national security investigation. NSLs may be issued for four commonly used types of records:

National Security Letters

→ *Not authorized by FISA but by other statutes.*

→ *Bulk collection is prohibited, however, by the USA FREEDOM Act.*

→ *FBI may only use NSLs if the information sought is relevant to international counterterrorism or counterintelligence investigation.*

1) telephone subscriber information, toll records, and other electronic communication transactional records, see 18 U.S.C. § 2709;
2) consumer-identifying information possessed by consumer reporting agencies (names, addresses, places of employment, institutions at which a consumer has maintained an account), see 15 U.S.C. § 1681u;
3) full credit reports, see 15 U.S.C. § 1681v (only for counterterrorism, not for counterintelligence investigations); and
4) financial records, see 12 U.S.C. § 3414.

B. Statistics – National Security Letters and Requests of Information

Counting NSLs. Today we are reporting (1) the total number of NSLs *issued* for all persons, and (2) the total number of requests for information (ROI) contained within those NSLs. When a single NSL contains multiple ROIs, each is considered a "request" and each request must be relevant to the same pending investigation. For example, if the government issued one NSL seeking subscriber information from one provider and that NSL identified three e-mail addresses for the provider to return records, this would count as one NSL issued and three ROIs.

- **The Department of Justice's Report on NSLs.** In May 2018, the Department of Justice released its *Annual Foreign Intelligence Surveillance Act Report* to Congress. That report, which is available online, provides the *number of requests* made for certain information concerning different U.S. persons pursuant to NSL authorities during calendar year 2017. The Department of Justice's report provides the number of individuals subject to an NSL whereas the ODNI's report provides the number of NSLs issued. Because one person may be subject to more than one NSL in an annual period, the number of NSLs issued and the number of persons subject to an NSL differs.

Why we report the number of NSL requests instead of the number of NSL targets. We are reporting the annual number of requests for multiple reasons. First, the FBI's systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of a facility. In other cases, this occurs because individual subscribers may identify themselves differently for each account (e.g., inclusion of middle name, middle initial, etc.) when creating an account.

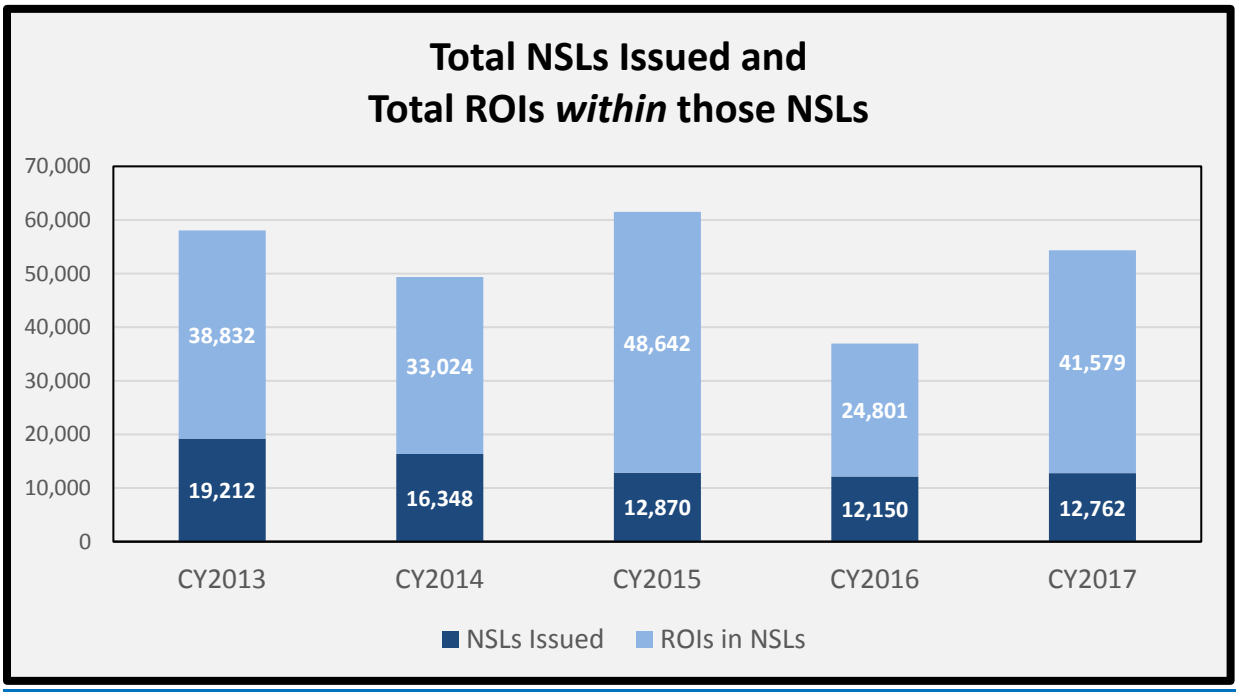
We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities (e.g., multiple e-mail accounts, landline telephone numbers and cellular phone numbers). The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

Figure 21a: Table of NSLs Issued and Requests for Information

National Security Letters (NSLs)	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of NSLs issued	19,212	16,348	12,870	12,150	**12,762**
Number of Requests for Information (ROI)	38,832	33,024	48,642	24,801	**41,579**

See 50 U.S.C. § 1873(b)(6).

Figure 21b: Chart of NSLs Issued and Requests for Information



APPENDIX

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

MAY 0 4 2018

The Honorable Richard Burr
Chairman
Select Committee on Intelligence
United States Senate

The Honorable Chuck Grassley
Chairman
Committee on the Judiciary
United States Senate

The Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence
U.S. House of Representatives

The Honorable Robert W. Goodlatte
Chairman
Committee on the Judiciary
U.S. House of Representatives

Dear Messrs. Chairmen:

Section 603(b)(2)(B) of the Foreign Intelligence Surveillance Act (FISA), as amended by the *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, (P.L.114-23), 129 Stat. 268 (hereinafter USA FREEDOM Act), requires the Director of National Intelligence (DNI) to make publicly available for the preceding 12-month period a good faith estimate of the number of queries concerning a known United States person of unminimized non-content information relating to electronic communications or wire communications obtained through acquisitions authorized under Section 702 of FISA, excluding the number of queries containing information used to prevent the return of information concerning a United States person.

If the DNI concludes that this good faith estimate cannot be determined accurately because not all of the relevant elements of the Intelligence Community (IC) are able to provide this good faith estimate, then FISA requires him to (i) certify that conclusion in writing to the committees identified above; (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate; (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and (iv) make such certification publicly available on an Internet website.

I conclude that the good faith estimate required under section 603(b)(2)(B) of FISA cannot be determined accurately because not all of the relevant elements of the IC are able to provide this good faith estimate. Specifically, the Central Intelligence Agency (CIA) remained unable to provide such information for calendar year 2017. The enclosed report includes the good faith estimate for those relevant IC elements that were able to provide such good faith estimate. Based on the information provided to me by the CIA, I reasonably anticipate that such an estimate will be able to be determined fully and accurately by the end of calendar year 2018 so as to be included in the 2019 report.

The Honorable Richard Burr
The Honorable Chuck Grassley
The Honorable Devin Nunes
The Honorable Robert W. Goodlatte

If you have any questions regarding this matter, please contact the Office of the Director of National Intelligence Office of Legislative Affairs at (703) 275-2474.

Sincerely,

Daniel R. Coats

Enclosure:
Statistical Transparency Report

cc: Executive Secretary, National Security Staff
Director, Central Intelligence Agency
Under Secretary of Defense for Intelligence
Under Secretary for Intelligence and Analysis, Department of Homeland Security
Director, National Security Agency
Director, National Reconnaissance Office
Director, Defense Intelligence Agency
Director, National Geospatial-Intelligence Agency
Assistant Secretary for Intelligence and Research, Department of State
Assistant Secretary for Intelligence and Analysis, Department of the Treasury
Executive Assistance Director, Intelligence Branch, Federal Bureau of Investigation
Chief of Intelligence, Senior Officer, Drug Enforcement Administration
Director, Office of Intelligence and Counterintelligence, Department of Energy
Deputy Chief of Staff, G2, U.S. Army
Director of Intelligence, U.S. Marine Corps
Director of Naval Intelligence, N2 U.S. Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, A2, U.S. Air Force
Deputy Chief of Staff for Intelligence and Criminal Investigations, U.S. Coast Guard
Assistant Attorney General for National Security, Department of Justice

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix Z

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, INC. Plaintiff, v. NATIONAL SECURITY AGENCY, et al., Defendants.	Civil Action No. 1:15-cv-00662-TSE Hon. T.S. Ellis, III

WIKIMEDIA FOUNDATION, INC.'S RESPONSES AND OBJECTIONS TO NATIONAL SECURITY AGENCY'S FIRST SET OF INTERROGATORIES

PROPOUNDING PARTY: **NATIONAL SECURITY AGENCY**

RESPONDING PARTY: **WIKIMEDIA FOUNDATION, INC.**

SET NUMBER: **ONE**

Pursuant to Federal Rule of Civil Procedure 33, Plaintiff Wikimedia Foundation, Inc. ("Plaintiff" or "Wikimedia") responds as follows to Defendant National Security Agency's ("Defendant" or "NSA") (collectively with Plaintiff, the "Parties") First Set of Interrogatories (the "Interrogatories"):

I. GENERAL RESPONSES.

1. Plaintiff's response to Defendant's Interrogatories is made to the best of Plaintiff's present knowledge, information, and belief. Discovery in this action is ongoing, and Plaintiff's responses may be substantially altered by further investigation, including further review of Plaintiff's own documents, as well as the review of documents produced by Defendant, which Plaintiff has just begun to receive. Said response is at all times subject to such additional or different information that discovery or further investigation may disclose and, while based on the

present state of Plaintiff's recollection, is subject to such refreshing of recollection, and such additional knowledge of facts, as may result from Plaintiff's further discovery or investigation.

2. Plaintiff reserves the right to make any use of, or to introduce at any hearing and at trial, information and/or documents responsive to Defendant's Interrogatories but discovered subsequent to the date of this response, including, but not limited to, any such information or documents obtained in discovery herein.

3. To the extent that Plaintiff responds to Defendant's Interrogatories by stating that Plaintiff will provide information and/or documents that Plaintiff deems to embody material that is private, business confidential, proprietary, trade secret, or otherwise protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7), Federal Rule of Evidence 501, or other applicable law, Plaintiff will do so only pursuant to the Parties' Stipulated Protective Order (ECF No. 120).

4. Plaintiff reserves all objections or other questions as to the competency, relevance, materiality, privilege, or admissibility as evidence in any subsequent proceeding in or trial of this or any other action for any purpose whatsoever of Plaintiff's responses herein and any document or thing identified or provided in response to Defendant's Interrogatories.

5. Plaintiff's responses will be subject to and limited by any agreements the Parties reach concerning the scope of discovery.

6. Plaintiff reserves the right to object on any ground at any time to such other or supplemental interrogatories as Defendant may at any time propound involving or relating to the subject matter of these Interrogatories.

II. GENERAL OBJECTIONS.

Plaintiff makes the following general objections, whether or not separately set forth in

response to each Interrogatory, to each instruction, definition, and Interrogatory made in Defendant's Interrogatories:

1. Plaintiff objects to the Interrogatories in their entirety insofar as any such instruction, definition, or Interrogatory seeks information or production of documents protected by the attorney-client privilege or the work product doctrine. Fed. R. Civ. Proc. 26(b)(1). Such information or documents shall not be provided in response to Defendant's Interrogatories and any inadvertent disclosure or production thereof shall not be deemed a waiver of any privilege with respect to such information or documents or of any work product immunity which may attach thereto. Fed. R. Civ. Proc. 26(b)(5)(B).

2. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks identification of documents, witnesses, or information that Defendant has withheld from Plaintiff. Fed. R. Civ. Proc. 26(b)(1), (2).

3. Plaintiff objects to the Interrogatories in their entirety to the extent any such Interrogatory requires Plaintiff to identify potentially thousands of pages of documents, not all of which have been or can be located and reviewed by counsel within the time period allowed for this response or within a reasonable time. Accordingly, said Interrogatories would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense.

4. Plaintiff objects to any Interrogatories that exceed the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and ordered by the Court.

5. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information that is available through or from public sources or records, or that are otherwise equally available to Defendant, on the ground that such instructions, definitions, and/or Interrogatories unreasonably subject Plaintiff to undue annoyance,

oppression, burden, and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

6. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory purport to impose obligations that are greater or more burdensome than or contradict those imposed by the applicable Federal and local rules. *See* Fed. R. Civ. Proc. 26, 33.

7. Plaintiff objects to the Interrogatories in their entirety as the Interrogatories contain more than the "25 written interrogatories, including all discrete subparts," permitted by the Federal Rules of Civil Procedure, Rule 33(a)(1), and Defendant has not sought leave to serve additional interrogatories.

8. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks documents or information no longer in existence or not currently in Plaintiff's possession, custody, or control, or to the extent they refer to persons, entities, or events not known to Plaintiff or controlled by Plaintiff, on the grounds that such definitions or Interrogatories are overly broad, seek to require more of Plaintiff than any obligation imposed by law, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would seek to impose upon Plaintiff an obligation to investigate, discover, or produce information or materials from third parties or otherwise that are accessible to Defendant or readily obtainable from public or other sources. Fed. R. Civ. Proc. 26(b)(1), (2).

9. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information or production of documents protected from disclosure by any right to privacy or any other applicable privilege or protection, including the right to confidentiality or privacy of third parties, any right of confidentiality provided for by Plaintiff's contracts or agreements with such third parties, or by Plaintiff's obligations under

applicable law or contract to protect such confidential information. Plaintiff reserves the right to withhold any responsive information or documents governed by a third-party confidentiality agreement until such time as the appropriate notice can be given or the appropriate permissions can be obtained. Plaintiff also objects generally to all instructions, definitions, or Interrogatories to the extent they seek disclosure of trade secrets and other confidential research or analyses, development, or commercial information of Plaintiff or any third party.

10. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory is overbroad and unduly burdensome, particularly to the extent they seek "all," "each," or "any" documents, witnesses or facts relating to various subject matters. Fed. R. Civ. Proc. 26(b)(1), (2). To the extent Plaintiff responds to such Interrogatories, Plaintiff will use reasonable diligence to identify responsive documents, witnesses or facts in its possession, custody, or control, based on its present knowledge, information, and belief.

11. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks expert discovery prematurely.

12. Plaintiff objects to any contention Interrogatories in their entirety as premature. Plaintiff will provide its response prior to the close of fact discovery.

13. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory purports to require Plaintiff to restore and/or search data sources that are not reasonably accessible on the grounds that such definitions and Interrogatories would subject Plaintiff to undue burden and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

III. DEFINITIONAL OBJECTIONS.

1. Plaintiff objects to definition number one (1) to the extent it defines "Plaintiff" and "Wikimedia" to include Plaintiff's "parent, subsidiary, and affiliated organizations, and all persons

acting on their behalf, including officials, agents, employees, attorneys, and consultants." Said definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside of Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Said definition is also vague and ambiguous in that it cannot be determined what is meant by the terms "affiliated organizations" and "all persons acting on their behalf." Plaintiff shall construe "Plaintiff" and "Wikimedia" to mean Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to definition number four (4) and to each Interrogatory that purports to require Plaintiff to "state the basis of," "stating the basis of," "state on what basis," or otherwise "state with particularity" or "identify" "all" facts, documents, or persons whose testimony support or dispute any given factual assertion, on the ground that any response thereto would require subjective judgment on the part of Plaintiff and its attorneys, and would further require disclosure of a conclusion or opinion of counsel in violation of the attorney work product doctrine and/or attorney-client privilege. Plaintiff further objects that this definition and all requests to identify documents in the Interrogatories are premature at this early stage of the litigation, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would impose an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

3. Plaintiff objects to definition number five (5) as unduly burdensome in that it purports to require Plaintiff to "identify" each "natural person" by providing information including "her most current home and business addresses, telephone numbers, and e-mail addresses, the name of her current employer, and her title."

4. Plaintiff objects to definition number six (6) as unduly burdensome in that it purports to require Plaintiff to "identify" an "entity that is not a natural person" by providing information including "its telephone number and e-mail address, and the full names, business addresses, telephone numbers, and e-mail addresses of both its chief executive officer and an agent designated by it to receive service of process."

5. Plaintiff objects to definition number seven (7) as unduly burdensome in that it purports to require Plaintiff to "identify" documents by providing "(a) the nature of the document (*i.e*, letter, memorandum, spreadsheet, database, etc.); (b) its date; (c) its author(s) (including title(s) or position(s)); (d) its recipient(s) (including title(s) or position(s)); (e) its number of pages or size; and (f) its subject matter," or by providing information in accordance with Defendant's "Specifications for Production of ESI and Digitized ('Scanned') Images attached to Defendant National Security Agency's First Set of Requests for Production." Plaintiff further objects that this definition and all requests to identify documents in the Interrogatories are premature at this early stage of the litigation, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would impose an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

IV. INSTRUCTIONAL OBJECTIONS

1. Plaintiff objects to instruction number one (1) to the extent it purports to request "knowledge or information" from Wikimedia's "parent, subsidiary, or affiliated organizations, and their officials, agents, employees, attorneys, consultants, and any other person acting on their behalf." Said request is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and

expense. Moreover, said request is vague and ambiguous in that it cannot be determined what is meant by the term "affiliated organizations" and "any other person acting on their behalf." Where an Interrogatory requests knowledge or information of Plaintiff, Plaintiff shall construe such request to mean knowledge or information from Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to instruction number three (3) as unduly burdensome and imposing an obligation to provide information greater than that required by the Federal Rules of Civil Procedure to the extent it purports to require Plaintiff to "identify each person known by Plaintiff to have such knowledge, and in each instance where Plaintiff avers insufficient knowledge or information as a grounds for not providing information or for providing only a portion of the information requested, set forth a description of the efforts made to locate information needed to answer the interrogatory."

3. Plaintiff objects to instruction number four (4) to the extent it seeks to require it to identify anything other than the specific claim of privilege or work product being made and the basis for such claim, and to the extent it seeks to require any information not specified in Discovery Guideline 10, on the grounds that the additional information sought by Defendant would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and constitutes information protected from discovery by privilege and as work product. Plaintiff is willing to discuss acceptable reciprocal obligations for disclosure of information withheld on the basis of attorney-client privilege or attorney work-product.

4. Plaintiff objects to instruction number five (5) to the extent it defines "the time period for which each interrogatory seeks a response" as "the period from July 10, 2008 (the date of enactment of the FISA Amendments Act of 2008, Pub. L. 110-261, 121 Stat. 522) until the date

of Plaintiff's response." This definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Where appropriate, Plaintiff has defined the specific time period encompassed by specific responses.

5. Plaintiff objects to instruction number six (6) that the Interrogatories are continuing, to the extent said instruction seeks unilaterally to impose an obligation to provide supplemental information greater than that required by Federal Rule of Civil Procedure 26(e) and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Plaintiff will comply with the requirements of the Federal Rules of Civil Procedure and is willing to discuss mutually acceptable reciprocal obligations for continuing discovery.

V. SPECIFIC OBJECTIONS AND RESPONSES TO INTERROGATORIES.

Without waiving or limiting in any manner any of the foregoing General Objections, Definitional Objections, or Instructional Objections, but rather incorporating them into each of the following responses to the extent applicable, Plaintiff responds to the specific Interrogatories in Defendant's Interrogatories as follows:

ALLEGED NSA INTERCEPTION OF SUBSTANTIALLY ALL INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS

INTERROGATORY NO. 1:

Notwithstanding the holding of the Court of Appeals in this case that "Plaintiffs lack standing to sue … under the Dragnet Allegation because they can't plausibly show that the NSA is intercepting their communications via a dragnet," Wikimedia Found. v. NSA, 857 F.3d 193, 216 (4th Cir. 2017), does Plaintiff still contend, for the purpose of establishing jurisdiction, that NSA Upstream surveillance involves the interception, copying, and review (as those terms are used in paragraph 56 of the Amended Complaint) of all or substantially all international Internet text-based

communications?

RESPONSE TO INTERROGATORY NO. 1:

In addition to the General Objections above which are incorporated herein, Plaintiff also objects that this Interrogatory seeks a statement of Plaintiff's legal strategy or information that is protected by the attorney-client privilege or the attorney work product doctrine. Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows: Yes.

INTERROGATORY NO. 2:

Unless Plaintiff's response to Interrogatory No. 1, above, is an unequivocal "no," then please state the basis of Plaintiff's contention that NSA Upstream surveillance involves the interception, copying, and review of all or substantially all international Internet text-based communications, including, but not limited to, the contentions that "Upstream surveillance is intended to enable the comprehensive monitoring of international internet traffic," see Amended Complaint ¶ 48; that "the NSA is temporarily copying and then sifting through the contents of what is apparently most e mails and other text-based communications that cross the border," see id. ¶ 69; that "it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data," see Pl.'s Opp. to Defs.' MTD at 18-19; and that the U.S. Government "has acknowledged … that the NSA … examines the full contents of essentially everyone's communications to determine whether they include references to the NSA's search terms," *see id*. at 10.

RESPONSE TO INTERROGATORY NO. 2:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff further submits that these matters may be the subject of expert testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff additionally objects that this Interrogatory is improperly compound in that it contains multiple subparts.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases for Plaintiff's contention include the following:

- Basic principles underlying how Internet communications are transmitted and how surveillance on a packet-switched network operates.
- Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (2014) ("PCLOB Report"), including pages 7–10, 12–13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica (June 4, 2015) (and associated documents)

- Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 (and associated documents)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)
- Charlie Savage, *Power Wars* (2015)

Additionally, Plaintiff's contention is based on the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted

selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

The fact that all or substantially all international Internet text-based communications are subject to Upstream surveillance follows necessarily from the information the government has officially disclosed, and it is corroborated by independent news reports. For Upstream surveillance to serve the purposes the government has said it serves, the NSA must be comprehensively monitoring text-based communications originating or terminating in the United States. This is the only way for the NSA to reliably obtain communications to, from, and about its thousands of targets around the world, because those communications travel along paths in and out of the country that are unpredictable and change over time. Moreover, the structure of the Internet backbone facilitates such comprehensive surveillance. Because international communications are channeled through a small number of Internet chokepoints—and because the NSA's own documents show that it is conducting Upstream surveillance at many of those chokepoints—it is straightforward for the government to conduct the comprehensive surveillance necessary for Upstream to function as described.

The government's descriptions of Upstream surveillance make clear that the government is interested in obtaining, with a high degree of confidence, all international communications to, from, and about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to *comprehensively* acquire communications that are sent to or from its targets." PCLOB Report 10 (emphasis added). And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can reliably acquire data packets associated with the proper communications." *Id.* at 143 (emphasis

added).

Because the routing of Internet traffic is unpredictable, however, the government can only "comprehensively" and "reliably" obtain communications to, from, and about its thousands of targets by conducting its surveillance on the different routes by which Internet communications enter and leave the country, and by examining substantially all international communications that travel those various routes.

The path that an Internet communication takes is inherently unpredictable. Internet communications are routed around the globe based on a complex set of rules and relationships that are applied dynamically, based on network conditions at any given moment. These network conditions change frequently, and so one cannot know in advance which path a particular communication will travel. Indeed, even the communications between two individuals in a single conversation (such as an Internet chat or email exchange) may take entirely different routes across the Internet backbone, even though the end-points are the same. For example, if an NSA target is having an Internet chat conversation with someone in the United States, the communications *from* the target will frequently follow a different path than those *to* the target. And, of course, a target's location may vary over time. For all these reasons, a target's communications may traverse one Internet circuit at one moment, but a different one later.

The fact that the NSA had, at last public count, 106,469 surveillance targets (some of which are groups with perhaps hundreds or even thousands of members) only reinforces the conclusion that Upstream surveillance of international text-based communications must be comprehensive. *See* ODNI, Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016 (Apr. 2017), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016. The

communications of so many targets scattered around the world will travel many different routes across the Internet backbone, based on the locations of those various targets, their individual movements over time, and changes in network conditions. These communications will be intermingled with those of the general population in the flow of Internet traffic. An intelligence agency that seeks to reliably intercept communications to, from, or about its targets, could do so only by searching substantially all text-based communications entering or leaving the country.

This allegation is based on the government's official disclosures and on necessary inferences from those disclosures, but it is also corroborated by news accounts. A *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi. The same *New York Times* report also explains why the NSA's Upstream surveillance is so far-reaching:

> "Computer scientists said that it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data; fiber-optic networks work by breaking messages into tiny packets that flow at the speed of light over different pathways to their shared destination, so they would need to be captured and reassembled."

Id.; see also Charlie Savage, *Power Wars* 207–11 (2015).

Not only does the NSA have an overriding incentive to copy and review substantially all international Internet communications, but the Internet backbone is structured in a way that enables it to do so.

The Internet backbone funnels almost all Internet communications entering and leaving the country through a limited number of chokepoints. The Internet backbone includes a relatively small number of international submarine cables (and a limited number of terrestrial cables) that transport Internet traffic into and out of the United States. Because there are relatively few high-capacity cables carrying international Internet communications, there are correspondingly few chokepoints—*i.e.*, junctions through which all international Internet communications must pass en route to their destinations. By installing its surveillance equipment at the small number of backbone chokepoints, the NSA is able to monitor substantially all text-based communications entering or leaving the United States. And the government has acknowledged that it conducts Upstream surveillance at international links and on the Internet backbone. [*Redacted*], 2011 WL 10945618, at *15; PCLOB Report 36–37.

NSA documents published in the press show that the NSA has installed surveillance equipment at many major chokepoints on the Internet backbone. One of these NSA documents states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *See* Plaintiff's First Amended Complaint ¶ 69. Another shows that just one of those participating providers has facilitated Upstream surveillance at seven major international chokepoints in the United States. *Id.* ¶ 68. Additional reporting states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents).

ALLEGED VOLUME AND GLOBAL DISTRIBUTION OF WIKIMEDIA'S INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS

INTERROGATORY NO. 3:

Please identify each category of Wikimedia international, text-based, Internet communications that Plaintiff contends, for purposes of establishing jurisdiction, is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, including but not limited to, user visits to Wikimedia sites; contributions and edits to Wikimedia websites; Wikimedia discussion forums; Wikimedia discussion pages; e mail sent via Wikimedia among registered users; communications "over wikis" among small or limited groups of users; mailing lists with restricted membership; other use of Wikimedia Projects, websites, and webpages by "community members" to interact with one another; internal log communications; "Community Consultations;" solicitations of user input and preferences; and other communications sent and received by Wikimedia staff in carrying out Wikimedia's work. *See* Amended Complaint ¶¶ 79, 84, 86, 92, 93, 102.

RESPONSE TO INTERROGATORY NO. 3:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows. As explained in Wikimedia's First Amended Complaint, Wikimedia contends that Upstream surveillance implicates at least three categories of communications (Am. Compl. ¶ 86): (1) Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other. Examples of these communications include, but are not limited to, page views to Wikimedia websites, edits and contributions to Wikimedia websites, emails between

registered Wikimedia users and emails on Wikimedia's mailing lists.

(2) Wikimedia's internal log communications.

(3) Electronic communications of Wikimedia staff. Examples of these communications include, but are not limited to, Gmail, Google chat, Internet Relay Chat, and Slack. Additionally, Wikimedia staff members use a variety of third-party tools to conduct their work, including, but not limited to, Google Apps/G Suite, Trello, Sugar, Qualtrics, User Testing and Salesforce.

INTERROGATORY NO. 4:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify the submarine or terrestrial cables entering or exiting the United States that have carried that category of Wikimedia communications in the past 24 months. To identify a submarine or terrestrial cable means to state its originating or terminating location in the United States, to state its terminating or originating location abroad, and to identify the person(s) owning or controlling it.

RESPONSE TO INTERROGATORY NO. 4:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad and unduly burdensome. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants and as ordered by the Court, and is not reasonably calculated to lead to the discovery of admissible evidence. Specifically, the categories of Plaintiff's communications subject to Upstream surveillance are not relevant to Plaintiff's standing. Plaintiff further objects that this Interrogatory seeks information that is within Defendants' control.

Plaintiff also objects that this Interrogatory is improperly compound in that it contains

multiple subparts. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

To a near certainty, Plaintiff's communications traverse all submarine and major terrestrial cables carrying public Internet data into and out of the United States. Publicly available data shows that submarine cables include those listed in Exhibit A. (Exhibit A was created in reliance on publicly available data that Plaintiff has not independently verified.)

INTERROGATORY NO. 5:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify the Internet circuits entering or exiting the United States that have carried that category of communication in the past 24 months. To identify a circuit means to state its location of entry to or exit from the United States, to state its country (or, if unknown, global region(s)) of origin or termination abroad, and to identify the person(s) owning or controlling it.

RESPONSE TO INTERROGATORY NO. 5:

In addition to the General Objections above which are incorporated herein, Plaintiff also objects that this Interrogatory is overbroad and unduly burdensome. Plaintiff further objects that this Interrogatory seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff further objects that this Interrogatory seeks information that is

within Defendants' control.

Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

On the basis of these General and Specific Objections, Plaintiff will not provide a response to this Interrogatory.

INTERROGATORY NO. 6:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify each foreign country to or from which such Wikimedia communications were sent in the past 24 months.

RESPONSE TO INTERROGATORY NO. 6:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, see ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. Between April 23, 2017

and December 31, 2017, Wikimedia's U.S. servers received HTTPS requests from, and transmitted HTTPS responses to, users in at least 242 non-U.S. countries, territories and regions. This figure is an estimate that was derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Every time Wikimedia receives an HTTPS request from a person accessing a Wikimedia Project webpage, it creates a corresponding log entry. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between January 1, 2015 and December 12, 2017, Wikimedia's office network router located in the United States sent Internet communications to at least approximately 221 non-U.S. countries, territories and regions.

This figure represents Internet outbound communications sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes communications sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally, who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of

Plaintiff's contractors located abroad will also be produced to Defendants.

INTERROGATORY NO. 7:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please state the total number of such Wikimedia communications made to and from the United States each year for the years 2008-2017, specifying in each case the manner in which Wikimedia counts the communications in that category (e.g., by site visit, page view, HTTP or HTTPS transmissions, e-mails, other forms of messaging, etc.).

RESPONSE TO INTERROGATORY NO. 7:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vastly overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, see ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received over 500 billion HTTPS requests from users outside of the United States. Each HTTPS request generates a corresponding response; thus Wikimedia exchanged over 1 trillion HTTPS requests and responses with its users between April 23, 2017 and December 31, 2017. These figures are estimates that were derived using MaxMind

geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States made at least approximately 22,934,372 Internet connections to 223 non-U.S. countries, territories and regions.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's contractors located abroad will also be produced to Defendants

INTERROGATORY NO. 8:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please state by foreign country the number of such Wikimedia communications made to or from the United States each year for the years 2008-2017, specifying in each case the manner in which Wikimedia counts the communications in that category (e.g., by site visit, page view, HTTP or HTTPS transmissions, e-mails, other forms of messaging, etc.).

RESPONSE TO INTERROGATORY NO. 8:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vastly overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. Plaintiff additionally objects to this Interrogatory as duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. The number of HTTPS requests that Wikimedia's U.S. servers received from users in each country, territory, or region between April 23, 2017 and December 31, 2017 is attached as Exhibit B and will be included in a forthcoming production to Defendants. Each HTTPS request generates a corresponding response

that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States sent at least approximately 22,934,372 Internet connections to at least 223 non-U.S. countries, territories and regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

These figures are estimates and were derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

These figures represent the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

These figures include connections sent through Wikimedia's Virtual Private Network (VPN).

These figures do not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia

engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's staff and contractors located abroad will also be produced to Defendants.

INTERROGATORY NO. 9:

Please identify the location, by (i) nation, (ii) state, province, or the equivalent, as applicable, and (iii) city, town, or county, as applicable, of each of Wikimedia's servers on which one or more of its "wiki"-based Projects and other related websites and pages (see Amended Complaint ¶ 78), is or since 2008 has been hosted, specifying which of Wikimedia's Projects, sites, or pages is hosted in whole or in part on each server.

RESPONSE TO INTERROGATORY NO. 9:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff additionally objects that this Interrogatory is impracticable in that it requests the identification of each webpage that has been hosted by a particular server. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects that the term "server" and the phrases "in whole or in part" are vague and ambiguous in the context of this Interrogatory. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The following is a list of the locations of each Wikimedia server on which one more of its

"wiki"-based Projects and other related websites and pages is or at some point in time between 2008 and the present has been hosted.

- United States
  - Ashburn, Virginia
  - Carrollton, Texas
  - Chicago, Illinois
  - Dallas, Texas
  - San Francisco, California
  - Tampa, Florida
- The Netherlands
  - Amsterdam, North Holland
  - Haarlem, North Holland
- South Korea
  - Seoul

For purposes of this response, Wikimedia construes the term "server" to mean any public facing Internet access point operated by Wikimedia.

The remainder of this Interrogatory calls for information that exceeds the scope of jurisdictional discovery and Plaintiff therefore will not provide a response at this time.

INTERROGATORY NO. 10:

Please state the number of "logs" or "log entries" (or, if not equivalent, both) contained in each "log communication" sent from Wikimedia servers abroad to Wikimedia servers in the United States, and the frequency with which such log communications are sent. *See* Amended Complaint ¶ 93.

RESPONSE TO INTERROGATORY NO. 10:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vague and ambiguous, overbroad, and not reasonably limited in time. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects to this Interrogatory as duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

One log or log entry is contained in a single communication. The frequency of log communications transmitted to Wikimedia's servers from outside of the United States is set forth in Plaintiff's response to Interrogatory No. 8.

INTERROGATORY NO. 11:

Please state the basis of Plaintiff's allegations, in paragraphs 61, 85, and 88 of the Amended Complaint, that Wikimedia's alleged "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia "communicate[s] with individuals in virtually every country on earth."

RESPONSE TO INTERROGATORY NO. 11:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants. Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Numerous facts support Wikimedia's allegations that its "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that

Wikimedia engages in "communications . . . with individuals in virtually every country on earth." As explained in Wikimedia's responses to NSA Interrogatory Nos. 6-8, Wikimedia users from all over the world read and contribute to Wikimedia's Project pages. This analysis is further supported by statistics showing that Wikimedia's Project pages are edited and viewed by millions of users around the world. Wikimedia publishes current monthly page view statistics by country (*available* at https://stats.wikimedia.org/wikimedia/squids/SquidReportPageViewsPerCountryOverview.htm), and maintains an archive with analogous data for past months (*available* at https://stats.wikimedia.org/archive/squid_reports/).

Wikimedia also has dozens of foreign independent but associated entities, including user groups, chapters and thematic organizations. *See* https://meta.wikimedia.org/wiki/Wikimedia_movement_affiliates#chapters.

In the last two years alone, Wikimedia has awarded grants and scholarships to users and programs in dozens of countries. Additionally, Wikimedia projects are currently active in 288 languages, further underscoring Wikimedia's global presence. *See* https://en.wikipedia.org/wiki/List_of_Wikipedias.

INTERROGATORY NO. 12:

Please state the basis of Plaintiff's allegation, in paragraph 61 of the Amended Complaint, that "Plaintiff['s] communications almost certainly traverse every international backbone link connecting the United States with the rest of the world," and the related contention that "Plaintiff['s] communications almost certainly traverse every major internet circuit connecting the United States with the rest of the world," see Pl.'s Opp. to Defs.' MTD at 23, including as part of the response a specification of what Plaintiff means by the term "link" and "circuit" and the

identification by location and ownership or control of each such international backbone link or circuit that Wikimedia communications allegedly traverse.

RESPONSE TO INTERROGATORY NO. 12:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's allegations are the scope and distribution of Plaintiff's international Internet communications.

According to the Foreign Intelligence Surveillance Court and the Privacy and Civil Liberties Oversight Board, Upstream surveillance is directed at "circuits" or "international Internet link[s]" on the Internet backbone. *See* PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of FISA 36–37 (2014) ("PCLOB Report"); [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). The NSA's Section 702 targeting procedures have similarly described how the NSA targets Internet "links." *See* Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (July 2009), *available at*

https://www.aclu.org/files/natsec/nsa/20130816/FAA%20Targeting%20Procedures.pdf.

Plaintiff's understanding is that a "circuit" or "link" is a pathway between devices in telecommunications networks. These circuits are carried on, for example, physical media such as cables and fibers, but there is not necessarily a one-to-one correspondence between each circuit and its underlying means of transmission. For example, multiple circuits may traverse a single fiber, and a single circuit may span multiple fibers.

ALLEGATIONS REGARDING NSA INTERCEPTION OF WIKIMEDIA'S INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS

INTERROGATORY NO. 13:

Please identify each of the international Internet "backbone chokepoints," whether cables, circuits, or other communications facilities, at which Plaintiff contends, in paragraph 66 of the Amended Complaint, the NSA must be conducting Upstream surveillance, stating for each such "backbone chokepoint" the basis of Plaintiff's contention.

RESPONSE TO INTERROGATORY NO. 13:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff also objects that this Interrogatory seeks information that is within Defendants' control. Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

An NSA document states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter

and leave the United States." *See* NSA Staff Processing Form, Subject: SSO's Support to the FBI for Implementation of their Cyber FISA Orders.

The "chokepoints" at which the NSA conducts Upstream surveillance have included the "seven access sites" identified in an NSA document, reproduced at paragraph 68 of Plaintiff's First Amended Complaint (ECF No. 70-1).

Additional reporting after the filing of the Amended Complaint states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. *See* Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents, one of which describes the surveillance of hundreds of circuits at a specific AT&T trans-Pacific cable site); Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents); Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents) (describing surveillance on AT&T's network, including on "OC-192 and 10GE peering circuits"; describing surveillance on Verizon's network, including at a cable-landing site called BRECKENRIDGE).

INTERROGATORY NO. 14:

Please state the basis of Plaintiff's allegation, in paragraph 49 of the Amended Complaint, that Upstream surveillance includes a process in which the NSA makes a copy of international text-based communications flowing across certain high-capacity cables, switches, and routers along the Internet backbone.

RESPONSE TO INTERROGATORY NO. 14:

In addition to the General Objections above which are incorporated herein, Plaintiff objects

that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's allegation are the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

In addition, a *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily

copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013; *see* also Charlie Savage, *Power Wars* 207–11 (2015).

INTERROGATORY NO. 15:

Please state the basis of Plaintiff's contentions regarding the manner in which the alleged copying, filtering, and content-review processes referred to in paragraph 49 of the Amended Complaint are carried out.

RESPONSE TO INTERROGATORY NO. 15:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff also objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's contentions are the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must

reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

In addition, a *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013; *see also* Charlie Savage, *Power Wars* 207–11 (2015).

Other bases of Plaintiff's contentions include:

- The PCLOB Report, including pages 7–10, 12–13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)

- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)

- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents)

- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)

- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)

- Charlie Savage, *Power Wars* (2015)

INTERROGATORY NO. 16:

Please state the basis of Plaintiff's allegations in paragraph 59 of the Amended Complaint, including the allegations that "[t]he NSA could readily configure its [alleged] surveillance equipment to ignore" Internet traffic that is "not amenable to … text-based searches;" that such traffic "is likely of no foreign-intelligence interest to the government;" and that "ignor[ing]" such traffic would result in "substantial efficiency gains."

RESPONSE TO INTERROGATORY NO. 16:

In addition to the General Objections above which are incorporated herein, Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff

responds as follows.

Plaintiff's allegations are based on basic principles governing the routing and transmission of Internet communications, as well as basic principles governing how surveillance on a packet-switched network operates.

Plaintiff's allegations are also based on the fact that a substantial percentage of Internet traffic consists of video traffic; and that video traffic from major video-traffic providers, such as Netflix, is likely of little foreign-intelligence interest to the government because it reflects only movie- and television-viewing habits.

INTERROGATORY NO. 17:

Please state the basis of Plaintiff's allegations, in paragraphs 62 and 64 of the Amended Complaint, respectively, that "in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link," and that "for every backbone link that the NSA monitors using Upstream surveillance, the monitoring must be comprehensive in order for the government to accomplish its stated goals."

RESPONSE TO INTERROGATORY NO. 17:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff also objects that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Plaintiff's allegation is based on basic principles governing the routing and transmission of Internet communications, as well as basic principles governing how surveillance on a packet-switched network operates.

INTERROGATORY NO. 18:

Please state the basis of Plaintiff's allegation, in paragraph 63 of the Amended Complaint, that "[t]o search the contents of any text-based communication for instances of the NSA's 'selectors' as that communication traverses a particular backbone link, the government must first copy and reassemble all of the packets that make up that communication."

RESPONSE TO INTERROGATORY NO. 18:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory seeks information that is the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Plaintiff's allegation is based on basic principles governing the routing and transmission of Internet communications, as well as basic principles governing how surveillance on a packet-switched network operates.

INTERROGATORY NO. 19:

Please state with particularity what Plaintiff means by the term "reliably" as used in

paragraphs 62, 63, and 66 of the Amended Complaint in the phrases "reliably obtain communications," and "reliably intercept … communications," and as the term "reliably," or its equivalent, may be used in Plaintiff's response to any of Defendants' other interrogatories.

RESPONSE TO INTERROGATORY NO. 19:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is compound, vague, ambiguous and overly burdensome in that it requests that Plaintiff define its use of the word "reliably" in a variety of discrete contexts, and in that it calls for a subjective judgment about what terms are "equivalent" to the term "reliably." Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The PCLOB has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10. And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can *reliably* acquire data packets associated with the proper communications." *Id*. at 143 (emphasis added).

Plaintiff's complaint uses the term "reliably" in different ways depending on context. For example, in paragraphs 62 and 63 of the Amended Complaint, Plaintiff uses the term "reliably" to signify that the government could not conduct Upstream surveillance as it has publicly described

it without undertaking certain steps. Paragraph 66 of Plaintiff's complaint quotes the PCLOB's use of the term "reliably."

INTERROGATORY NO. 20:

Please state the basis of Plaintiff's allegations, in paragraphs 65 and 66 of the Amended Complaint, that in conducting Upstream surveillance "the government's aim is to 'comprehensively' … obtain communications to, from, and about targets scattered around the world," and that "the government is interested in obtaining, with a high degree of confidence, all international communications to, from, or about its targets."

RESPONSE TO INTERROGATORY NO. 20:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The PCLOB has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10. And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can *reliably* acquire data packets associated with the proper communications." *Id*. at 143 (emphasis added); *see also* PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI).

INTERROGATORY NO. 21:

To the extent not already stated or identified in response to Interrogatory Nos. 13-20, above, or in response to Defendant United States Department of Justice's First Set of Interrogatories, Interrogatory Nos. 1-6, please state the basis of Plaintiff's contention that the NSA is intercepting, copying, and reviewing at least some of its communications.

RESPONSE TO INTERROGATORY NO. 21:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff also objects that this Interrogatory seeks information that is the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff also objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Plaintiff's contention is based on the volume and distribution of its communications, basic principles governing the routing and transmission of Internet communications, and basic principles governing how surveillance on a packet-switched network operates.

Dated: January 11, 2018

/s/Ashley Gorski
Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Counsel for Plaintiff Wikimedia Foundation, Inc.

EXHIBIT A

Report on International Submarine Cables Landing in the US

Source: underlying data cloned from https://github.com/telegeography/www.submarinecablemap.com, most recent commit at 2018-01-02 14:09:33-05:00 (7d7cd9e8096d624717f2b4e56ebc72831e2ba7f6)

US Landing Points for International Submarine Cables

Landing 1

Bandon, Oregon, United States

Location: (124.4°W, 43.12°N)

1 International Cable:

- FASTER

  Owners:
  Google, KDDI, SingTel, China Telecom, China Mobile, Global Transit
  Other Countries:
  Japan, Taiwan

Landing 2

Bellport, New York, United States

Location: (72.94°W, 40.76°N)

1 International Cable:

- Yellow

  Owners:
  Level 3
  Other Country:
  United Kingdom

Landing 3 Boca Raton, FL, United States

Location: (80.09°W, 26.35°N)

6 International Cables:

- South America-1 (SAm-1)

  Owners:
  Telxius
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

- Bahamas Internet Cable System (BICS)

  Owners:
  Caribbean Crossings
  Other Country:
  Bahamas

- Monet

  Owners:
  Angola Cables, Google, Algar Telecom, Antel Uruguay
  Other Country:
  Brazil

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

- GlobeNet

  Owners:
  BTG Pactual
  Other Countries:
  Bermuda, Brazil, Colombia, Venezuela

- Colombia-Florida Subsea Fiber (CFX-1)

  Owners:
  C&W Networks
  Other Countries:
  Colombia, Jamaica

Landing 4

Brookhaven, New York, United States

Location: (72.91°W, 40.77°N)

1 International Cable:

- Atlantic Crossing-1 (AC-1)

  Owners:
  Level 3
  Other Countries:
  Germany, Netherlands, United Kingdom

Landing 5

Buffalo, New York, United States

Location: (78.88°W, 42.89°N)

1 International Cable:

- Crosslake Fibre

  Owners:
  Crosslake Fibre
  Other Country:
  Canada

Landing 6

Charlestown, Rhode Island, United States

Location: (71.65°W, 41.41°N)

1 International Cable:

- Challenger Bermuda-1 (CB-1)

  Owners:
  Cable Co.
  Other Country:
  Bermuda

Landing 7

El Segundo, California, United States

Location: (118.4°W, 33.92°N)

1 International Cable:

- Pacific Light Cable Network (PLCN)

  Owners:
  Pacific Light Data Communication Co. Ltd., Google, Facebook
  Other Countries:
  China, Philippines, Taiwan

Landing 8

Grover Beach, California, United States

Location: (120.6°W, 35.12°N)

2 International Cables:

- Pan-American Crossing (PAC)

  Owners:
  Level 3
  Other Countries:
  Costa Rica, Mexico, Panama

- Pacific Crossing-1 (PC-1)

  Owners:
  NTT
  Other Country:
  Japan

Landing 9

Harbour Pointe, Washington, United States

Location: (122.3°W, 47.89°N)

1 International Cable:

- Pacific Crossing-1 (PC-1)

  Owners:
  NTT
  Other Country:
  Japan

Landing 10

Hermosa Beach, California, United States

Location: (118.4°W, 33.86°N)

2 International Cables:

- JUPITER

  Owners:
  Amazon, Facebook, NTT, PLDT, PCCW, Softbank Telecom
  Other Countries:
  Japan, Philippines

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

Landing 11

Hillsboro, Oregon, United States

Location: (123°W, 45.52°N)

2 International Cables:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

Landing 12 Hollywood, Florida, United States

Location: (80.16°W, 26.01°N)

4 International Cables:

- Columbus-III

  Owners:
  Telecom Italia Sparkle, AT&T, Verizon, Telefonica, Portugal Telecom, Tata Communications, Ukrtelecom, Telkom South Africa, Telecom Argentina, Instituto Costarricense de Electricidad, Embratel, Cyta
  Other Countries:
  Italy, Portugal, Spain

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Maya-1

  Owners:
  Verizon, AT&T, Sprint, Hondutel, Telefonica, Orbitel, Telecom Italia Sparkle, C&W Networks, Entel Chile, Embratel, ETB, Axtel, Instituto Costarricense de Electricidad, Proximus, Prepa Networks, Orange, Tricom, RSL Telecom, América Móvil
  Other Countries:
  Cayman Islands, Colombia, Costa Rica, Honduras, Mexico, Panama

Landing 13

Island Park, New York, United States

Location: (73.66°W, 40.6°N)

1 International Cable:

- FLAG Atlantic-1 (FA-1)

  Owners:
  Global Cloud Xchange
  Other Countries:
  France, United Kingdom

Landing 14

Isla Verde, Puerto Rico, United States

Location: (66.02°W, 18.44°N)

3 International Cables:

- Saint Maarten Puerto Rico Network One (SMPR-1)

  Owners:
  TelEm Group, Dauphin Telecom
  Other Countries:
  Saint Martin, Sint Maarten

- ARCOS

  Owners:
  C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
  Other Countries:
  Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

- Antillas 1

  Owners:
  AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
  Other Country:
  Dominican Republic

Landing 15

Jacksonville, Florida, United States

Location: (81.66°W, 30.33°N)

3 International Cables:

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- South America Pacific Link (SAPL)

  Owners:
  Ocean Networks
  Other Countries:
  Chile, Panama

- Pacific Caribbean Cable System (PCCS)

  Owners:
  C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
  Other Countries:
  Aruba, Colombia, Curaçao, Ecuador, Panama

Landing 16

Kahe Point, Hawaii, United States

Location: (158.1°W, 21.35°N)

1 International Cable:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

Landing 17

Kapolei, HI, United States

Location: (158.1°W, 21.34°N)

1 International Cable:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

Landing 18

Kawaihae, Hawaii, United States

Location: (155.8°W, 20.04°N)

1 International Cable:

- Honotua

  Owners:
  OPT French Polynesia
  Other Country:
  French Polynesia

Landing 19

Keawaula, Hawaii, United States

Location: (158.2°W, 21.43°N)

2 International Cables:

- Telstra Endeavour

  Owners:
  Telstra
  Other Country:
  Australia

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

Landing 20

Los Angeles, California, United States

Location: (118.2°W, 34.05°N)

1 International Cable:

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

Landing 21

Lynn, Massachusetts, United States

Location: (70.95°W, 42.46°N)

1 International Cable:

- GTT Atlantic

  Owners:
  GTT
  Other Countries:
  Canada, Ireland, United Kingdom

Landing 22

Makaha, Hawaii, United States

Location: (158.2°W, 21.46°N)

3 International Cables:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

- South America Pacific Link (SAPL)

  Owners:
  Ocean Networks
  Other Countries:
  Chile, Panama

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

Landing 23

Manasquan, New Jersey, United States

Location: (74.05°W, 40.12°N)

3 International Cables:

- TAT-14

  Owners:
  BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
  Other Countries:
  Denmark, France, Germany, Netherlands, United Kingdom

- Gemini Bermuda

  Owners:
  C&W Networks
  Other Country:
  Bermuda

- Apollo

  Owners:
  Vodafone
  Other Countries:
  France, United Kingdom

Landing 24

Manchester, California, United States

Location: (123.7°W, 38.97°N)

1 International Cable:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

Landing 25

Miramar, Puerto Rico, United States

Location: (66.08°W, 18.45°N)

2 International Cables:

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Antillas 1

  Owners:
  AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
  Other Country:
  Dominican Republic

Landing 26

Morro Bay, California, United States

Location: (120.8°W, 35.37°N)

2 International Cables:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

Landing 27

Naples, FL, United States

Location: (81.8°W, 26.14°N)

1 International Cable:

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

Landing 28

Nedonna Beach, Oregon, United States

Location: (123.9°W, 45.64°N)

1 International Cable:

- Trans-Pacific Express (TPE) Cable System

  Owners:
  China Telecom, China Unicom, Chunghwa Telecom, KT, Verizon, NTT, AT&T
  Other Countries:
  China, Japan, Taiwan

Landing 29

North Miami Beach, Florida, United States

Location: (80.16°W, 25.93°N)

1 International Cable:

- ARCOS

  Owners:
  C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
  Other Countries:
  Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

Landing 30

Northport, New York, United States

Location: (73.34°W, 40.91°N)

1 International Cable:

- FLAG Atlantic-1 (FA-1)

  Owners:
  Global Cloud Xchange
  Other Countries:
  France, United Kingdom

Landing 31

Pacific City, OR, United States

Location: (124°W, 45.2°N)

2 International Cables:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

- New Cross Pacific (NCP) Cable System

  Owners:
  China Telecom, China Unicom, Chunghwa Telecom, KT, China Mobile, Microsoft, Softbank Telecom
  Other Countries:
  China, Japan, Taiwan

Landing 32

Pago Pago, American Samoa

Location: (170.7°W, -14.28°N)

2 International Cables:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

- Samoa-American Samoa (SAS)

  Owners:
  American Samoa Government, Elandia
  Other Country:
  Samoa

Landing 33 Piti, Guam

Location: (-144.7°W, 13.46°N)

5 International Cables:

- HANTRU1 Cable System

  Owners:
  Hannon Armstrong, Federated States of Micronesia Telecommunications Company, Marshall Islands Telecommunications Authority
  Other Country:
  Federated States of Micronesia

- PIPE Pacific Cable-1 (PPC-1)

  Owners:
  TPG
  Other Countries:
  Australia, Papua New Guinea

- Hong Kong-Guam (HK-G)

  Owners:
  RTI Connectivity
  Other Country:
  China

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

Landing 34

Redondo Beach, California, United States

Location: (118.4°W, 33.84°N)

1 International Cable:

- Unity/EAC-Pacific

  Owners:
  Telstra, Google, Global Transit, SingTel, KDDI, Airtel (Bharti)
  Other Country:
  Japan

Landing 35

San Juan, Puerto Rico, United States

Location: (66.11°W, 18.47°N)

7 International Cables:

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- South America-1 (SAm-1)

  Owners:
  Telxius
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

- Global Caribbean Network (GCN)

  Owners:
  Leucadia National Corporation, Loret Group
  Other Country:
  Guadeloupe

- Pacific Caribbean Cable System (PCCS)

  Owners:
  C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
  Other Countries:
  Aruba, Colombia, Curaçao, Ecuador, Panama

- Southern Caribbean Fiber

  Owners:
  Digicel
  Other Countries:
  Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

- BRUSA

  Owners:
  Telxius
  Other Country:
  Brazil

Landing 36 San Luis Obispo, California, United States

Location: (120.7°W, 35.29°N)

1 International Cable:

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

Landing 37 Sarasota, Florida, United States

Location: (82.54°W, 27.34°N)

1 International Cable:

- AURORA

  Owners:
  FP Telecommunications
  Other Countries:
  Belize, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Honduras, Mexico, Nicaragua, Panama

Landing 38

Shirley, New York, United States

Location: (72.87°W, 40.8°N)

2 International Cables:

- AEConnect (AEC)

  Owners:
  Aqua Comms
  Other Country:
  Ireland

- Apollo

  Owners:
  Vodafone
  Other Countries:
  France, United Kingdom

Landing 39

Spanish River Park, Florida, United States

Location: (80.07°W, 26.38°N)

1 International Cable:

- Bahamas Internet Cable System (BICS)

  Owners:
  Caribbean Crossings
  Other Country:
  Bahamas

Landing 40

Spencer Beach, Hawaii, United States

Location: (155.8°W, 20.02°N)

1 International Cable:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

Landing 41

St. Croix, Virgin Islands, United States

Location: (64.82°W, 17.77°N)

5 International Cables:

- South American Crossing (SAC)/Latin American Nautilus (LAN)

  Owners:
  Level 3, Telecom Italia Sparkle
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Panama, Peru, Venezuela

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Pan American (PAN-AM)

  Owners:
  AT&T, Telefonica del Peru, Softbank Telecom, Telecom Italia Sparkle, Sprint, CANTV, Tata Communications, Telefónica de Argentina, Telstra, Verizon, Entel Chile, Telecom Argentina, Telconet, Instituto Costarricense de Electricidad, C&W Networks, Embratel
  Other Countries:
  Aruba, Chile, Colombia, Ecuador, Panama, Peru, Venezuela

- Global Caribbean Network (GCN)

  Owners:
  Leucadia National Corporation, Loret Group
  Other Country:
  Guadeloupe

- Southern Caribbean Fiber

  Owners:
  Digicel
  Other Countries:
  Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

Landing 42

Tanguisson Point, Guam

Location: (-144.8°W, 13.55°N)

2 International Cables:

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

- Australia-Japan Cable (AJC)

  Owners:
  Softbank Telecom, Telstra, Verizon, AT&T
  Other Countries:
  Australia, Japan

Landing 43

Tuckerton, New Jersey, United States

Location: (74.34°W, 39.6°N)

2 International Cables:

- TAT-14

  Owners:
  BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
  Other Countries:
  Denmark, France, Germany, Netherlands, United Kingdom

- GlobeNet

  Owners:
  BTG Pactual
  Other Countries:
  Bermuda, Brazil, Colombia, Venezuela

Landing 44

Tumon Bay, Guam

Location: (-144.8°W, 13.51°N)

2 International Cables:

- Guam Okinawa Kyushu Incheon (GOKI)

  Owners:
  AT&T
  Other Country:
  Japan

- Australia-Japan Cable (AJC)

  Owners:
  Softbank Telecom, Telstra, Verizon, AT&T
  Other Countries:
  Australia, Japan

Landing 45

Vero Beach, Florida, United States

Location: (80.39°W, 27.64°N)

1 International Cable:

- Bahamas 2

  Owners:
  AT&T, Telefonica, Verizon
  Other Country:
  Bahamas

Landing 46

Virginia Beach, Virginia, United States

Location: (76.06°W, 36.76°N)

3 International Cables:

- MAREA

  Owners:
  Facebook, Microsoft, Telxius
  Other Country:
  Spain

- Midgardsormen

  Owners:
  Midgardsormen
  Other Country:
  Denmark

- BRUSA

  Owners:
  Telxius
  Other Country:
  Brazil

Landing 47

Wall Township, New Jersey, United States

Location: (74.06°W, 40.15°N)

2 International Cables:

- Tata TGN-Atlantic

  Owners:
  Tata Communications
  Other Country:
  United Kingdom

- Seabras-1

  Owners:
  Seaborn Group
  Other Country:
  Brazil

International Submarine Cables Landing in the US

Cable 1 AEConnect (AEC)

More info:
http://www.aquacomms.com
Owners:
Aqua Comms
Length:
5,536 km
US Landing Point:

- Shirley, New York, United States

Other Country:
Ireland

Cable 2 America Movil Submarine Cable System-1 (AMX-1)

More info:
http://www.americamovil.com
Owners:
América Móvil
Length:
17,800 km
US Landing Points:

- Hollywood, Florida, United States
- Jacksonville, Florida, United States
- San Juan, Puerto Rico, United States

Other Countries:
Brazil, Colombia, Dominican Republic, Guatemala, Mexico

Cable 3 Americas-II

Owners:
Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
Length:
8,373 km
US Landing Points:

- Hollywood, Florida, United States
- Miramar, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Countries:
Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

Cable 4 Antillas 1

Owners:
AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
Length:
650 km
US Landing Points:

- Isla Verde, Puerto Rico, United States
- Miramar, Puerto Rico, United States

Other Country:
Dominican Republic

Cable 5 Apollo

More info:
http://www.vodafone.com/business/article-cs-apollo-submarine-cable-system
Owners:
Vodafone
Length:
13,000 km
US Landing Points:

- Manasquan, New Jersey, United States
- Shirley, New York, United States

Other Countries:
France, United Kingdom

Cable 6 ARCOS

More info:
http://www.cwnetworks.com/
Owners:
C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
Length:
8,600 km
US Landing Points:

- North Miami Beach, Florida, United States
- Isla Verde, Puerto Rico, United States

Other Countries:
Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

Cable 7 Asia-America Gateway (AAG) Cable System

More info:
http://www.asia-america-gateway.com
Owners:
Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
Length:
20,000 km
US Landing Points:

- Keawaula, Hawaii, United States
- San Luis Obispo, California, United States
- Tanguisson Point, Guam

Other Countries:
Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

Cable 8 Atlantic Crossing-1 (AC-1)

More info:
http://www.level3.com
Owners:
Level 3
Length:
14,301 km
US Landing Point:

- Brookhaven, New York, United States

Other Countries:
Germany, Netherlands, United Kingdom

Cable 9 AURORA

More info:
http://fptelecoms.com/
Owners:
FP Telecommunications
Length:
n.a.
US Landing Point:

- Sarasota, Florida, United States

Other Countries:
Belize, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Honduras, Mexico, Nicaragua, Panama

Cable 10 Australia-Japan Cable (AJC)

More info:
http://www.ajcable.com
Owners:
Softbank Telecom, Telstra, Verizon, AT&T
Length:
12,700 km
US Landing Points:

- Tanguisson Point, Guam
- Tumon Bay, Guam

Other Countries:
Australia, Japan

Cable 11 Bahamas 2

Owners:
AT&T, Telefonica, Verizon
Length:
470 km
US Landing Point:

- Vero Beach, Florida, United States

Other Country:
Bahamas

Cable 12 Bahamas Internet Cable System (BICS)

More info:
http://www.caribbeancrossings.com
Owners:
Caribbean Crossings
Length:
1,100 km
US Landing Points:

- Boca Raton, FL, United States
- Spanish River Park, Florida, United States

Other Country:
Bahamas

Cable 13 BRUSA

More info:
http://www.telxius.com
Owners:
Telxius
Length:
11,000 km
US Landing Points:

- San Juan, Puerto Rico, United States
- Virginia Beach, Virginia, United States

Other Country:
Brazil

Cable 14 Challenger Bermuda-1 (CB-1)

More info:
http://cableco.bm
Owners:
Cable Co.
Length:
1,448 km
US Landing Point:

- Charlestown, Rhode Island, United States

Other Country:
Bermuda

Cable 15 Colombia-Florida Subsea Fiber (CFX-1)

More info:
http://www.cwnetworks.com/
Owners:
C&W Networks
Length:
2,400 km
US Landing Point:

- Boca Raton, FL, United States

Other Countries:
Colombia, Jamaica

Cable 16 Columbus-III

Owners:
Telecom Italia Sparkle, AT&T, Verizon, Telefonica, Portugal Telecom, Tata Communications, Ukrtelecom, Telkom South Africa, Telecom Argentina, Instituto Costarricense de Electricidad, Embratel, Cyta
Length:
9,833 km
US Landing Point:

- Hollywood, Florida, United States

Other Countries:
Italy, Portugal, Spain

Cable 17 Crosslake Fibre

More info:
http://www.crosslakefibre.ca
Owners:
Crosslake Fibre
Length:
131 km
US Landing Point:

- Buffalo, New York, United States

Other Country:
Canada

Cable 18 Deep Blue Cable

More info:
http://www.deepbluecable.com
Owners:
Deep Blue Cable
Length:
12,000 km
US Landing Points:

- Boca Raton, FL, United States
- San Juan, Puerto Rico, United States
- Naples, FL, United States

Other Countries:
Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

Cable 19 FASTER

Owners:
Google, KDDI, SingTel, China Telecom, China Mobile, Global Transit
Length:
11,629 km
US Landing Point:

- Bandon, Oregon, United States

Other Countries:
Japan, Taiwan

Cable 20 FLAG Atlantic-1 (FA-1)

More info:
http://www.globalcloudxchange.com
Owners:
Global Cloud Xchange
Length:
14,500 km
US Landing Points:

- Island Park, New York, United States
- Northport, New York, United States

Other Countries:
France, United Kingdom

Cable 21 Gemini Bermuda

More info:
http://www.cwnetworks.com
Owners:
C&W Networks
Length:
1,287 km
US Landing Point:

- Manasquan, New Jersey, United States

Other Country:
Bermuda

Cable 22 Global Caribbean Network (GCN)

More info:
http://www.globalcaribbean.net
Owners:
Leucadia National Corporation, Loret Group
Length:
n.a.
US Landing Points:

- San Juan, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Country:
Guadeloupe

Cable 23 GlobeNet

More info:
http://www.globenet.net
Owners:
BTG Pactual
Length:
23,500 km
US Landing Points:

- Boca Raton, FL, United States
- Tuckerton, New Jersey, United States

Other Countries:
Bermuda, Brazil, Colombia, Venezuela

Cable 24 GTT Atlantic

More info:
http://www.gtt.net
Owners:
GTT
Length:
12,200 km
US Landing Point:

- Lynn, Massachusetts, United States

Other Countries:
Canada, Ireland, United Kingdom

Cable 25

Guam Okinawa Kyushu Incheon (GOKI)

More info:
http://www.att.com
Owners:
AT&T
Length:
4,244 km
US Landing Point:

- Tumon Bay, Guam

Other Country:
Japan

Cable 26

HANTRU1 Cable System

Owners:
Hannon Armstrong, Federated States of Micronesia Telecommunications Company, Marshall Islands Telecommunications Authority
Length:
2,917 km
US Landing Point:

- Piti, Guam

Other Country:
Federated States of Micronesia

Cable 27 Hawaiki

More info:
http://hawaikicable.co.nz
Owners:
Hawaiki Cable Company
Length:
14,000 km
US Landing Points:

- Kapolei, HI, United States
- Pacific City, OR, United States
- Pago Pago, American Samoa

Other Countries:
Australia, New Zealand

Cable 28 Hong Kong-Guam (HK-G)

Owners:
RTI Connectivity
Length:
3,900 km
US Landing Point:

- Piti, Guam

Other Country:
China

Cable 29 Honotua

More info:
http://www.opt.pf
Owners:
OPT French Polynesia
Length:
4,805 km
US Landing Point:

- Kawaihae, Hawaii, United States

Other Country:
French Polynesia

Cable 30 Japan-U.S. Cable Network (JUS)

Owners:
Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
Length:
22,682 km
US Landing Points:

- Makaha, Hawaii, United States
- Manchester, California, United States
- Morro Bay, California, United States

Other Country:
Japan

Cable 31 JUPITER

Owners:
Amazon, Facebook, NTT, PLDT, PCCW, Softbank Telecom
Length:
14,000 km
US Landing Point:

- Hermosa Beach, California, United States

Other Countries:
Japan, Philippines

Cable 32 MAREA

Owners:
Facebook, Microsoft, Telxius
Length:
6,605 km
US Landing Point:

- Virginia Beach, Virginia, United States

Other Country:
Spain

Cable 33 Maya-1

More info:
http://www.maya-1.com
Owners:
Verizon, AT&T, Sprint, Hondutel, Telefonica, Orbitel, Telecom Italia Sparkle, C&W Networks, Entel Chile, Embratel, ETB, Axtel, Instituto Costarricense de Electricidad, Proximus, Prepa Networks, Orange, Tricom, RSL Telecom, América Móvil
Length:
4,400 km
US Landing Point:

- Hollywood, Florida, United States

Other Countries:
Cayman Islands, Colombia, Costa Rica, Honduras, Mexico, Panama

Cable 34 Midgardsormen

More info:
http://midgardsormen.net
Owners:
Midgardsormen
Length:
7,848 km
US Landing Point:

- Virginia Beach, Virginia, United States

Other Country:
Denmark

Cable 35 Monet

Owners:
Angola Cables, Google, Algar Telecom, Antel Uruguay
Length:
10,556 km
US Landing Point:

- Boca Raton, FL, United States

Other Country:
Brazil

Cable 36 New Cross Pacific (NCP) Cable System

Owners:
China Telecom, China Unicom, Chunghwa Telecom, KT, China Mobile, Microsoft, Softbank Telecom
Length:
13,618 km
US Landing Point:

- Pacific City, OR, United States

Other Countries:
China, Japan, Taiwan

Cable 37

Pacific Caribbean Cable System (PCCS)

Owners:
C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
Length:
6,000 km
US Landing Points:

- Jacksonville, Florida, United States
- San Juan, Puerto Rico, United States

Other Countries:
Aruba, Colombia, Curaçao, Ecuador, Panama

Cable 38

Pacific Crossing-1 (PC-1)

More info:
http://www.pc1.com
Owners:
NTT
Length:
20,900 km
US Landing Points:

- Grover Beach, California, United States
- Harbour Pointe, Washington, United States

Other Country:
Japan

Cable 39

Pacific Light Cable Network (PLCN)

More info:
http://pldc.com.hk
Owners:
Pacific Light Data Communication Co. Ltd., Google, Facebook
Length:
12,871 km
US Landing Point:

- El Segundo, California, United States

Other Countries:
China, Philippines, Taiwan

Cable 40

Pan-American Crossing (PAC)

More info:
http://www.level3.com
Owners:
Level 3
Length:
10,000 km
US Landing Point:

- Grover Beach, California, United States

Other Countries:
Costa Rica, Mexico, Panama

Cable 41 Pan American (PAN-AM)

Owners:
AT&T, Telefonica del Peru, Softbank Telecom, Telecom Italia Sparkle, Sprint, CANTV, Tata Communications, Telefónica de Argentina, Telstra, Verizon, Entel Chile, Telecom Argentina, Telconet, Instituto Costarricense de Electricidad, C&W Networks, Embratel
Length:
7,050 km
US Landing Point:

- St. Croix, Virgin Islands, United States

Other Countries:
Aruba, Chile, Colombia, Ecuador, Panama, Peru, Venezuela

Cable 42 PIPE Pacific Cable-1 (PPC-1)

More info:
http://www.pipenetworks.com/ppc1
Owners:
TPG
Length:
6,900 km
US Landing Point:

- Piti, Guam

Other Countries:
Australia, Papua New Guinea

Cable 43 Saint Maarten Puerto Rico Network One (SMPR-1)

Owners:
TelEm Group, Dauphin Telecom
Length:
375 km
US Landing Point:

- Isla Verde, Puerto Rico, United States

Other Countries:
Saint Martin, Sint Maarten

Cable 44 Samoa-American Samoa (SAS)

Owners:
American Samoa Government, Elandia
Length:
250 km
US Landing Point:

- Pago Pago, American Samoa

Other Country:
Samoa

Cable 45 Seabras-1

More info:
http://www.seabornnetworks.com
Owners:
Seaborn Group
Length:
10,800 km
US Landing Point:

- Wall Township, New Jersey, United States

Other Country:
Brazil

Cable 46 SEA-US

Owners:
RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
Length:
14,500 km
US Landing Points:

- Hermosa Beach, California, United States
- Makaha, Hawaii, United States
- Piti, Guam

Other Countries:
Federated States of Micronesia, Indonesia, Palau, Philippines

Cable 47 South America-1 (SAm-1)

More info:
http://www.telxius.com/
Owners:
Telxius
Length:
25,000 km
US Landing Points:

- Boca Raton, FL, United States
- San Juan, Puerto Rico, United States

Other Countries:
Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

Cable 48

South American Crossing (SAC)/Latin American Nautilus (LAN)

More info:
http://www.level3.com
Owners:
Level 3, Telecom Italia Sparkle
Length:
20,000 km
US Landing Point:

- St. Croix, Virgin Islands, United States

Other Countries:
Argentina, Brazil, Chile, Colombia, Panama, Peru, Venezuela

Cable 49

South America Pacific Link (SAPL)

More info:
http://www.oceannetworks.com
Owners:
Ocean Networks
Length:
17,600 km
US Landing Points:

- Jacksonville, Florida, United States
- Makaha, Hawaii, United States

Other Countries:
Chile, Panama

Cable 50 Southern Caribbean Fiber

More info:
http://www.southern-caribbean.com
Owners:
Digicel
Length:
n.a.
US Landing Points:

- San Juan, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Countries:
Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

Cable 51 Southern Cross Cable Network (SCCN)

More info:
http://www.southerncrosscables.com
Owners:
Spark New Zealand, SingTel Optus, Verizon
Length:
30,500 km
US Landing Points:

- Hillsboro, Oregon, United States
- Kahe Point, Hawaii, United States
- Morro Bay, California, United States
- Spencer Beach, Hawaii, United States

Other Countries:
Australia, Fiji, New Zealand

Cable 52 TAT-14

More info:
https://www.tat-14.com
Owners:
BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
Length:
15,295 km
US Landing Points:

- Manasquan, New Jersey, United States
- Tuckerton, New Jersey, United States

Other Countries:
Denmark, France, Germany, Netherlands, United Kingdom

Cable 53 Tata TGN-Atlantic

More info:
http://www.tatacommunications.com
Owners:
Tata Communications
Length:
13,000 km
US Landing Point:

- Wall Township, New Jersey, United States

Other Country:
United Kingdom

Cable 54 Tata TGN-Pacific

More info:
http://www.tatacommunications.com
Owners:
Tata Communications
Length:
22,300 km
US Landing Points:

- Hillsboro, Oregon, United States
- Los Angeles, California, United States
- Piti, Guam

Other Country:
Japan

Cable 55 Telstra Endeavour

More info:
https://www.telstraglobal.com
Owners:
Telstra
Length:
9,125 km
US Landing Point:

- Keawaula, Hawaii, United States

Other Country:
Australia

Cable 56 Trans-Pacific Express (TPE) Cable System

More info:
http://tpecable.org
Owners:
China Telecom, China Unicom, Chunghwa Telecom, KT, Verizon, NTT, AT&T
Length:
17,000 km
US Landing Point:

- Nedonna Beach, Oregon, United States

Other Countries:
China, Japan, Taiwan

Cable 57 Unity/EAC-Pacific

Owners:
Telstra, Google, Global Transit, SingTel, KDDI, Airtel (Bharti)
Length:
9,620 km
US Landing Point:

- Redondo Beach, California, United States

Other Country:
Japan

Cable 58 Yellow

More info:
http://www.level3.com
Owners:
Level 3
Length:
7,001 km
US Landing Point:

- Bellport, New York, United States

Other Country:
United Kingdom

EXHIBIT B

Country, Territory, or Region	Number of HTTPS Requests to Wikimedia's U.S. Servers from April 23, 2017 to December 31, 2017
Afghanistan	20369894
Åland	117152
Albania	9813195
Algeria	156438189
Andorra	316946
Angola	105745420
Anguilla	4426739
Antigua and Barbuda	48037599
Argentina	19010881507
Armenia	18140327
Aruba	64193040
Australia	27114015484
Austria	52611694
Azerbaijan	107261925
Bahamas	151162707
Bahrain	8619910
Bangladesh	3176953826
Barbados	158106659
Belarus	84619956
Belgium	76321220
Belize	67244483
Benin	25265648
Bermuda	55289619
Bhutan	50416741
Bolivia	2018496453
Bonaire, Sint Eustatius, and Saba	13719337
Bosnia and Herzegovina	7960706
Botswana	2492444
Brazil	42781878450
British Indian Ocean Territory	14140
British Virgin Islands	10461523
Brunei	204756696
Bulgaria	41739970
Burkina Faso	72081285
Burundi	26725989
Cabo Verde	882511
Cambodia	472574422
Cameroon	116414708
Canada	48324693988
Cayman Islands	54000322
Central African Republic	1283047
Chad	40213806
Chile	9659037697

China	12584652290
Christmas Island	579670
Cocos [Keeling] Islands	106232
Colombia	16167706781
Comoros	1091223
Congo	195263297
Cook Islands	4088747
Costa Rica	1778677233
Croatia	19440436
Cuba	241281047
Curaçao	83087694
Cyprus	8347851
Czechia	74427132
Denmark	41180871
Djibouti	2292821
Dominica	17578663
Dominican Republic	2729299547
East Timor	35559845
Ecuador	5171181590
Egypt	68341152
El Salvador	1257386602
Equatorial Guinea	772007
Eritrea	60580
Estonia	9430466
Ethiopia	85497296
Falkland Islands	42130
Faroe Islands	195220
Federated States of Micronesia	6012383
Fiji	111027541
Finland	34542127
France	428122202
French Guiana	24749484
French Polynesia	105399149
French Southern Territories	743
Gabon	22322222
Gambia	5715554
Georgia	25583815
Germany	681511112
Ghana	44290723
Gibraltar	446362
Greece	53903595
Greenland	19382135
Grenada	35156030
Guadeloupe	87446940
Guatemala	2143452845
Guernsey	361898
Guinea	71901723

Guinea-Bissau	3706011
Guyana	108894211
Haiti	359392927
Hashemite Kingdom of Jordan	97594115
Honduras	1110628708
Hong Kong	11662091368
Hungary	55141049
Iceland	3140460
India	4776424926
Indonesia	17930654308
Iran	169551705
Iraq	27532939
Ireland	2915689068
Isle of Man	420522
Israel	136663663
Italy	308507489
Ivory Coast	4788982
Jamaica	541057089
Japan	113000000000
Jersey	438591
Kazakhstan	48793066
Kenya	61816471
Kiribati	2309857
Kosovo	440768
Kuwait	15390854
Kyrgyzstan	28319444
Laos	146029975
Latvia	11396822
Lebanon	14769754
Lesotho	12138382
Liberia	22366792
Libya	10894231
Liechtenstein	383883
Luxembourg	7386689
Macao	550047603
Macedonia	6785331
Madagascar	50887134
Malawi	6410883
Malaysia	8647611090
Maldives	124882076
Mali	30779056
Malta	3444213
Marshall Islands	3903305
Martinique	113112912
Mauritania	7266862
Mauritius	3235747
Mayotte	384633

Mexico	34178655407
Monaco	760422
Mongolia	378557613
Montenegro	3163785
Montserrat	1703867
Morocco	75093242
Mozambique	23042895
Myanmar [Burma]	555925780
Namibia	1364089
Nauru	716431
Nepal	824458922
Netherlands	314138585
New Caledonia	146196439
New Zealand	4974407925
Nicaragua	663794290
Niger	12893334
Nigeria	63405617
Niue	228788
Norfolk Island	165666
North Korea	1161183
Norway	48334001
Oman	7345673
Pakistan	481888376
Palau	3878789
Palestine	11882097
Panama	1733368181
Papua New Guinea	70580002
Paraguay	1101016965
Peru	10036096249
Philippines	12481173527
Pitcairn Islands	24226
Poland	274029978
Portugal	36859280
Qatar	17430941
Republic of Korea	11895460720
Republic of Lithuania	14924046
Republic of Moldova	15966392
Republic of the Congo	10928527
Réunion	2596349
Romania	140435673
Russia	401995918
Rwanda	36617960
Saint Helena	3361
Saint Kitts and Nevis	10037867
Saint Lucia	52811468
Saint Martin	9020272
Saint Pierre and Miquelon	6559606

Saint Vincent and the Grenadines	26989667
Saint-Barthélemy	448558
Samoa	5361146
San Marino	84815
São Tomé and Príncipe	315703
Saudi Arabia	54880396
Senegal	20064032
Serbia	50231403
Seychelles	1255981
Sierra Leone	23469731
Singapore	7218003729
Sint Maarten	20016168
Slovak Republic	8194905
Slovakia	13986326
Slovenia	6709561
Solomon Islands	11992687
Somalia	14276645
South Africa	41439302
South Georgia and the South Sandwich Islands	25507
South Sudan	13351919
Spain	181252108
Sri Lanka	72364979
St Kitts and Nevis	11384455
Sudan	25095741
Suriname	112376817
Svalbard and Jan Mayen	9060
Swaziland	13495244
Sweden	64789765
Switzerland	78135290
Syria	33031303
Taiwan	26446703306
Tajikistan	61431060
Tanzania	51538316
Thailand	10518810064
Togo	13185655
Tokelau	34305
Tonga	5398379
Trinidad and Tobago	475418043
Tunisia	33320421
Turkey	2067814073
Turkmenistan	1973624
Turks and Caicos Islands	13438622
Tuvalu	160716
Uganda	169288227
Ukraine	507837265
United Arab Emirates	73046384

United Kingdom	718823645
Uruguay	2012643741
Uzbekistan	29477693
Vanuatu	13851682
Vatican City	43867
Venezuela	7548335270
Vietnam	9042940682
Wallis and Futuna	2022934
Western Sahara	3149
Yemen	9262140
Zambia	87273901
Zimbabwe	55138516