

Exhibit 2

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

WIKIMEDIA FOUNDATION,

*

Plaintiff,

*

v.

* **Civil Action No.: 15-cv-00662-TSE**

NATIONAL SECURITY AGENCY, *et al.*,

*

Defendants.

*

* * * * *

REQUESTS FOR ADMISSION

Pursuant to Federal Rule of Civil Procedure 36, Local Rule 104, and Appendix A to the Local Rules, the Wikimedia Foundation (“WIKIMEDIA” or “PLAINTIFF”), by its undersigned attorneys, serves these Requests for Admission on defendants National Security Agency (“NSA”); the Office of the Director of National Intelligence (“ODNI”); the United States Department of Justice (“DOJ”); Admiral Michael S. Rogers, in his official capacity as the Director of the NSA; Daniel Coats, in his official capacity as the Director of National Intelligence (“DNI”); and Jefferson B. Sessions, III, in his official capacity as Attorney General (collectively, the “DEFENDANTS”), and demands that DEFENDANTS answer each Request for Admission herein in writing and under oath and within thirty (30) days of the date of service of the Requests for Admission, in accordance with the Definitions and Instructions set forth below.

DEFINITIONS

Notwithstanding any definition set forth below, each word, term, or phrase used in this Request is intended to have the broadest meaning permitted under the Federal Rules of Civil

Procedure. As used in this Request, the following terms are to be interpreted in accordance with these definitions:

Answer: The term “ANSWER” means Defendants’ Answer to Plaintiff’s First Amended Complaint in this action, filed on October 16, 2017.

Bulk: To COPY or REVIEW INTERNET COMMUNICATIONS in “BULK” means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

Circuit: The term “CIRCUIT” has the same meaning as “circuit” 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,” dated July 2, 2014 (“PCLOB Report”), at pages 36 to 37.

Communication: The term “COMMUNICATION” means information transmitted by any means, whether orally, electronically, by document, or otherwise.

Concern or Concerning: The terms “CONCERN” and “CONCERNING” mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

Copy: The term “COPY” means to duplicate a piece of data (for any duration, no matter how brief).

Describe: The term “DESCRIBE” means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events,

agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

Document: The term “DOCUMENT” shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way to a requested document. A draft or non-identical copy is a separate document within the meaning of the term “DOCUMENT.”

Identify (with respect to PERSONS): When referring to a PERSON, to “IDENTIFY” means to state the PERSON’s full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

Identify (with respect to documents): When referring to documents, to “IDENTIFY” means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

Interacted with: “INTERACTED WITH” means to have used a device to COPY or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication.

International Communication: The term “INTERNATIONAL COMMUNICATION” means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

Internet Backbone: The term “INTERNET BACKBONE” means the set of high-capacity cables, switches, and routers that facilitates both domestic and international Internet communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

Internet Communication: The term “INTERNET COMMUNICATION” means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

Internet Packet: The term “INTERNET PACKET” means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol (“IP”) address and some payload.

Internet Transaction: The term “INTERNET TRANSACTION” has the same meaning as “Internet transaction” within the PCLOB Report at pages 39 and 125 and note 517.

NSA: The terms “National Security Agency” and “NSA” include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA’s direction.

Parties: The terms “PLAINTIFF” and “DEFENDANT,” as well as a party’s full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors, employees, agents, representatives, attorneys, consultants, and contractors. This definition is not

intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court's jurisdiction to enter any appropriate order.

Person: The term "PERSON" is defined as any natural person or any business, legal or governmental entity, or association.

Process: The term "PROCESS" has the same meaning as "process," "process[ed]," or "process[ing]" within the July 2014 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, *available at* <https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf> ("2014 NSA Minimization Procedures").

Retain: The term "RETAIN" has the same meaning as "retain," "retained," or "retention" within the 2014 NSA Minimization Procedures.

Review: The term "REVIEW" means to scan, search, screen, capture, monitor, analyze, redirect, divert, or gather information about the contents of.

Selector: The term "SELECTOR" has the same meaning as "selector" within the 2014 NSA Minimization Procedures.

Target: The term "TARGET" means the subjects who are "targeted" pursuant to 50 U.S.C. § 1881a.

United States: When used as a term of geographic location, "UNITED STATES" means all areas under the territorial sovereignty of the United States.

Wholly Domestic Communication: The term "WHOLLY DOMESTIC COMMUNICATION" means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

You/Your: The terms “YOU” or “YOUR” include the defendant agency, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. “All” means “any and all”; “any” means “any and all.” “Including” means “including but not limited to.” “And” and “or” encompass both “and” and “or.” Words in the masculine, feminine, or neutral form shall include each of the other genders.

INSTRUCTIONS

1. YOU are requested to answer each Request for Admission set forth below separately and completely in writing under oath. In answering these Requests for Admission, respond truthfully and in good faith on the basis of all information that is known or readily obtainable by YOU.

2. As required by Federal Rule of Civil Procedure 36(a)(4), if good faith requires that YOU deny only a portion of any matter as to which an admission is requested, or that YOU qualify any response as to any given Request for Admission, specify and admit so much of the Request as is true and deny or qualify only that portion of the Request as to which good faith requires a denial or qualification.

3. Each Request for Admission shall be answered fully unless it is objected to in good faith, in which event the reasons for YOUR objection shall be stated in detail. If an objection pertains to only a portion of a Request for Admission, or a word, phrase, or clause contained within it, YOU are required to state YOUR objection to that portion only and to respond to the remainder of the Request for Admission, using YOUR best efforts to do so.

4. If YOU assert that any information responsive to any Request for Admission is privileged or otherwise protected from discovery, YOU are requested to expressly make a claim of privilege and to describe the nature of the information not disclosed, in a manner that, without revealing information itself privileged or protected, will enable PLAINTIFF to assess the claim of privilege. For any DOCUMENT or information withheld on the grounds that it is privileged or otherwise claimed to be excludable from discovery, identify the information or DOCUMENT, describe its subject matter and date, identify all authors and all recipients (including copied and blind copied recipients), and specify the basis for the claimed privilege or other grounds of exclusion.

5. YOUR responses to these Requests should be based upon information known to YOU CONCERNING facts or events that occurred, in whole or in part, as of June 22, 2015.

6. These Requests for Admission are continuing in nature and YOUR responses to them are to be promptly supplemented or amended if, after the time of YOUR initial responses, YOU learn that any response is or has become in some material respect incomplete or incorrect, to the full extent provided for by Federal Rule of Civil Procedure 26(e).

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.

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.

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.

REQUEST FOR ADMISSION NO. 4:

Admit that the INTERNET BACKBONE includes high-capacity terrestrial cables that carry traffic 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.

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.

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.

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.

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.

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.

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.

REQUEST FOR ADMISSION NO. 12:

Admit that, in the course of Upstream surveillance, the NSA RETAINS WHOLLY DOMESTIC COMMUNICATIONS.

REQUEST FOR ADMISSION NO. 13:

Admit that the NSA conducts Upstream surveillance on multiple INTERNET BACKBONE CIRCUITS.

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).

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).

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Dated: November 7, 2017

/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

Exhibit A

Why are we interested in HTTP?



facebook



YAHOO!



twitter

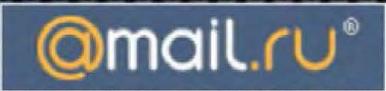


myspace.com
a place for friends

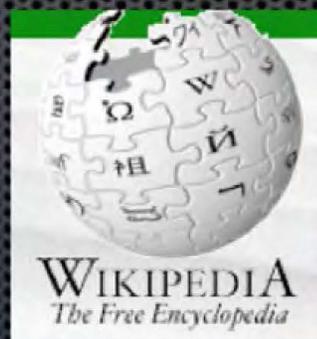
Because nearly everything a typical user does on the Internet uses HTTP



CNN.com



@mail.ru



Google
Earth



Gmail
by Google BETA

Exhibit B



Fingerprints and Appids

- Useful for identifying classes of traffic or particular targets (for SIGDEV or collection):
 - `mail/webmail/yahoo`
 - `browser/cellphone/blackberry`
 - `topic/s2B/chinese_missile`
- appid – a contest, highest scoring appid wins
- fingerprint – many fingerprints per session
- microplugin – a fingerprint or appid that is relatively complex (e.g. extracts and databases metadata)



Fingerprints and Appids (more)

- Written in language called "GENESIS" (go genesis-language):

```
appid('encyclopedia/wikipedia', 2.0) =  
  http_host('wikipedia' or 'wikimedia');  
fingerprint('dns/malware/MalwareDomains') =  
  dns_host('erofreex.info' or 'datayakoz.info'  
  or 'erogirlx.info' or 'pornero.info' or ...)
```

- If a fingerprint contains a schema definition, a search form automatically appears in the XKEYSCORE GUI
- Power users can drop in to C++ to express themselves

Exhibit C



STORMBREW At a Glance

Seven Access Sites – International “Choke Points”

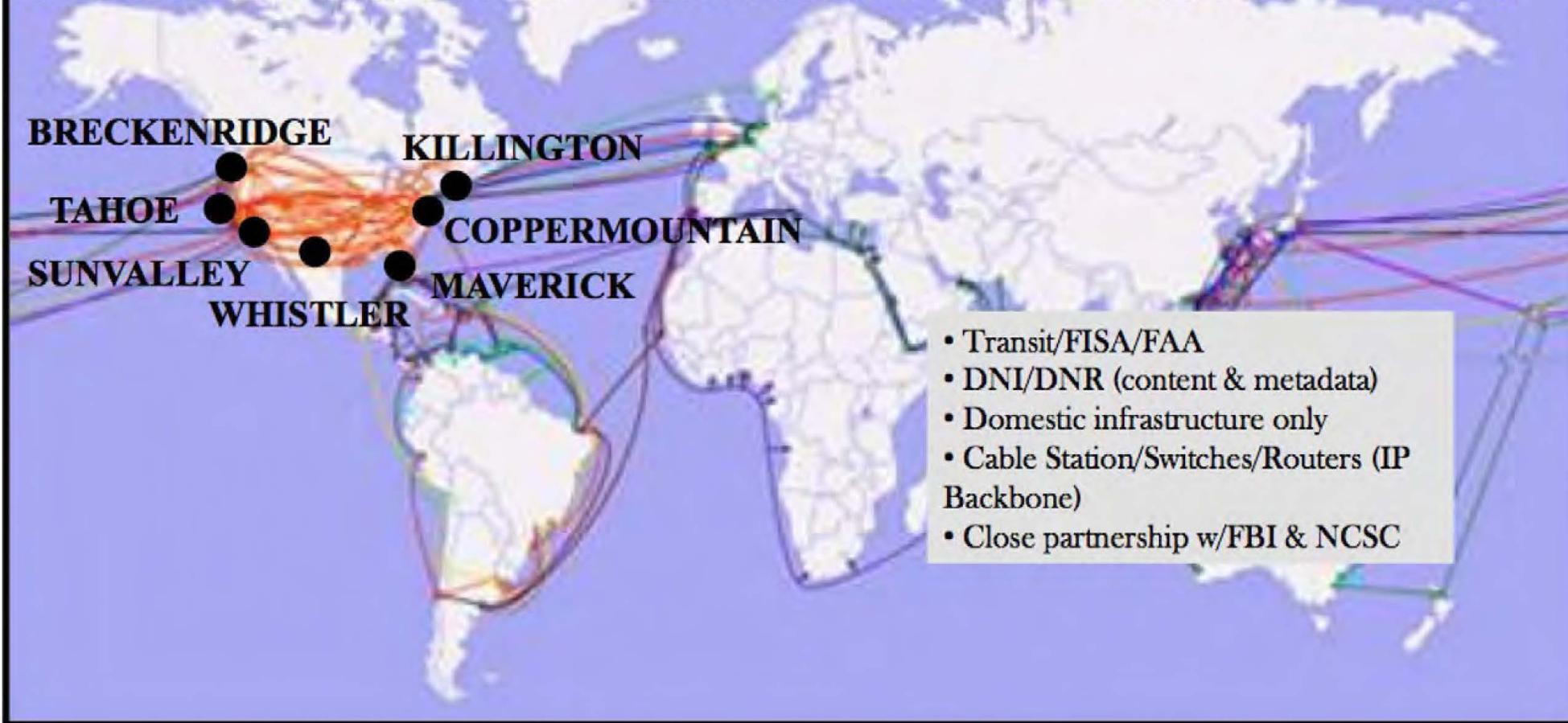


Exhibit D

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO SIGINT DIR	EXREG CONTROL NUMBER 2012-704	KCC CONTROL NUMBER S353-113-11
THRU	ACTION <input checked="" type="checkbox"/> APPROVAL <input type="checkbox"/> SIGNATURE <input type="checkbox"/> INFORMATION	EXREG SUSPENSE
SUBJECT (S//REL) SSO's Support to the FBI for Implementation of their Cyber FISA Orders		KCC SUSPENSE
DISTRIBUTION V2, V3, V07		ELEMENT SUSPENSE

SUMMARY

RECOMMENDATION: (U//FOUO) Approve the provision of the assistance to FBI, with the proviso that the FBI remains responsible for any additional expenses incurred.

PURPOSE: (S//REL) To obtain the SIGINT Director's approval for the Office of Special Source Operations (SSO) to provide ongoing technical assistance to the Federal Bureau of Investigation (FBI) for the implementation of the various orders they have obtained, and will obtain, from the Foreign Intelligence Surveillance Court (FISC) in certain Cyber cases involving agents of foreign powers (e.g. - [REDACTED] soon, [REDACTED]). The preparation of this Staff Processing Form was a collaborative effort between SSO and the NSA Office of General Counsel (OGC).

BACKGROUND: (S//REL) On December 20, 2011, NSA received a request for technical assistance from the FBI seeking access to infrastructure established by NSA for collection of foreign intelligence from U.S. telecommunications providers. The FISC has issued a number of orders at the request of the FBI authorizing electronic surveillance directed at communications related to computer intrusions being conducted by foreign powers. The orders include some that are limited to pen register/trap and trace (PRTT) information as well as others that authorize collection of content. The first of these for which NSA assistance has been requested is directed at communications related to intrusions conducted by the [REDACTED] (Docket Number 11-91), regarding what FBI refers to as STYGIAN FLOW.

(S//REL) In mid-2011, prior to receipt of the request for technical assistance, SSO became aware of FBI's plans to seek these orders and has been in discussions with FBI throughout the latter half of the year, in the belief that use of NSA's collection/processing infrastructure would allow the FBI to

Continued...

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
OGC	[REDACTED] / email / 30 Jan.				
FIB	[REDACTED] / email / 9 Feb.		S3	[REDACTED] / s / 3-20-12	
SI	[REDACTED] / s /		S35	[REDACTED]	
NTOC	[REDACTED] / s /		SV	[REDACTED] / 6/31 Jan.	
T	[REDACTED] / s / 6 Feb.		POC	[REDACTED]	

ORIGINATOR [REDACTED]	ORG. S353	PHONE (Secure) [REDACTED]	DATE PREPARED 20111221
--------------------------	--------------	------------------------------	---------------------------

FORM A6796DE REV NOV 2008(Supersedes A6796 FEB 05 which is obsolete)
 NSN: 7540-FM-001-5465
 Derived From: NSA/CSS Manual 1-52
 Dated: 8 January 2007
 Declassify On: 20320108

SECURITY CLASSIFICATION

SECRET//REL TO USA, FVEY

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION**Page 2 of 4: CATS 2012-704 (S//REL TO USA, FVEY) SSO's Support to the FBI for Implementation of their Cyber FISA Orders**

maximize the value of the collection without incurring the expenses associated with duplication of that infrastructure. Although FBI conducts numerous electronic surveillances without NSA's assistance, the vast majority of them are directed against targets located inside the United States, and U.S. providers served with FISC orders are ordinarily able to identify and deliver to the FBI most, if not all, of the targets' communications that they carry. That is because such electronic surveillance is typically effected at a point or points in the provider's infrastructure in physical proximity to the target's location. In the case of computer intrusions being conducted by foreign powers, the providers may be carrying a target's communications, but it is much more difficult to identify and locate them, because the communications in question will enter and leave the United States via any convenient path, and their path may be obscured to avoid detection. In other words, in these cases, because the target's location is outside the United States and not well-characterized, effecting the surveillance via FBI's traditional means is not effective.

(S//REL) However, in support of FAA and in anticipation of the need to conduct similar collection activities for computer network defense purposes, over the last decade, NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States. Collection at such chokepoints is much better suited to electronic surveillance directed at targets located outside the United States than FBI's traditional means of collection. In theory, FBI could rely on the orders it has obtained to direct U.S. providers to conduct surveillance at these chokepoints without relying on NSA capabilities, but it would take a considerable amount of time to do so, and FBI would have to reimburse the providers to recreate (i.e., duplicate) what NSA has already put in place. The cost alone would be prohibitive, and the time lost in doing so would necessarily result in a loss of foreign intelligence.

(S//REL) The assistance being sought by the FBI is limited in nature. The U.S. providers served with Secondary Orders in this matter will assume full responsibility for the provisioning of PR/TT and content collection to the FBI. Since all of the authorized "facilities" (typically known as "targeted selectors" in NSA parlance) to date are Internet Protocol (IP) addresses used by the targets, there is no question as to the providers' abilities to employ devices under their control (e.g., routers) to provision fully-compliant, authorized intercept.

(S//REL) Neither the providers nor the FBI will require NSA's Government off the Shelf (GOTS) Digital Network Intelligence (DNI) collection and processing solutions (e.g., TURMOIL, XKEYSCORE). Instead, metadata and full content derived from the authorized intercept will be produced using Commercial off the Shelf (COTS) processing solutions. If these COTS processing solutions involve components developed at NSA's expense and used, primarily, for NSA's Cyber survey purposes, the SSO will make careful and informed decisions prior to authorizing use of these components.

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

Page 3 of 4: CATS 2012-704 (S//REL TO USA, FVEY) SSO's Support to the FBI for Implementation of their Cyber FISA Orders

(S//REL) Prior to authorizing use of the extensive secure Wide Area Networks established at the two primary providers (cover terms, LITHIUM and ARTIFICE, respectively) as the end-to-end data delivery infrastructure to connect intercept and processing locations with the FBI's designated Cyber data repository at the Engineering Research Facility, Quantico, VA, SSO will make careful and informed decisions to ensure this capability is undertaken on a 100% non-interference basis with NSA's current and future data backhaul needs on these same networks.

(S//REL) All data (metadata and/or content) collected under the auspices of these FISC orders will be forwarded securely and directly to the designated FBI repository. The FISC orders do contain a provision, as follows: "NCIJTF personnel participating in this joint investigation may have access to raw data prior to minimization." However, access to raw data by NTOC members of the NCIJTF will be facilitated under the purview of the FBI and not through any actions that SSO might take as the collected data passes through NSA's secure Wide Area Networks. Should the FBI's cyber orders from the FISC be modified in the future to authorize raw data retention by NSA, SSO will coordinate with all cognizant NSA offices (e.g., Data Governance, OGC, SV) to ensure the proper data delivery mechanism is put in place.

(S//REL) Should the FBI require a sustained and high-level of dedicated analytical resources (i.e., cleared, technical manpower) at the providers in order to optimize the collection effectiveness of their PR/TT and content orders, they will contract for those services directly with the providers. If, on the other hand, the FBI's requirement for provider analytical support is more ad hoc and aperiodic in nature during the period of time these orders remain in effect, SSO will make careful and informed decisions prior to authorizing labor charges against the relevant SSO contracts with the providers for these services on behalf of the FBI. Any charges that cannot be justified as necessary for NSA purposes will not be made unless/until FBI agrees to reimburse NSA.

DISCUSSION: (S//REL) If SID decides to approve the requested assistance, SSO will assist the FBI in effecting any cyber orders submitted to it after the NSA/OGC has verified that each of them contains language permitting NSA's involvement. As stated in Attachment 1, NSA will have the opportunity to review and respond to any proposed use of FISA-derived information from these collections prior to the Attorney General authorizing the use of such information in any criminal proceedings.

(S//REL) The assistance SSO is being asked to provide to the FBI will not preclude NSA's SIGINT targeting of these same fully-qualified, overseas IP addresses under the auspices of the FISA

Continued...

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

Page 4 of 4: CATS 2012-704 (S//REL TO USA, FVEY) SSO's Support to the FBI for Implementation of their Cyber FISA Orders

(S//REL) The assistance SSO is being asked to provide to the FBI will not preclude NSA's SIGINT targeting of these same fully-qualified, overseas IP addresses under the auspices of the FISA Amendments Act (FAA) of 2008. To the contrary, the relatively recent discovery of these FBI Cyber FISA orders and the countless pages of SIGINT-derived evidence that was cited in the respective Applications to the FISC have already formed the basis for a dialog between NSA's OGC and the Department of Justice's National Security Division.

(C) DIRECTOR, SIGNALS INTELLIGENCE DECISION:

CONCUR: Perrett H. Hoar DATE: 3 - 8 27 - 12

NON-CONCUR: _____ DATE: _____

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

Exhibit E

TOP SECRET//COMINT//NOFORN//20320108

EXHIBIT A

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

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

2009 JUL 29 PM 3:14
CLERK OF COURT

(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 ("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. (U) 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 information concerning the communications facility or facilities used by that person.

(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 to determine what that lead information discloses about the person's location; (2) they conduct research in NSA databases, available reports and collateral information (i.e., information to which NSA has access but did not originate, such as reports from other agencies and publicly available information) to determine whether NSA knows the location of the person, or knows information that would provide evidence concerning that location; and (3) they conduct technical analyses of the facility or facilities 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.

(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

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

overseas, or it will target Internet links that terminate in a foreign country. 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 the location of the facility or facilities being used by the potential target.

(S) The following are examples of the types of lead information that NSA may examine:

- a) Has the target stated that he is located outside the United States? For example, has NSA or another intelligence agency collected a statement or statements made by the target indicating that he is located outside the United States?
- b) Has a human intelligence source or other source of lead information indicated that the target is located outside the United States?
- c) Does the lead information provided by an intelligence or law enforcement agency of the United States government or an intelligence or law enforcement service of a foreign government indicate that the target is located outside the United States?
- d) Was the lead information about the target found on a hard drive or other medium that was seized in a foreign country?
- e) With whom has the target had direct contact, and what do we know about the location of such persons? For example, if lead information indicates the target is in direct contact with several members of a foreign-based terrorist organization or foreign-based political organization who themselves are located overseas, that may suggest, depending on the totality of the circumstances, that the target is also located overseas.

(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, as well as publicly available information, 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, NSA databases may include a report produced by the Central Intelligence Agency (CIA) with the fact that a known terrorist is using a telephone with a particular number, or detailed information on worldwide telephony numbering plans for wire and wireless telephone systems.

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

(S) NSA Technical Analysis of the Facility

(S) NSA may also apply technical analysis concerning the facility from which it intends to acquire foreign intelligence information 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:

(S) For telephone numbers:

- a) Identify the country code of the telephone number, and determine what it indicates about the person's location.
- b) Review commercially available and NSA telephone numbering databases for indications of the type of telephone being used (e.g. landline, wireless mobile, satellite, etc.), information that may provide an understanding of the location of the target.

(S) For electronic communications accounts/addresses/identifiers:

Review NSA content repositories and Internet communications data repositories (which contain, among other things, Internet communications metadata) for previous Internet activity. This information may contain network layer (e.g., Internet Protocol addresses) or machine identifier (e.g., Media Access Control addresses) information, which NSA compares to information contained in NSA's communication network databases and commercially available Internet Protocol address registration information in order to determine the location of the target.

(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, lead information provided by an intelligence or law enforcement service of a foreign government may indicate not only that the target is located in a foreign country, but that the target is a citizen of that or another foreign country. 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 maintains records of telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are being used by United States persons. Prior to targeting, a particular telephone number or electronic communications account/address/identifier will be compared against those records in order to ascertain whether NSA has reason to believe that telephone number or electronic communications account/address/identifier is being used by a United States person.

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

(S) In the absence of specific information regarding whether a target is a United States person, a person reasonably believed to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person can be positively identified as a United States person, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

(S) Assessment of the Foreign Intelligence Purpose of the Targeting

(S) In assessing whether the target possesses 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:

- Information indicates that the telephone number has been used to communicate directly with another telephone number reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
- Information indicates that a user of the telephone number has communicated directly with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Information indicates that the telephone number is listed in the telephone directory of a telephone used by an individual associated with a foreign power or foreign territory;
- Information indicates that the telephone number has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Publicly available sources of information (e.g., telephone listings) match the telephone number to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Information contained in various NSA-maintained knowledge databases containing foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register and trap or trace device, or other information, reveals that the telephone number has been previously used by an individual associated with a foreign power or foreign territory;¹ or

¹ (TS//SI//NF) The NSA knowledge databases that would be used to satisfy this factor contain fused intelligence information concerning international terrorism culled from signals intelligence, human intelligence, law enforcement information, and other sources. The information compiled in these databases is information that assists the signals intelligence system in effecting collection on intelligence targets. For example, a report produced by the CIA may include the fact that a known terrorist is using a telephone with a particular number. NSA would include that information in its knowledge databases.

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

- Information made available to NSA analysts as a result of processing telephony metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the telephone number is used by an individual associated with a foreign power or foreign territory.
- b. With respect to Internet communications:
- Information indicates that the electronic communications account/address/identifier has been used to communicate directly with an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
 - Information indicates that a user of the electronic communications account/address/identifier has communicated directly with an individual reasonably believed to be associated with a foreign power or foreign territory;
 - Information indicates that the electronic communications account/address/identifier is included in the "buddy list" or address book of an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
 - Information indicates that the electronic communications account/address/identifier has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
 - Public Internet postings match the electronic communications account/address/identifier to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
 - Information contained in various NSA-maintained knowledge databases of foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, the use of a pen register or trap and trace device, or other information, reveals that electronic communications account/address/identifier has been previously used by an individual associated with a foreign power or foreign territory;
 - Information made available to NSA analysts as a result of processing metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the electronic communications account/address/identifier is used by an individual associated with a foreign power or foreign territory; or
 - Information indicates that Internet Protocol ranges and/or specific electronic identifiers or signatures (e.g., specific types of cryptology or steganography) are used almost exclusively by individuals associated with a foreign power or foreign territory,

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

or are extensively used by individuals associated with a foreign power or foreign territory.

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:

For telephone numbers:

- Routinely comparing telephone numbers tasked pursuant to these procedures against information that has been incidentally collected from the Global System for Mobiles (GSM) Home Location Registers (HLR). These registers receive updates whenever a GSM phone moves into a new service area. Analysis of this HLR information provides a primary indicator of a foreign user of a mobile telephone entering the United States.
- 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.

For electronic communications accounts/addresses/identifiers:

- Routinely checking all electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against available databases that contain Internet communications data (including metadata) to determine if an electronic communications account/address/identifier was accessed from overseas. Such databases contain communications contact information and summaries of communications activity from NSA signals intelligence collection. The foreign access determination is made based on comparing the Internet Protocol address associated with the account activity to other information NSA possesses about geographical area(s) serviced by particular Internet Protocol addresses. If the IP address associated with the target activity is identified as a U.S.-based network gateway (e.g., a Hotmail server) or a private Internet Protocol address, then NSA analysts will be required to perform additional research to determine if the access was in a foreign country using additional criteria such as machine identifier or case notation (NSA circuit identifier) of a communications link known to be foreign. Such databases normally maintain information about such activity for a 12-month period. This data will be used in an attempt to rule out false positives from U.S.-based network gateways. If the account access is determined to be from a U.S.-based machine, further analytic checks will be performed using content collection to determine if the target has moved into the United States.

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

- Routinely comparing electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against a list of electronic communications accounts/addresses/identifiers already identified by NSA as being accessed from inside the United States. This will help ensure that no target has been recognized to be located in the United States.
- 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.

(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. In cases where NSA cannot resolve an apparent conflict between information indicating that the target has entered the United States and information indicating that the target remains located outside the United States, NSA will presume that the target has entered the United States and will terminate the acquisition from that target. If at a later time NSA determines that the target is in fact located outside the United States, NSA may re-initiate the acquisition in accordance with these procedures.

(S) If NSA determines that a target who at the time of targeting was believed to be a non-United States person was in fact 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. (U) 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 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, such as a report number or communications intercept identifier, which NSA will maintain. 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. (U) OVERSIGHT AND COMPLIANCE

(S) NSA's Signals Intelligence Directorate (SID) Oversight and Compliance, with NSA's Office of General Counsel (OGC), 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. SID Oversight and Compliance 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. SID

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

Oversight and Compliance 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. SID Oversight and Compliance will also ensure that necessary corrective actions are taken to address any identified deficiencies. To that end, SID Oversight and Compliance 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 at least once every sixty days.

(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 was in fact 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.

TOP SECRET//COMINT//NOFORN//20320108

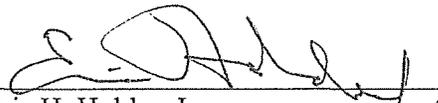
TOP SECRET//COMINT//NOFORN//20320108

- 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. (U) 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.

7-28-09
Date


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

TOP SECRET//COMINT//NOFORN//20320108

Exhibit F

~~TOP SECRET//SI//NOFORN//20320108~~

EXHIBIT B

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

**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~~

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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 disseminations 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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(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;

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(U) Section 8 - Collaboration with Foreign Governments

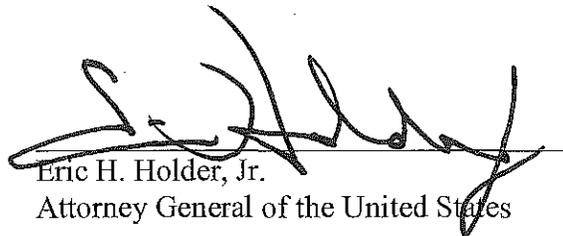
- (a) (U) Procedures for the dissemination of evaluated and minimized information. Pursuant to section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may 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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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

~~TOP SECRET//SI//NOFORN//20320108~~

Exhibit 3

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

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

* * * * *

PLAINTIFF’S SECOND SET OF REQUESTS FOR ADMISSION

Pursuant to Federal Rule of Civil Procedure 36, Local Rule 104, and Appendix A to the Local Rules, the Wikimedia Foundation (“WIKIMEDIA” or “PLAINTIFF”), by its undersigned attorneys, serves these Requests for Admission on defendants National Security Agency (“NSA”); the Office of the Director of National Intelligence (“ODNI”); the United States Department of Justice (“DOJ”); Admiral Michael S. Rogers, in his official capacity as the Director of the NSA; Daniel Coats, in his official capacity as the Director of National Intelligence (“DNI”); and Jefferson B. Sessions, III, in his official capacity as Attorney General (collectively, the “DEFENDANTS”), and demands that DEFENDANTS answer each Request for Admission herein in writing and under oath and within thirty (30) days of the date of service of the Requests for Admission, in accordance with the Definitions and Instructions set forth below.

DEFINITIONS

Notwithstanding any definition set forth below, each word, term, or phrase used in this Request is intended to have the broadest meaning permitted under the Federal Rules of Civil

Procedure. As used in this Request, the following terms are to be interpreted in accordance with these definitions:

Answer: The term “ANSWER” means Defendants’ Answer to Plaintiff’s First Amended Complaint in this action, filed on October 16, 2017.

Bulk: To COPY or REVIEW INTERNET COMMUNICATIONS in “BULK” means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

Circuit: The term “CIRCUIT” has the same meaning as “circuit” 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,” dated July 2, 2014 (“PCLOB Report”), at pages 36 to 37.

Communication: The term “COMMUNICATION” means information transmitted by any means, whether orally, electronically, by document, or otherwise.

Concern or Concerning: The terms “CONCERN” and “CONCERNING” mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

Copy: The term “COPY” means to duplicate a piece of data (for any duration, no matter how brief).

Describe: The term “DESCRIBE” means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events,

agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

Document: The term “DOCUMENT” shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way to a requested document. A draft or non-identical copy is a separate document within the meaning of the term “DOCUMENT.”

Identify (with respect to PERSONS): When referring to a PERSON, to “IDENTIFY” means to state the PERSON’s full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

Identify (with respect to documents): When referring to documents, to “IDENTIFY” means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

Interacted with: The term “INTERACTED WITH” means to have used a device to COPY or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication or transaction in the ordinary course of its transmission or storage.

International Communication: The term “INTERNATIONAL COMMUNICATION” means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

Internet Backbone: The term “INTERNET BACKBONE” means the set of high-capacity cables, switches, and routers that facilitates both domestic and international Internet communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

Internet Communication: The term “INTERNET COMMUNICATION” means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

Internet Packet: The term “INTERNET PACKET” means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol (“IP”) address and some payload.

Internet Transaction: The term “INTERNET TRANSACTION” has the same meaning as “Internet transaction” within the PCLOB Report at pages 39 and 125 and note 517.

NSA: The terms “National Security Agency” and “NSA” include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA’s direction.

Parties: The terms “PLAINTIFF” and “DEFENDANT,” as well as a party’s full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors, employees, agents, representatives, attorneys, consultants, and contractors. This definition is not

intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court's jurisdiction to enter any appropriate order.

Person: The term "PERSON" is defined as any natural person or any business, legal or governmental entity, or association.

Process: The term "PROCESS" has the same meaning as "process," "process[ed]," or "process[ing]" within the July 2014 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, *available at* <https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf> ("2014 NSA Minimization Procedures").

Retain: The term "RETAIN" has the same meaning as "retain," "retained," or "retention" within the 2014 NSA Minimization Procedures.

Review: The term "REVIEW" means to scan, search, screen, capture, monitor, analyze, redirect, divert, or gather information about the contents of.

Selector: The term "SELECTOR" has the same meaning as "selector" within the 2014 NSA Minimization Procedures.

Target: The term "TARGET" means the subjects who are "targeted" pursuant to 50 U.S.C. § 1881a.

United States: When used as a term of geographic location, "UNITED STATES" means all areas under the territorial sovereignty of the United States.

Wholly Domestic Communication: The term "WHOLLY DOMESTIC COMMUNICATION" means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

You/Your: The terms “YOU” or “YOUR” include the defendant agency, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. “All” means “any and all”; “any” means “any and all.” “Including” means “including but not limited to.” “And” and “or” encompass both “and” and “or.” Words in the masculine, feminine, or neutral form shall include each of the other genders.

INSTRUCTIONS

1. YOU are requested to answer each Request for Admission set forth below separately and completely in writing under oath. In answering these Requests for Admission, respond truthfully and in good faith on the basis of all information that is known or readily obtainable by YOU.

2. As required by Federal Rule of Civil Procedure 36(a)(4), if good faith requires that YOU deny only a portion of any matter as to which an admission is requested, or that YOU qualify any response as to any given Request for Admission, specify and admit so much of the Request as is true and deny or qualify only that portion of the Request as to which good faith requires a denial or qualification.

3. Each Request for Admission shall be answered fully unless it is objected to in good faith, in which event the reasons for YOUR objection shall be stated in detail. If an objection pertains to only a portion of a Request for Admission, or a word, phrase, or clause contained within it, YOU are required to state YOUR objection to that portion only and to respond to the remainder of the Request for Admission, using YOUR best efforts to do so.

4. If YOU assert that any information responsive to any Request for Admission is privileged or otherwise protected from discovery, YOU are requested to expressly make a claim of privilege and to describe the nature of the information not disclosed, in a manner that, without revealing information itself privileged or protected, will enable PLAINTIFF to assess the claim of privilege. For any DOCUMENT or information withheld on the grounds that it is privileged or otherwise claimed to be excludable from discovery, identify the information or DOCUMENT, describe its subject matter and date, identify all authors and all recipients (including copied and blind copied recipients), and specify the basis for the claimed privilege or other grounds of exclusion.

5. YOUR responses to these Requests should be based upon information known to YOU CONCERNING facts or events that occurred, in whole or in part, as of June 22, 2015.

6. These Requests for Admission are continuing in nature and YOUR responses to them are to be promptly supplemented or amended if, after the time of YOUR initial responses, YOU learn that any response is or has become in some material respect incomplete or incorrect, to the full extent provided for by Federal Rule of Civil Procedure 26(e).

7. To the extent any of these Requests require PLAINTIFF'S email addresses, IP addresses, or other similar identifiers to respond, PLAINTIFF will serve YOU that information separately.

8. To the extent any of these Requests involve information that is confidential, proprietary, or private information for which special protection from public disclosure and from use for any purpose other than prosecuting this litigation is warranted, a Stipulated Protective Order to address such information is currently under negotiation.

REQUESTS FOR ADMISSION

REQUEST FOR ADMISSION NO. 34:

Admit that, in conducting Upstream surveillance, the NSA has COPIED at least one WIKIMEDIA INTERNET COMMUNICATION.

REQUEST FOR ADMISSION NO. 35:

Admit that, in conducting Upstream surveillance, the NSA has REVIEWED the content of at least one WIKIMEDIA INTERNET COMMUNICATION.

REQUEST FOR ADMISSION NO. 36:

Admit that, in conducting Upstream surveillance, the NSA has RETAINED at least one WIKIMEDIA INTERNET COMMUNICATION.

Dated: November 29, 2017

/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

Exhibit 4

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

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

* * * * *

PLAINTIFF’S THIRD SET OF REQUESTS FOR ADMISSION

Pursuant to Federal Rule of Civil Procedure 36, Local Rule 104, and Appendix A to the Local Rules, the Wikimedia Foundation (“WIKIMEDIA” or “PLAINTIFF”), by its undersigned attorneys, serves this Third Set of Requests for Admission on defendants National Security Agency (“NSA”) and Admiral Michael S. Rogers, in his official capacity as the Director of the NSA (together, the “DEFENDANTS”), and demands that DEFENDANTS answer each Request for Admission herein in writing and under oath and within thirty (30) days of the date of service of the Requests for Admission, in accordance with the Definitions and Instructions set forth below.

DEFINITIONS

Notwithstanding any definition set forth below, each word, term, or phrase used in this Request is intended to have the broadest meaning permitted under the Federal Rules of Civil Procedure. As used in this Request, the following terms are to be interpreted in accordance with these definitions:

Answer: The term “ANSWER” means Defendants’ Answer to Plaintiff’s First Amended Complaint in this action, filed on October 16, 2017.

Bulk: To COPY or REVIEW INTERNET COMMUNICATIONS in “BULK” means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

Circuit: The term “CIRCUIT” has the ordinary meaning of that term within the telecommunications industry as understood by YOU in the context of Upstream surveillance.

Communication: The term “COMMUNICATION” means information transmitted by any means, whether orally, electronically, by document, or otherwise.

Concern or Concerning: The terms “CONCERN” and “CONCERNING” mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

Copy: The term “COPY” means to duplicate a piece of data (for any duration, no matter how brief).

Describe: The term “DESCRIBE” means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events, agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

Document: The term “DOCUMENT” shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way

to a requested document. A draft or non-identical copy is a separate document within the meaning of the term “DOCUMENT.”

Identify (with respect to PERSONS): When referring to a PERSON, to “IDENTIFY” means to state the PERSON’s full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

Identify (with respect to documents): When referring to documents, to “IDENTIFY” means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

Interacted with: The term “INTERACTED WITH” means to have used a device to COPY or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication or transaction in the ordinary course of its transmission or storage.

International Communication: The term “INTERNATIONAL COMMUNICATION” means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

Internet Backbone: The term “INTERNET BACKBONE” means the set of high-capacity cables, switches, and routers that facilitates both domestic and international Internet

communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

Internet Communication: The term “INTERNET COMMUNICATION” means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

Internet Packet: The term “INTERNET PACKET” means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol (“IP”) address and some payload.

Internet Transaction: The term “INTERNET TRANSACTION” has the same meaning as “Internet transaction” within the PCLOB Report at pages 39 and 125 and note 517.

NSA: The terms “National Security Agency” and “NSA” include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA’s direction.

Parties: The terms “PLAINTIFF” and “DEFENDANT,” as well as a party’s full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors, employees, agents, representatives, attorneys, consultants, and contractors. This definition is not intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court’s jurisdiction to enter any appropriate order.

Person: The term “PERSON” is defined as any natural person or any business, legal or governmental entity, or association.

Process: The term “PROCESS” has the same meaning as “process,” “process[ed],” or “process[ing]” within the July 2014 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, available at <https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf> (“2014 NSA Minimization Procedures”).

Retain: The term “RETAIN” has the same meaning as “retain,” “retained,” or “retention” within the 2014 NSA Minimization Procedures.

Review: The term “REVIEW” means to examine, scan, screen, capture, monitor, analyze, or gather information about the contents of.

Selector: The term “SELECTOR” has the same meaning as “selector” within the 2014 NSA Minimization Procedures.

Target: The term “TARGET” means the subjects who are “targeted” pursuant to 50 U.S.C. § 1881a.

United States: When used as a term of geographic location, “UNITED STATES” means all areas under the territorial sovereignty of the United States.

Wholly Domestic Communication: The term “WHOLLY DOMESTIC COMMUNICATION” means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

You/Your: The terms “YOU” or “YOUR” include the defendant agency, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. “All” means “any and all”; “any” means “any and all.” “Including” means “including but not limited to.” “And” and “or” encompass both “and” and “or.” Words in the masculine, feminine, or neutral form shall include each of the other genders.

INSTRUCTIONS

1. YOU are requested to answer each Request for Admission set forth below separately and completely in writing under oath. In answering these Requests for Admission, respond truthfully and in good faith on the basis of all information that is known or readily obtainable by YOU.

2. As required by Federal Rule of Civil Procedure 36(a)(4), if good faith requires that YOU deny only a portion of any matter as to which an admission is requested, or that YOU qualify any response as to any given Request for Admission, specify and admit so much of the Request as is true and deny or qualify only that portion of the Request as to which good faith requires a denial or qualification.

3. Each Request for Admission shall be answered fully unless it is objected to in good faith, in which event the reasons for YOUR objection shall be stated in detail. If an objection pertains to only a portion of a Request for Admission, or a word, phrase, or clause contained within it, YOU are required to state YOUR objection to that portion only and to respond to the remainder of the Request for Admission, using YOUR best efforts to do so.

4. If YOU assert that any information responsive to any Request for Admission is privileged or otherwise protected from discovery, YOU are requested to expressly make a claim of privilege and to describe the nature of the information not disclosed, in a manner that, without

revealing information itself privileged or protected, will enable PLAINTIFF to assess the claim of privilege. For any DOCUMENT or information withheld on the grounds that it is privileged or otherwise claimed to be excludable from discovery, identify the information or DOCUMENT, describe its subject matter and date, identify all authors and all recipients (including copied and blind copied recipients), and specify the basis for the claimed privilege or other grounds of exclusion.

5. Unless otherwise stated, YOUR responses to these Requests should be based upon information known to YOU CONCERNING facts or events that occurred, in whole or in part, as of June 22, 2015.

6. These Requests for Admission are continuing in nature and YOUR responses to them are to be promptly supplemented or amended if, after the time of YOUR initial responses, YOU learn that any response is or has become in some material respect incomplete or incorrect, to the full extent provided for by Federal Rule of Civil Procedure 26(e).

REQUESTS FOR ADMISSION

REQUEST FOR ADMISSION NO. 37:

Admit that, in conducting Upstream surveillance on or before June 22, 2015, the NSA screened the contents of Internet web traffic (that is, the application layer of HTTP and HTTPS communications).

REQUEST FOR ADMISSION NO. 38:

Admit that, in conducting Upstream surveillance as of the date of the service of this request, the NSA screens the contents of Internet web traffic (that is, the application layer of HTTP and HTTPS communications).

REQUEST FOR ADMISSION NO. 39:

Admit that the document attached hereto as Exhibit A, which describes the monitoring of hundreds of CIRCUITS at one international cable site, is a true and correct excerpted copy of a genuine NSA document.

REQUEST FOR ADMISSION NO. 40:

If YOU contend, for the purpose of contesting jurisdiction in this matter, that encryption bears in any way on the interception, accessing, COPYING, filtering, REVIEWING, ingestion, or RETENTION of WIKIMEDIA'S COMMUNICATIONS in the course of Upstream surveillance, admit that YOU have the ability to decrypt, decipher, or render intelligible the contents of some HTTPS communications subject to Upstream surveillance.

Dated: March 17, 2018

/s/ Ashley Gorski
Ashley Gorski
Patrick Toomey
Asma Peracha
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

Exhibit A

(TS//SI//NF) FAIRVIEW: CLIFFSIDE Site - Collection Resumes After ~5 Months

By [REDACTED] on 2011-08-23 0805

(TS//SI//NF) On 5 Aug 2011, collection of DNR and DNI traffic at the FAIRVIEW CLIFFSIDE trans-pacific cable site resumed, after being down for approximately five months. Collection operations at CLIFFSIDE had been down since 11 March 2011, due to the cable damage as a result of the earthquake off of the coast of Japan. The initial damage assessment showed the loss of collection of 275 E1 DNR circuits and 55 DNI circuits. Since the cable was repaired and returned to service (5 Aug), FAIRVIEW operations has tasked 205 E1 DNR circuits and 37 DNI circuits for collection. Environmental survey continues to compare the old environment footprint to the new environment footprint and FAIRVIEW operations will continue to task collection for all new and restored circuits.

POC: [REDACTED] S35333, [REDACTED] (FAIRVIEW Collection Manager)

Exhibit 5

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

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

* * * * *

INTERROGATORIES

Pursuant to Federal Rule of Civil Procedure 33, Local Rule 104, and Appendix A to the Local Rules, the Wikimedia Foundation (“WIKIMEDIA” or “PLAINTIFF”), by its undersigned attorneys, propounds these Interrogatories, to which defendants National Security Agency (“NSA”); the Office of the Director of National Intelligence (“ODNI”); the United States Department of Justice (“DOJ”); Admiral Michael S. Rogers, in his official capacity as the Director of the NSA; Daniel Coats, in his official capacity as the Director of National Intelligence (“DNI”); and Jefferson B. Sessions, III, in his official capacity as Attorney General (collectively, the “DEFENDANTS”) shall respond separately and fully, in writing and under oath, within the time prescribed by the Federal Rules of Civil Procedure, in accordance with the Definitions and Instructions set forth below.

DEFINITIONS

Notwithstanding any definition below, each word, term, or phrase used in these Interrogatories is intended to have the broadest meaning permitted under the Federal Rules of Civil Procedure. As used in these Interrogatories, the following terms are to be interpreted in accordance with these definitions:

Answer: The term “ANSWER” means Defendants’ Answer to Plaintiff’s First Amended Complaint in this action, filed on October 16, 2017.

Bulk: To COPY or REVIEW INTERNET COMMUNICATIONS in “BULK” means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

Circuit: The term “CIRCUIT” has the same meaning as “circuit” 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,” dated July 2, 2014 (“PCLOB Report”), at pages 36 to 37.

Communication: The term “COMMUNICATION” means information transmitted by any means, whether orally, electronically, by document, or otherwise.

Concern or Concerning: The terms “CONCERN” and “CONCERNING” mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

Copy: The term “COPY” means to duplicate a piece of data (for any duration, no matter how brief).

Describe: The term “DESCRIBE” means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events, agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

Document: The term “DOCUMENT” shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way to a requested document. A draft or non-identical copy is a separate document within the meaning of the term “DOCUMENT.”

Identify (with respect to PERSONS): When referring to a PERSON, to “IDENTIFY” means to state the PERSON’s full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

Identify (with respect to documents): When referring to documents, to “IDENTIFY” means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

Interacted with: “INTERACTED WITH” means to have used a device to COPY or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication.

International Communication: The term “INTERNATIONAL COMMUNICATION” means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

Internet Backbone: The term “INTERNET BACKBONE” means the set of high-capacity cables, switches, and routers that facilitates both domestic and international Internet communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

Internet Communication: The term “INTERNET COMMUNICATION” means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

Internet Packet: The term “INTERNET PACKET” means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol (“IP”) address and some payload.

Internet Transaction: The term “INTERNET TRANSACTION” has the same meaning as “Internet transaction” within the PCLOB Report at pages 39 and 125 and note 517.

NSA: The terms “National Security Agency” and “NSA” include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA’s direction.

Parties: The terms “PLAINTIFF” and “DEFENDANT,” as well as a party’s full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors, employees, agents, representatives, attorneys, consultants, and contractors. This definition is not intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court’s jurisdiction to enter any appropriate order.

Person: The term “PERSON” is defined as any natural person or any business, legal or governmental entity, or association.

Process: The term “PROCESS” has the same meaning as “process,” “process[ed],” or “process[ing]” within the July 2014 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, available at <https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf> (“2014 NSA Minimization Procedures”).

Retain: The term “RETAIN” has the same meaning as “retain,” “retained,” or “retention” within the 2014 NSA Minimization Procedures.

Review: The term “REVIEW” means to scan, search, screen, capture, monitor, analyze, redirect, divert, or gather information about the contents of.

Selector: The term “SELECTOR” has the same meaning as “selector” within the 2014 NSA Minimization Procedures.

Target: The term “TARGET” means the subjects who are “targeted” pursuant to 50 U.S.C. § 1881a.

United States: When used as a term of geographic location, “UNITED STATES” means all areas under the territorial sovereignty of the United States.

Wholly Domestic Communication: The term “WHOLLY DOMESTIC COMMUNICATION” means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

You/Your: The terms “YOU” or “YOUR” include the defendant agency, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. “All” means “any and all”; “any” means “any and all.” “Including” means “including but not limited to.” “And” and “or” encompass both “and” and “or.” Words in the masculine, feminine, or neutral form shall include each of the other genders.

INSTRUCTIONS

1. YOU are requested to answer each Interrogatory set forth below separately and completely in writing under oath. YOUR response hereto is to be signed and verified by the person making it, and the objections signed by the attorney making them, as required by Federal Rule of Civil Procedure 33(b). It is intended that the following discovery requests will not solicit any information protected either by the attorney–client privilege or work product doctrine which was created or developed by counsel for the responding party after the date on which this litigation was commenced. If any inquiry is susceptible of a construction which calls for the production of such information, that material need not be provided and no privilege log pursuant to Federal Rule of Civil Procedure 26(b)(5) or Discovery Guideline 10(d) will be required as to such information.

2. Each Interrogatory shall be answered fully unless it is objected to in good faith, in which event the reasons for YOUR objection shall be stated in detail. Pursuant to Discovery Guideline 10(b), no part of an Interrogatory should be left unanswered merely because an objection is interposed to another part of the Interrogatory. Pursuant to Discovery Guideline

10(a), if a partial or incomplete answer is provided, the responding party shall state that the answer is partial or incomplete.

3. If any DOCUMENT or oral COMMUNICATION coming within the Interrogatories is withheld on any basis, such as a claim of attorney–client privilege or attorney work product, YOU are to IDENTIFY each such DOCUMENT or oral COMMUNICATION and provide the following information, unless divulging such information would cause disclosure of allegedly privileged information:

(A) For oral communications:

- (i) The name of the person making the communication and the names of persons present while the communication was made, and, where not apparent, the relationship of the persons present to the person making the communication;
- (ii) The date and place of the communication;
- (iii) The general subject matter of the communication; and
- (iv) The nature of the claimed privilege so as to explain the basis asserted for withholding the oral communication in sufficient detail so as to enable the claim of privilege to be adjudicated, if necessary.

(B) For DOCUMENTS:

- (i) The type of DOCUMENT (e.g., letter, memorandum, email, etc.);
- (ii) Its date, if any, or an estimate thereof, and so indicated as an estimate if no date appears on the DOCUMENT;
- (iii) Its author(s), if any;
- (iv) Its addressee(s), if any, and, where not apparent, the relationship between its author(s) and addressee(s);
- (v) The names of all persons or entities to whom the DOCUMENT, thing, or

copies thereof were circulated or its contents communicated, if any;

(vi) The general subject matter of the DOCUMENT; and

(vii) The nature of the claimed privilege so as to explain the basis asserted for withholding the DOCUMENT or thing in sufficient detail so as to enable the claim of privilege to be adjudicated, if necessary.

4. To the extent any purportedly privileged DOCUMENT contains non-privileged subject matter, the non-privileged portion must be produced to the fullest extent possible with the purportedly privileged material redacted.

5. If YOU elect to specify and produce business records in answer to any interrogatory, the specification shall be in sufficient detail to permit PLAINTIFF to locate and IDENTIFY, as readily as YOU can, the business records from which the answer may be ascertained or, if produced electronically, produced in a manner consistent with the District of Maryland's Guideline 2.04 of the ESI Principles.

6. If an Interrogatory is silent as to the time period for which information is sought, YOUR response should include all information known to YOU CONCERNING events that occurred, in whole or in part, at any time during the time period of January 1, 2014 to November 7, 2017. If YOUR response is different as to particular time periods between January 1, 2014 and November 7, 2017, so state and provide all information known to YOU CONCERNING events with respect to each period.

7. These Interrogatories are continuing in nature and YOU must promptly supplement or amend YOUR responses to them if, after the time of YOUR initial responses, YOU learn that any response is or has become in some material respect incomplete or incorrect, to the full extent provided for by Federal Rule of Civil Procedure 26(e).

8. If, in answering these Interrogatories, the responding party encounters any ambiguities when construing a question, instruction, or definition, the responding party's answer shall set forth the matter deemed ambiguous and the construction used in answering.

INTERROGATORIES

INTERROGATORY NO. 1:

DESCRIBE YOUR understanding of the definition of the term "international Internet link" as 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)—and provide all information supporting that understanding.

INTERROGATORY NO. 2:

DESCRIBE YOUR understanding of the definition of the term "circuit" as used at pages 36 to 37 of the PCLOB Report, and provide all information supporting that understanding, including but not limited to all information furnished by DEFENDANTS to the Privacy and Civil Liberties Oversight Board concerning this term.

INTERROGATORY NO. 3:

DESCRIBE YOUR understanding of the definition of the term "filtering mechanism" as used at pages 10 and 47–48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

INTERROGATORY NO. 4:

DESCRIBE YOUR understanding of the definition of the term "scanned" as used at page 10 of the Memorandum in Support of Defendants' Motion to Dismiss the First Amended

Complaint, *Wikimedia Foundation v. NSA*, No. 15-cv-662-TSE (D. Md. Aug. 6, 2015), and provide all information supporting that understanding.

INTERROGATORY NO. 5:

DESCRIBE YOUR understanding of the definition of the term “screen” as used at page 48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

INTERROGATORY NO. 6:

DESCRIBE YOUR understanding of the definition of the term “discrete communication” as used in the 2014 NSA Minimization Procedures, and provide all information supporting that understanding.

INTERROGATORY NO. 7:

DESCRIBE YOUR understanding of all features that a series of INTERNET PACKETS comprising an “Internet transaction” has in common, as the term “Internet transaction” is used in at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding. For example, the INTERNET PACKETS comprising an “Internet transaction” might share source and destination IP addresses, source and destination ports, and protocol type (albeit with the source and destination IP addresses and ports reversed for packets flowing in the opposite direction).

INTERROGATORY NO. 8:

DESCRIBE YOUR understanding of the definitions of the terms “single communication transaction” and “multi-communication transaction” as used by the government in its submission to the Foreign Intelligence Surveillance Court, filed on August 16, 2011, and provide all

information supporting that understanding. *See* [Redacted], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011).

INTERROGATORY NO. 9:

DESCRIBE YOUR understanding of the definitions of the terms “access” and “larger body of international communications” as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

INTERROGATORY NO. 10:

DESCRIBE YOUR understanding of the definition of the term “acquired” as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

INTERROGATORY NO. 11:

DESCRIBE YOUR understanding of the definition of the term “collection” as used at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

INTERROGATORY NO. 12:

DESCRIBE YOUR understanding of the definition of the term “Internet ‘backbone’” as used at page 1 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

INTERROGATORY NO. 13:

DESCRIBE in detail all steps taken by the NSA to PROCESS communications in the course of Upstream surveillance.

INTERROGATORY NO. 14:

DESCRIBE the entire process by which, pursuant to Upstream surveillance, the contents of INTERNET COMMUNICATIONS are INTERACTED WITH.

Dated: November 7, 2017

/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

Exhibit 6

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

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

* * * * *

PLAINTIFF’S SECOND SET OF INTERROGATORIES

Pursuant to Federal Rule of Civil Procedure 33, Local Rule 104, and Appendix A to the Local Rules, the Wikimedia Foundation (“WIKIMEDIA” or “PLAINTIFF”), by its undersigned attorneys, propounds these Interrogatories, to which defendants National Security Agency (“NSA”) and Admiral Michael S. Rogers, in his official capacity as the Director of the NSA (together, the “DEFENDANTS”), shall respond fully, in writing and under oath, within the time prescribed by the Federal Rules of Civil Procedure, in accordance with the Definitions and Instructions set forth below.

DEFINITIONS

Notwithstanding any definition below, each word, term, or phrase used in these Interrogatories is intended to have the broadest meaning permitted under the Federal Rules of Civil Procedure. As used in these Interrogatories, the following terms are to be interpreted in accordance with these definitions:

Answer: The term “ANSWER” means Defendants’ Answer to Plaintiff’s First Amended Complaint in this action, filed on October 16, 2017.

Bulk: To COPY or REVIEW INTERNET COMMUNICATIONS in “BULK” means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

Circuit: The term “CIRCUIT” has the ordinary meaning of that term within the telecommunications industry as understood by YOU in the context of Upstream surveillance.

Communication: The term “COMMUNICATION” means information transmitted by any means, whether orally, electronically, by document, or otherwise.

Concern or Concerning: The terms “CONCERN” and “CONCERNING” mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

Copy: The term “COPY” means to duplicate a piece of data (for any duration, no matter how brief).

Describe: The term “DESCRIBE” means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events, agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

Document: The term “DOCUMENT” shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way

to a requested document. A draft or non-identical copy is a separate document within the meaning of the term “DOCUMENT.”

Identify (with respect to PERSONS): When referring to a PERSON, to “IDENTIFY” means to state the PERSON’s full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

Identify (with respect to documents): When referring to documents, to “IDENTIFY” means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

Interacted with: “INTERACTED WITH” means to have used a device to COPY or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication.

International Communication: The term “INTERNATIONAL COMMUNICATION” means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

Internet Backbone: The term “INTERNET BACKBONE” means the set of high-capacity cables, switches, and routers that facilitates both domestic and international Internet

communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

Internet Communication: The term “INTERNET COMMUNICATION” means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

Internet Packet: The term “INTERNET PACKET” means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol (“IP”) address and some payload.

Internet Transaction: The term “INTERNET TRANSACTION” has the same meaning as “Internet transaction” within the PCLOB Report at pages 39 and 125 and note 517.

NSA: The terms “National Security Agency” and “NSA” include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA’s direction.

Parties: The terms “PLAINTIFF” and “DEFENDANT,” as well as a party’s full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors, employees, agents, representatives, attorneys, consultants, and contractors. This definition is not intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court’s jurisdiction to enter any appropriate order.

Person: The term “PERSON” is defined as any natural person or any business, legal or governmental entity, or association.

Process: The term “PROCESS” has the same meaning as “process,” “process[ed],” or “process[ing]” within the July 2014 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, *available at* <https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf> (“2014 NSA Minimization Procedures”).

Retain: The term “RETAIN” has the same meaning as “retain,” “retained,” or “retention” within the 2014 NSA Minimization Procedures.

Review: The term “REVIEW” means to examine, scan, screen, capture, monitor, analyze, or gather information about the contents of.

Selector: The term “SELECTOR” has the same meaning as “selector” within the 2014 NSA Minimization Procedures.

Target: The term “TARGET” means the subjects who are “targeted” pursuant to 50 U.S.C. § 1881a.

United States: When used as a term of geographic location, “UNITED STATES” means all areas under the territorial sovereignty of the United States.

Wholly Domestic Communication: The term “WHOLLY DOMESTIC COMMUNICATION” means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

You/Your: The terms “YOU” or “YOUR” mean the defendant agency these interrogatories are served on, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. “All” means “any and all”; “any” means “any and all.” “Including” means “including but not limited to.” “And” and “or” encompass both “and” and “or.” Words in the masculine, feminine, or neutral form shall include each of the other genders.

INSTRUCTIONS

1. YOU are requested to answer each Interrogatory set forth below separately and completely in writing under oath. YOUR response hereto is to be signed and verified by the person making it, and the objections signed by the attorney making them, as required by Federal Rule of Civil Procedure 33(b). It is intended that the following discovery requests will not solicit any communications with counsel that refer or relate to this lawsuit and that are subject to the attorney-client privilege or work-product protection. If any inquiry is susceptible of a construction which calls for the production of such information, that material need not be provided and no privilege log pursuant to Federal Rule of Civil Procedure 26(b)(5) or Discovery Guideline 10(d) will be required as to such information.

2. Each Interrogatory shall be answered fully unless it is objected to in good faith, in which event the reasons for YOUR objection shall be stated in detail. Pursuant to Discovery Guideline 10(b), no part of an Interrogatory should be left unanswered merely because an objection is interposed to another part of the Interrogatory. Pursuant to Discovery Guideline 10(a), if a partial or incomplete answer is provided, the responding party shall state that the answer is partial or incomplete.

3. If any DOCUMENT or oral COMMUNICATION coming within the Interrogatories is withheld on any basis, such as a claim of attorney–client privilege or attorney

work product, YOU are to IDENTIFY each such DOCUMENT or oral COMMUNICATION and provide the following information, unless divulging such information would cause disclosure of allegedly privileged information:

(A) For oral communications:

- (i) The name of the person making the communication and the names of persons present while the communication was made, and, where not apparent, the relationship of the persons present to the person making the communication;
- (ii) The date and place of the communication;
- (iii) The general subject matter of the communication; and
- (iv) The nature of the claimed privilege so as to explain the basis asserted for withholding the oral communication in sufficient detail so as to enable the claim of privilege to be adjudicated, if necessary.

(B) For DOCUMENTS:

- (i) The type of DOCUMENT (e.g., letter, memorandum, email, etc.);
- (ii) Its date, if any, or an estimate thereof, and so indicated as an estimate if no date appears on the DOCUMENT;
- (iii) Its author(s), if any;
- (iv) Its addressee(s), if any, and, where not apparent, the relationship between its author(s) and addressee(s);
- (v) The names of all persons or entities to whom the DOCUMENT, thing, or copies thereof were circulated or its contents communicated, if any;
- (vi) The general subject matter of the DOCUMENT; and

(vii) The nature of the claimed privilege so as to explain the basis asserted for withholding the DOCUMENT or thing in sufficient detail so as to enable the claim of privilege to be adjudicated, if necessary.

4. To the extent any purportedly privileged DOCUMENT contains non-privileged subject matter, the non-privileged portion must be produced to the fullest extent possible with the purportedly privileged material redacted.

5. If YOU elect to specify and produce business records in answer to any interrogatory, the specification shall be in sufficient detail to permit PLAINTIFF to locate and IDENTIFY, as readily as YOU can, the business records from which the answer may be ascertained or, if produced electronically, produced in a manner consistent with the District of Maryland's Guideline 2.04 of the ESI Principles.

6. If an Interrogatory is silent as to the time period for which information is sought, YOUR response should include all information known to YOU CONCERNING events that occurred, in whole or in part, at any time during the time period of January 1, 2014 to March 17, 2018. If YOUR response is different as to particular time periods between January 1, 2014 and March 17, 2018, so state and provide all information known to YOU CONCERNING events with respect to each period.

7. These Interrogatories are continuing in nature and YOU must promptly supplement or amend YOUR responses to them if, after the time of YOUR initial responses, YOU learn that any response is or has become in some material respect incomplete or incorrect, to the full extent provided for by Federal Rule of Civil Procedure 26(e).

8. If, in answering these Interrogatories, the responding party encounters any ambiguities when construing a question, instruction, or definition, the responding party's answer shall set forth the matter deemed ambiguous and the construction used in answering.

INTERROGATORIES

INTERROGATORY NO. 15:

DESCRIBE any and all statements or facts YOU contend are inaccurate concerning Upstream surveillance in pages 7-10, 22, 32-33, 35-41 & n.157, 79, 111 n.476, 119-26, and 143-45 of the Privacy and Civil Liberties Oversight Board's *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), based on Upstream surveillance as it was conducted on the date the report was publicly released.

INTERROGATORY NO. 16:

DESCRIBE the approximate percentage of CIRCUITS carrying Internet communications into or out of the United States (not CIRCUITS carrying solely telephonic or private network communications) that were monitored in the course of Upstream surveillance in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.

INTERROGATORY NO. 17:

DESCRIBE the approximate percentage of international submarine cables carrying Internet communications into or out of the United States (not international submarine cables carrying solely telephonic or private network communications) that were monitored in the course of Upstream surveillance in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.

INTERROGATORY NO. 18:

DESCRIBE, by any metric commonly used in the telecommunications industry, such as bytes or packets, the approximate amount of Internet traffic that was subject to filtering in the course of Upstream surveillance, prior to retaining Internet communications that contain a selector, in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.

INTERROGATORY NO. 19:

DESCRIBE, by any metric commonly used in the telecommunications industry, such as bytes or packets, the approximate amount of Internet traffic that was screened in the course of Upstream surveillance, prior to retaining Internet communications that contain a selector, in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.

INTERROGATORY NO. 20:

If YOU contend, for the purpose of contesting jurisdiction in this matter, that encryption bears in any way on the interception, accessing, COPYING, filtering, REVIEWING, ingestion, or RETENTION of WIKIMEDIA'S COMMUNICATIONS in the course of Upstream surveillance, DESCRIBE the protocols used to encrypt INTERNET COMMUNICATIONS or INTERNET TRANSACTIONS subject to Upstream surveillance for which the NSA has the ability to decrypt, decipher, or render intelligible the contents of those COMMUNICATIONS.

Dated: March 17, 2018

/s/ Ashley Gorski
Ashley Gorski
Patrick Toomey

Asma Peracha
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

Exhibit 7

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

WIKIMEDIA FOUNDATION,

*

Plaintiff,

*

v.

* **Civil Action No.: 15-cv-00662-TSE**

NATIONAL SECURITY AGENCY, *et al.*,

*

Defendants.

*

* * * * *

REQUEST FOR PRODUCTION OF DOCUMENTS

Pursuant to Federal Rule of Civil Procedure 34, Local Rule 104, and Appendix A to the Local Rules, the Wikimedia Foundation (“WIKIMEDIA” or “PLAINTIFF”), by its undersigned attorneys, requests that defendants National Security Agency (“NSA”); the Office of the Director of National Intelligence (“ODNI”); the United States Department of Justice (“DOJ”); Admiral Michael S. Rogers, in his official capacity as the Director of the NSA; Daniel Coats, in his official capacity as the Director of National Intelligence (“DNI”); and Jefferson B. Sessions, III, in his official capacity as Attorney General (collectively, the “DEFENDANTS”), respond to this Request within the time prescribed by Federal Rule of Civil Procedure 34(b), and produce or make available for inspection and copying the following documents and electronically stored information (“ESI”) on the 7th day of December, 2017, and continuing from day to day thereafter, until completed, at the offices of the American Civil Liberties Union Foundation, 125 Broad Street, 18th floor, New York, New York, 10004, in accordance with the Definitions and Instructions set forth below.

DEFINITIONS

Notwithstanding any definition set forth below, each word, term, or phrase used in this Request is intended to have the broadest meaning permitted under the Federal Rules of Civil Procedure. As used in this Request, the following terms are to be interpreted in accordance with these definitions:

Answer: The term “ANSWER” means Defendants’ Answer to Plaintiff’s First Amended Complaint in this action, filed on October 16, 2017.

Bulk: To COPY or REVIEW INTERNET COMMUNICATIONS in “BULK” means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

Circuit: The term “CIRCUIT” has the same meaning as “circuit” 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,” dated July 2, 2014 (“PCLOB Report”), at pages 36 to 37.

Communication: The term “COMMUNICATION” means information transmitted by any means, whether orally, electronically, by document, or otherwise.

Concern or Concerning: The terms “CONCERN” and “CONCERNING” mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

Copy: The term “COPY” means to duplicate a piece of data (for any duration, no matter how brief).

Describe: The term “DESCRIBE” means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events, agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

Document: The term “DOCUMENT” shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way to a requested document. A draft or non-identical copy is a separate document within the meaning of the term “DOCUMENT.”

Identify (with respect to PERSONS): When referring to a PERSON, to “IDENTIFY” means to state the PERSON’s full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

Identify (with respect to documents): When referring to documents, to “IDENTIFY” means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

Interacted with: “INTERACTED WITH” means to have used a device to COPY or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such

communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication.

International Communication: The term “INTERNATIONAL COMMUNICATION” means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

Internet Backbone: The term “INTERNET BACKBONE” means the set of high-capacity cables, switches, and routers that facilitates both domestic and international Internet communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

Internet Communication: The term “INTERNET COMMUNICATION” means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

Internet Packet: The term “INTERNET PACKET” means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol (“IP”) address and some payload.

Internet Transaction: The term “INTERNET TRANSACTION” has the same meaning as “Internet transaction” within the PCLOB Report at pages 39 and 125 and note 517.

NSA: The terms “National Security Agency” and “NSA” include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA’s direction.

Parties: The terms “PLAINTIFF” and “DEFENDANT,” as well as a party’s full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors, employees, agents, representatives, attorneys, consultants, and contractors. This definition is not intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court’s jurisdiction to enter any appropriate order.

Person: The term “PERSON” is defined as any natural person or any business, legal or governmental entity, or association.

Process: The term “PROCESS” has the same meaning as “process,” “process[ed],” or “process[ing]” within the July 2014 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, available at <https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf> (“2014 NSA Minimization Procedures”).

Retain: The term “RETAIN” has the same meaning as “retain,” “retained,” or “retention” within the 2014 NSA Minimization Procedures.

Review: The term “REVIEW” means to scan, search, screen, capture, monitor, analyze, redirect, divert, or gather information about the contents of.

Selector: The term “SELECTOR” has the same meaning as “selector” within the 2014 NSA Minimization Procedures.

Target: The term “TARGET” means the subjects who are “targeted” pursuant to 50 U.S.C. § 1881a.

United States: When used as a term of geographic location, “UNITED STATES” means all areas under the territorial sovereignty of the United States.

Wholly Domestic Communication: The term “WHOLLY DOMESTIC COMMUNICATION” means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

You/Your: The terms “YOU” or “YOUR” include the defendant agency, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. “All” means “any and all”; “any” means “any and all.” “Including” means “including but not limited to.” “And” and “or” encompass both “and” and “or.” Words in the masculine, feminine, or neutral form shall include each of the other genders.

INSTRUCTIONS

1. Responsive DOCUMENTS include those in YOUR possession, custody, or control.
2. Each DOCUMENT or tangible thing produced in response hereto shall be produced as it is kept in the ordinary course of business, including all file folders, binders, notebooks, and other devices by which such papers or things may be organized or separated, or it shall be organized and labeled to correspond with the Request(s) to which it is responsive. If the requested DOCUMENTS are maintained in a file, the file folder is included in the request for production of those DOCUMENTS.
3. DOCUMENTS that are in the form of electronically stored information are to be produced as follows: (1) for Microsoft Excel and Microsoft Power Point DOCUMENTS, in their native format; and (2) for all other DOCUMENTS, as single-page “.tiff” images with extracted

text, whenever such text is available, and with accompanying optical character recognition files where extracted text is unavailable, and with all reasonably available metadata fields. Upon review of the production, WIKIMEDIA reserves its right to request that YOU produce additional metadata for particular DOCUMENTS, and that certain DOCUMENTS or things be produced in native or other format. This instruction may be superseded by the agreement of the PLAINTIFF and DEFENDANTS as to the appropriate format for production of electronically stored information.

4. All DOCUMENTS that are physically attached to each other shall be produced in that form. DOCUMENTS that are segregated or separated from other DOCUMENTS, whether by inclusion in binders, files, or sub-files, or by the use of dividers, tabs, or any other method, shall be produced in that form. DOCUMENTS shall be produced in the order in which they were maintained.

5. If any copy of any DOCUMENT is not identical to the original or any other copy thereof by reason of any alteration, marginalia, comment, or other material contained therein, thereon, or attached thereto, or otherwise, all such non-identical copies shall be produced separately.

6. Pursuant to Federal Rule of Civil Procedure 34(b)(2)(B), if YOU object to a Request, the grounds for each objection must be stated with specificity. If an objection pertains to only a portion of a Request, a word, phrase, or clause contained within it, YOU must state the objection to that portion only and respond to the remainder of the request, using YOUR best efforts to do so. Also pursuant to Federal Rule of Civil Procedure 34(b)(2)(B), if YOU intended to produce copies of DOCUMENTS or of ESI instead of permitting inspection, YOU must so state.

7. If, in responding to this Request for Production, YOU encounter any ambiguities when construing a request or definition, the response shall set forth the matter deemed ambiguous and the construction used in responding.

8. Pursuant to Federal Rule of Civil Procedure 34(b)(2)(C), an objection must state whether any responsive materials are being withheld on the basis of that objection.

9. Whenever in this Request YOU are asked to identify or produce a DOCUMENT which is deemed by YOU to be properly withheld from production for inspection or copying:

A. If YOU are withholding the DOCUMENT under claim of privilege (including, but not limited to, the work product doctrine), please provide a log identifying each such document by specifying:

(i) The type of DOCUMENT (e.g., letter, memorandum, email, etc.) or some other means of accurately identifying it;

(ii) Its date, if any, or an estimate thereof, and so indicated as an estimate if no date appears on the DOCUMENT;

(iii) Its author(s), if any;

(iv) Its addressee(s), if any, and, where not apparent, the relationship between its author(s) and addressee(s);

(v) Each recipient and addresses of all PERSONS or entities to whom the DOCUMENT, thing, or copies thereof were circulated or its contents communicated, if any;

(vi) The general subject matter of the DOCUMENT; and

(vii) The nature of the claimed privilege so as to explain the basis asserted

for withholding the DOCUMENT or thing in sufficient detail so as to enable the claim of privilege to be adjudicated, if necessary.

- B. If YOU are withholding the DOCUMENT for any reason other than an objection that it is beyond the scope of discovery, identify as to each document and, in addition to the information requested in paragraph 9.A above, please state the reason for withholding the DOCUMENT. If YOU are withholding production on the basis that ESI is not reasonably accessible because of undue burden or cost, provide the information required by Discovery Guideline 10(e) under Appendix A to the Local Rules.

10. When a DOCUMENT contains both privileged and non-privileged material, the non-privileged material must be disclosed to the fullest extent possible with the purportedly privileged material redacted.

11. If a privilege is asserted with regard to part of the material contained in a DOCUMENT, the party claiming the privilege must clearly indicate the portions as to which the privilege is claimed.

12. When a DOCUMENT has been redacted or altered in any fashion, identify as to each DOCUMENT the reason for the redaction or alteration, the date of the redaction or alteration, and the PERSON performing the redaction or alteration. Any redaction must be clearly visible on the redacted DOCUMENT.

13. Any DOCUMENT or things requested that cannot be produced in full should be produced to the extent possible, specifying the reasons for the inability to produce the remainder and stating whatever information, knowledge, or belief YOU have CONCERNING the unproduced portion.

14. It is intended that these Requests will not solicit any material protected either by the attorney–client privilege or by the work product doctrine which was created by, or developed by, counsel for the responding party after the date on which this litigation was commenced. If any Request is susceptible of a construction which calls for the production of such material, that material need not be provided and no privilege log pursuant to Federal Rule of Civil Procedure 26(b)(5) or Discovery Guideline 9(a) will be required as to such material.

15. These Requests are continuing so as to require prompt supplemental responses as required under Federal Rule of Civil Procedure 26(e) up to and including the time of trial of the present dispute. If YOU come into possession, custody, or control of responsive DOCUMENTS or things after the initial production, YOU should supplement the production by promptly producing such DOCUMENTS or things.

16. If a Request is silent as to the time period for which information is sought, YOUR response should include all information known to YOU CONCERNING events that occurred, in whole or in part, at any time during the time period of July 8, 2008 to November 7, 2017.

REQUESTS FOR PRODUCTION

REQUEST FOR PRODUCTION NO. 1:

All DOCUMENTS referenced, paraphrased, or summarized in YOUR answers to Interrogatories.

REQUEST FOR PRODUCTION NO. 2:

DOCUMENTS sufficient to show or estimate the average number of optical fibers within the international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

REQUEST FOR PRODUCTION NO. 3:

All DOCUMENTS listing, depicting, tallying, or describing the international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

REQUEST FOR PRODUCTION NO. 4:

All DOCUMENTS listing, depicting, tallying, or describing the points at which international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES arrive at or depart from the UNITED STATES.

REQUEST FOR PRODUCTION NO. 5:

All DOCUMENTS listing, depicting, tallying, or describing the terrestrial cables that are part of the INTERNET BACKBONE within the UNITED STATES.

REQUEST FOR PRODUCTION NO. 6:

DOCUMENTS sufficient to show or estimate the number of persons TARGETED for Upstream surveillance pursuant to 50 U.S.C. § 1881a in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

REQUEST FOR PRODUCTION NO. 7:

DOCUMENTS sufficient to show or estimate the number of SELECTORS used in conducting Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

REQUEST FOR PRODUCTION NO. 8:

DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS COPIED using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

REQUEST FOR PRODUCTION NO. 9:

DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS REVIEWED for SELECTORS using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

REQUEST FOR PRODUCTION NO. 10:

DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS RETAINED using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

REQUEST FOR PRODUCTION NO. 11:

DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS RETAINED using Upstream surveillance that are to, from, or about “U.S. persons,” as defined at 50 U.S.C. § 1801(i), in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

REQUEST FOR PRODUCTION NO. 12:

DOCUMENTS sufficient to show or estimate the average number of discrete INTERNET COMMUNICATIONS contained in a multi-communication transaction.

REQUEST FOR PRODUCTION NO. 13:

DOCUMENTS sufficient to show or estimate the number of CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

REQUEST FOR PRODUCTION NO. 14:

DOCUMENTS sufficient to show or estimate the combined bandwidth of the CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

REQUEST FOR PRODUCTION NO. 15:

DOCUMENTS sufficient to show or estimate the number of “international Internet link[s]”— as that term was 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)—monitored using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

REQUEST FOR PRODUCTION NO. 16:

DOCUMENTS sufficient to show or estimate the number of Internet “chokepoints” or “choke points” (as that term is used by YOU) inside the UNITED STATES through which INTERNATIONAL COMMUNICATIONS enter and leave the UNITED STATES and where the NSA has established Upstream surveillance collection or PROCESSING capabilities.

REQUEST FOR PRODUCTION NO. 17:

All DOCUMENTS defining or describing the meaning of the term “Internet transaction.”

REQUEST FOR PRODUCTION NO. 18:

All Foreign Intelligence Surveillance Court–approved targeting procedures relevant at any time to DEFENDANTS’ implementation of Upstream surveillance.

REQUEST FOR PRODUCTION NO. 19:

All Foreign Intelligence Surveillance Court–approved minimization procedures relevant at any time to DEFENDANTS’ implementation of Upstream surveillance.

REQUEST FOR PRODUCTION NO. 20:

Any supplemental procedures relevant at any time to DEFENDANTS’ implementation of Upstream surveillance.

REQUEST FOR PRODUCTION NO. 21:

All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court orders and opinions CONCERNING Upstream surveillance.

REQUEST FOR PRODUCTION NO. 22:

All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court submissions CONCERNING Upstream surveillance.

Dated: November 7, 2017

/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

Exhibit 8

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

WIKIMEDIA FOUNDATION,

*

Plaintiff,

*

v.

* **Civil Action No.: 15-cv-00662-TSE**

NATIONAL SECURITY AGENCY, *et al.*,

*

Defendants.

*

* * * * *

PLAINTIFF’S SECOND SET OF REQUESTS FOR PRODUCTION OF DOCUMENTS

Pursuant to Federal Rule of Civil Procedure 34, Local Rule 104, and Appendix A to the Local Rules, the Wikimedia Foundation (“WIKIMEDIA” or “PLAINTIFF”), by its undersigned attorneys, requests that defendants National Security Agency (“NSA”); the Office of the Director of National Intelligence (“ODNI”); the United States Department of Justice (“DOJ”); Admiral Michael S. Rogers, in his official capacity as the Director of the NSA; Daniel Coats, in his official capacity as the Director of National Intelligence (“DNI”); and Jefferson B. Sessions, III, in his official capacity as Attorney General (collectively, the “DEFENDANTS”), respond to this Request within the time prescribed by Federal Rule of Civil Procedure 34(b), and produce or make available for inspection and copying the following documents and electronically stored information (“ESI”) on the 29th day of December, 2017, and continuing from day to day thereafter, until completed, at the offices of the American Civil Liberties Union Foundation, 125 Broad Street, 18th floor, New York, New York, 10004, in accordance with the Definitions and Instructions set forth below.

DEFINITIONS

Notwithstanding any definition set forth below, each word, term, or phrase used in this Request is intended to have the broadest meaning permitted under the Federal Rules of Civil Procedure. As used in this Request, the following terms are to be interpreted in accordance with these definitions:

Answer: The term “ANSWER” means Defendants’ Answer to Plaintiff’s First Amended Complaint in this action, filed on October 16, 2017.

Bulk: To COPY or REVIEW INTERNET COMMUNICATIONS in “BULK” means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

Circuit: The term “CIRCUIT” has the same meaning as “circuit” 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,” dated July 2, 2014 (“PCLOB Report”), at pages 36 to 37.

Communication: The term “COMMUNICATION” means information transmitted by any means, whether orally, electronically, by document, or otherwise.

Concern or Concerning: The terms “CONCERN” and “CONCERNING” mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

Copy: The term “COPY” means to duplicate a piece of data (for any duration, no matter how brief).

Describe: The term “DESCRIBE” means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events, agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

Document: The term “DOCUMENT” shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way to a requested document. A draft or non-identical copy is a separate document within the meaning of the term “DOCUMENT.”

Identify (with respect to PERSONS): When referring to a PERSON, to “IDENTIFY” means to state the PERSON’s full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

Identify (with respect to documents): When referring to documents, to “IDENTIFY” means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

Interacted with: The term “INTERACTED WITH” means to have used a device to COPY or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION

while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication or transaction in the ordinary course of its transmission or storage.

Interaction with: The term “INTERACTION WITH” means the use of a device to COPY or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication or transaction in the ordinary course of its transmission or storage.

International Communication: The term “INTERNATIONAL COMMUNICATION” means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

Internet Backbone: The term “INTERNET BACKBONE” means the set of high-capacity cables, switches, and routers that facilitates both domestic and international Internet communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

Internet Communication: The term “INTERNET COMMUNICATION” means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

Internet Packet: The term “INTERNET PACKET” means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol (“IP”) address and some payload.

Internet Transaction: The term “INTERNET TRANSACTION” has the same meaning as “Internet transaction” within the PCLOB Report at pages 39 and 125 and note 517.

NSA: The terms “National Security Agency” and “NSA” include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA’s direction.

Parties: The terms “PLAINTIFF” and “DEFENDANT,” as well as a party’s full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors, employees, agents, representatives, attorneys, consultants, and contractors. This definition is not intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court’s jurisdiction to enter any appropriate order.

Person: The term “PERSON” is defined as any natural person or any business, legal or governmental entity, or association.

Process: The term “PROCESS” has the same meaning as “process,” “process[ed],” or “process[ing]” within the July 2014 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, available at <https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf> (“2014 NSA Minimization Procedures”).

Retain: The term “RETAIN” has the same meaning as “retain,” “retained,” or “retention” within the 2014 NSA Minimization Procedures.

Review: The term “REVIEW” means to scan, search, screen, capture, monitor, analyze, redirect, divert, or gather information about the contents of.

Selector: The term “SELECTOR” has the same meaning as “selector” within the 2014 NSA Minimization Procedures.

Target: The term “TARGET” means the subjects who are “targeted” pursuant to 50 U.S.C. § 1881a.

United States: When used as a term of geographic location, “UNITED STATES” means all areas under the territorial sovereignty of the United States.

Wholly Domestic Communication: The term “WHOLLY DOMESTIC COMMUNICATION” means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

You/Your: The terms “YOU” or “YOUR” include the defendant agency, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. “All” means “any and all”; “any” means “any and all.” “Including” means “including but not limited to.” “And” and “or” encompass both “and” and “or.” Words in the masculine, feminine, or neutral form shall include each of the other genders.

INSTRUCTIONS

1. Responsive DOCUMENTS include those in YOUR possession, custody, or control.
2. Each DOCUMENT or tangible thing produced in response hereto shall be produced as it is kept in the ordinary course of business, including all file folders, binders, notebooks, and other devices by which such papers or things may be organized or separated, or it

shall be organized and labeled to correspond with the Request(s) to which it is responsive. If the requested DOCUMENTS are maintained in a file, the file folder is included in the request for production of those DOCUMENTS.

3. DOCUMENTS that are in the form of electronically stored information are to be produced as follows: (1) for Microsoft Excel and Microsoft Power Point DOCUMENTS, in their native format; and (2) for all other DOCUMENTS, as single-page “.tiff” images with extracted text, whenever such text is available, and with accompanying optical character recognition files where extracted text is unavailable, and with all reasonably available metadata fields. Upon review of the production, WIKIMEDIA reserves its right to request that YOU produce additional metadata for particular DOCUMENTS, and that certain DOCUMENTS or things be produced in native or other format. This instruction may be superseded by the agreement of the PLAINTIFF and DEFENDANTS as to the appropriate format for production of electronically stored information.

4. All DOCUMENTS that are physically attached to each other shall be produced in that form. DOCUMENTS that are segregated or separated from other DOCUMENTS, whether by inclusion in binders, files, or sub-files, or by the use of dividers, tabs, or any other method, shall be produced in that form. DOCUMENTS shall be produced in the order in which they were maintained.

5. If any copy of any DOCUMENT is not identical to the original or any other copy thereof by reason of any alteration, marginalia, comment, or other material contained therein, thereon, or attached thereto, or otherwise, all such non-identical copies shall be produced separately.

6. Pursuant to Federal Rule of Civil Procedure 34(b)(2)(B), if YOU object to a Request, the grounds for each objection must be stated with specificity. If an objection pertains to only a portion of a Request, a word, phrase, or clause contained within it, YOU must state the objection to that portion only and respond to the remainder of the request, using YOUR best efforts to do so. Also pursuant to Federal Rule of Civil Procedure 34(b)(2)(B), if YOU intended to produce copies of DOCUMENTS or of ESI instead of permitting inspection, YOU must so state.

7. If, in responding to this Request for Production, YOU encounter any ambiguities when construing a request or definition, the response shall set forth the matter deemed ambiguous and the construction used in responding.

8. Pursuant to Federal Rule of Civil Procedure 34(b)(2)(C), an objection must state whether any responsive materials are being withheld on the basis of that objection.

9. Whenever in this Request YOU are asked to identify or produce a DOCUMENT which is deemed by YOU to be properly withheld from production for inspection or copying:

A. If YOU are withholding the DOCUMENT under claim of privilege (including, but not limited to, the work product doctrine), please provide a log identifying each such document by specifying:

(i) The type of DOCUMENT (e.g., letter, memorandum, email, etc.) or some other means of accurately identifying it;

(ii) Its date, if any, or an estimate thereof, and so indicated as an estimate if no date appears on the DOCUMENT;

(iii) Its author(s), if any;

- (iv) Its addressee(s), if any, and, where not apparent, the relationship between its author(s) and addressee(s);
- (v) Each recipient and addresses of all PERSONS or entities to whom the DOCUMENT, thing, or copies thereof were circulated or its contents communicated, if any;
- (vi) The general subject matter of the DOCUMENT; and
- (vii) The nature of the claimed privilege so as to explain the basis asserted for withholding the DOCUMENT or thing in sufficient detail so as to enable the claim of privilege to be adjudicated, if necessary.

B. If YOU are withholding the DOCUMENT for any reason other than an objection that it is beyond the scope of discovery, identify as to each document and, in addition to the information requested in paragraph 9.A above, please state the reason for withholding the DOCUMENT. If YOU are withholding production on the basis that ESI is not reasonably accessible because of undue burden or cost, provide the information required by Discovery Guideline 10(e) under Appendix A to the Local Rules.

10. When a DOCUMENT contains both privileged and non-privileged material, the non-privileged material must be disclosed to the fullest extent possible with the purportedly privileged material redacted.

11. If a privilege is asserted with regard to part of the material contained in a DOCUMENT, the party claiming the privilege must clearly indicate the portions as to which the privilege is claimed.

12. When a DOCUMENT has been redacted or altered in any fashion, identify as to each DOCUMENT the reason for the redaction or alteration, the date of the redaction or alteration, and the PERSON performing the redaction or alteration. Any redaction must be clearly visible on the redacted DOCUMENT.

13. Any DOCUMENT or things requested that cannot be produced in full should be produced to the extent possible, specifying the reasons for the inability to produce the remainder and stating whatever information, knowledge, or belief YOU have CONCERNING the unproduced portion.

14. It is intended that these Requests will not solicit any material protected either by the attorney–client privilege or by the work product doctrine which was created by, or developed by, counsel for the responding party after the date on which this litigation was commenced. If any Request is susceptible of a construction which calls for the production of such material, that material need not be provided and no privilege log pursuant to Federal Rule of Civil Procedure 26(b)(5) or Discovery Guideline 9(a) will be required as to such material.

15. These Requests are continuing so as to require prompt supplemental responses as required under Federal Rule of Civil Procedure 26(e) up to and including the time of trial of the present dispute. If YOU come into possession, custody, or control of responsive DOCUMENTS or things after the initial production, YOU should supplement the production by promptly producing such DOCUMENTS or things.

16. If a Request is silent as to the time period for which information is sought, YOUR response should include all information known to YOU CONCERNING events that occurred, in whole or in part, at any time during the time period of July 8, 2008 to November 7, 2017.

17. To the extent any of these Requests require PLAINTIFF'S email addresses, IP addresses, or other similar identifiers to respond, PLAINTIFF will serve YOU that information separately.

18. To the extent any of these Requests involve information that is confidential, proprietary, or private information for which special protection from public disclosure and from use for any purpose other than prosecuting this litigation is warranted, a Stipulated Protective Order to address such information is currently under negotiation.

REQUESTS FOR PRODUCTION

REQUEST FOR PRODUCTION NO. 23:

Any INTERNET COMMUNICATION of WIKIMEDIA that any DEFENDANT INTERACTED WITH in connection with Upstream surveillance.

REQUEST FOR PRODUCTION NO. 24:

All DOCUMENTS CONCERNING any INTERACTION WITH the INTERNET COMMUNICATIONS of WIKIMEDIA in connection with Upstream surveillance.

Dated: November 29, 2017

/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

Exhibit 9

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

_____)	
WIKIMEDIA FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	No. 1:15-cv-00662-TSE
)	
NATIONAL SECURITY AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	
_____)	

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

~~TOP SECRET//SI//NOFORN//20320108~~

EXHIBIT B

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

**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~~

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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 disseminations 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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(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;

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(U) Section 8 - Collaboration with Foreign Governments

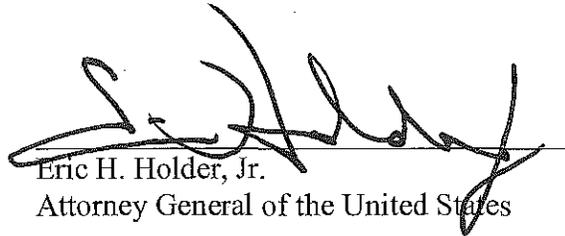
- (a) (U) Procedures for the dissemination of evaluated and minimized information. Pursuant to section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may 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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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

~~TOP SECRET//SI//NOFORN//20320108~~

Exhibit 10

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

_____)	
WIKIMEDIA FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	No. 1:15-cv-00662-TSE
)	
NATIONAL SECURITY AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	
_____)	

**OBJECTIONS OF DEFENDANTS NATIONAL SECURITY AGENCY
AND ADM. MICHAEL S. ROGERS, DIRECTOR,
TO PLAINTIFF’S THIRD SET 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 as follows to Plaintiff Wikimedia Foundation’s Third Set of Requests for Admission, dated March 17, 2018.

**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 "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.

5. 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).

6. As set forth in response to specific interrogatories below, the NSA Defendants object to Instruction No. 4 in Plaintiff's Requests for Admission to the extent that identification or description of each document or oral communication as to which privilege is claimed would itself divulge privileged information.

7. The NSA Defendants object to Plaintiff's Requests for Admission as seeking irrelevant information to the extent that they seek information not involving the NSA's Upstream Internet acquisition techniques as authorized by Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1881a. In formulating these responses, the NSA Defendants have limited the scope of their inquiry of knowledgeable persons, as well as their searches of appropriate records, to those persons and records reasonably calculated to possess information involving the NSA's Upstream Internet acquisition techniques as authorized by Section 702 of the FISA.

8. 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.

9. 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 TO PLAINTIFF’S
THIRD SET OF REQUESTS FOR ADMISSION**

REQUEST FOR ADMISSION NO. 37: Admit that, in conducting Upstream surveillance on or before June 22, 2015, the NSA screened the contents of Internet web traffic (that is, the application layer of HTTP and HTTPS communications).

OBJECTION: The NSA Defendants object to Request for Admission No. 37 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. 37 on the grounds that the term “contents of Internet web traffic” is vague and ambiguous. In responding to Request for Admission No. 37, the NSA Defendants construe “contents of Internet web traffic” to mean “the application layer of HTTP and HTTPS communications.”

The NSA Defendants further object to Request for Admission No. 37 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. 38: Admit that, in conducting Upstream surveillance as of the date of the service of this request, the NSA screens the contents of Internet web traffic (that is, the application layer of HTTP and HTTPS communications).

OBJECTION: The NSA Defendants object to Request for Admission No. 38 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. 38 on the grounds that the term “contents of Internet web traffic” is vague and ambiguous. In responding to Request for Admission No. 38, the NSA Defendants construe “contents of Internet web traffic” to mean “the application layer of HTTP and HTTPS communications.”

The NSA Defendants further object to Request for Admission No. 38 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. 39: Admit that the document attached hereto as Exhibit A, which describes the monitoring of hundreds of CIRCUITS at one international cable site, is a true and correct excerpted copy of a genuine NSA document.

OBJECTION: To the extent that Plaintiff seeks to establish the authenticity of Exhibit A as evidence of intelligence activities allegedly conducted by the NSA, Defendants object to Request for Admission No. 39 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. 40: If YOU contend, for the purpose of contesting jurisdiction in this matter, that encryption bears in any way on the interception, accessing, COPYING, filtering, REVIEWING, ingestion, or RETENTION of WIKIMEDIA'S COMMUNICATIONS in the course of Upstream surveillance, admit that YOU have the ability to decrypt, decipher, or render intelligible the contents of some HTTPS communications subject to Upstream surveillance.

OBJECTION: The NSA Defendants object to Request for Admission No. 40 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. 40 insofar as the definition of "Reviewing," by encompassing fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

The NSA Defendants further object to Request for Admission No. 40 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).

Dated: March 22, 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. HEIMAN
OLIVIA HUSSEY-SCOTT
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 11

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

_____)	
WIKIMEDIA FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	No. 1:15-cv-00662-TSE
)	
NATIONAL SECURITY AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	
_____)	

**OBJECTIONS AND RESPONSES BY DEFENDANTS NATIONAL
SECURITY AGENCY AND ADM. MICHAEL S. ROGERS,
DIRECTOR, TO PLAINTIFF’S INTERROGATORIES**

Pursuant to Rule 33 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 Interrogatories, dated November 7, 2017.

**GENERAL OBJECTIONS AND
OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS**

1. The NSA Defendants object to Plaintiff’s Interrogatories to the extent, as set forth in response to specific interrogatories below, that they seek information regarding the activities of the NSA, which is absolutely protected from disclosure by the statutory privilege under 50 U.S.C. § 3605(a).

2. The NSA Defendants object to Plaintiff’s Interrogatories to the extent, as set forth in response to specific interrogatories 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.

3. As set forth in response to each interrogatory below, the NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

4. As set forth in response to specific interrogatories 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 interrogatories 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 interrogatories below, the NSA Defendants object to the definition of the term “Review” as compound, unduly burdensome and oppressive,

and so vague and ambiguous as to render the specific interrogatories in which it is used incapable of reasoned response.

7. As set forth in response to specific interrogatories below, the NSA Defendants object to the definition of the term “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 the specific interrogatories in which it is used incapable of reasoned response.

8. As set forth in response to specific interrogatories below, the NSA Defendants object to Plaintiff’s Interrogatories 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. As set forth in response to specific interrogatories below, the NSA Defendants object to Instruction No. 3 in Plaintiff’s Interrogatories to the extent that identification or description of each document or oral communication as to which privilege is claimed would itself divulge privileged information.

10. The NSA Defendants object to Plaintiff’s Interrogatories to the extent that they seek information not involving the NSA’s Upstream Internet acquisition techniques as authorized by Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. § 1881a. In formulating these answers, the NSA Defendants have limited the scope of their inquiry of knowledgeable persons, as well as their searches of appropriate records, to those persons and records reasonably calculated to possess information involving the NSA’s Upstream Internet acquisition techniques as authorized by Section 702 of the FISA.

11. 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.

12. Nothing contained in the following objections and responses shall be construed as a waiver of any applicable objection or privilege as to any interrogatory 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 INTERROGATORIES

INTERROGATORY NO. 1: DESCRIBE YOUR understanding of the definition of the term “international Internet link” as 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)—and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 1 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants also object to Interrogatory No. 1 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 Interrogatory No. 1 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the

term ‘international Internet link’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 1 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 1 on the ground that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 2: DESCRIBE YOUR understanding of the definition of the term “circuit” as used at pages 36 to 37 of the PCLOB Report, and provide all information supporting that understanding, including but not limited to all information furnished by DEFENDANTS to the Privacy and Civil Liberties Oversight Board concerning this term.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 2 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants also object to Interrogatory No. 2 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘circuit’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

The NSA Defendants further object to this interrogatory on the ground that 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.

Finally, to the extent that Interrogatory No. 2 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 2 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding a “circuit,” within the context of Internet communications, traditionally consists of two stations, each capable of transmitting and receiving analog or digital information, and a medium of signal transmission connecting the two stations. The medium of signal transmission can be electrical wire or cable, optical fiber, electromagnetic fields (e.g., radio transmission), or light. Individual circuits may be subdivided further to create multiple “virtual circuits” through application of various technologies including but not limited to multiplexing techniques.

As of the time of this response the NSA Defendants are unaware of any information furnished by Defendants to the PCLOB regarding the meaning of the term “circuit” that would differ from the understanding set forth above.

INTERROGATORY NO. 3: DESCRIBE YOUR understanding of the definition of the term “filtering mechanism” as used at pages 10 and 47–48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 3 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 3 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘filtering mechanism’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 3 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 3 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term “filtering mechanism,” as used in the above-referenced brief when filed, meant, in unclassified terms, the devices utilized in the Upstream Internet collection process that were designed to eliminate wholly domestic Internet transactions, and transactions that did not contain at least one tasked selector, before they could

be ingested into Government databases. Today the term “filtering mechanism” would mean, in unclassified terms, the devices utilized in the Upstream Internet collection process that are designed to eliminate wholly domestic Internet transactions, and to identify for acquisition Internet transactions to or from persons targeted in accordance with the current NSA targeting procedures.

INTERROGATORY NO. 4: DESCRIBE YOUR understanding of the definition of the term “scanned” as used at page 10 of the Memorandum in Support of Defendants’ Motion to Dismiss the First Amended Complaint, *Wikimedia Foundation v. NSA*, No. 15-cv-662-TSE (D. Md. Aug. 6, 2015), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 4 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 4 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘scanned’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 4 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 4 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term “scanned,” as used in the above-referenced brief when filed, meant, in unclassified terms, the use of a screening device in the Upstream Internet collection process to acquire only Internet transactions containing at least one tasked selector. Today the term “scanned” would mean, in unclassified terms, the use of a screening device in the Upstream Internet collection process designed to identify for acquisition Internet transactions to or from persons targeted in accordance with the current NSA targeting procedures.

INTERROGATORY NO. 5: DESCRIBE YOUR understanding of the definition of the term “screen” as used at page 48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 5 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 5 on the grounds that its instruction to “provide all information supporting [their] understanding [of the definition of the term ‘screen’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 5 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 5 on the grounds that it seeks information 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

object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term “screen,” as used in the above-referenced brief when filed, meant, in unclassified terms, the use of a screening device in the Upstream Internet collection process to acquire only Internet transactions containing at least one tasked selector. Today, the term “screened” would mean, in unclassified terms, the use of a screening device in the Upstream Internet collection process designed to identify for acquisition Internet transactions to or from persons targeted in accordance with the current NSA targeting procedures.

INTERROGATORY NO. 6: DESCRIBE YOUR understanding of the definition of the term “discrete communication” as used in the 2014 NSA Minimization Procedures, and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to Interrogatory No. 6 on the grounds that 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. The NSA Defendants also object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 6 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 6 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the

term ‘discrete communication’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 6 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 6 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, in the context of the 2014 NSA Section 702 Minimization Procedures, the term “discrete communication” means a single communication.

INTERROGATORY NO. 7: DESCRIBE YOUR understanding of all features that a series of INTERNET PACKETS comprising an “Internet transaction” has in common, as the term “Internet transaction” is used in at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding. For example, the INTERNET PACKETS comprising an “Internet transaction” might share source and destination IP addresses, source and destination ports, and protocol type (albeit with the source and destination IP addresses and ports reversed for packets flowing in the opposite direction).

OBJECTION: NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 7 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 7 on the grounds that its instruction to “provide all information supporting [their] understanding [of the ‘features that a

series of Internet packets comprising an “Internet transaction” has in common’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, the NSA Defendants object to Interrogatory No. 7 on the ground that it seeks classified information about alleged NSA intelligence activities 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 8: DESCRIBE YOUR understanding of the definitions of the terms “single communication transaction” and “multi-communication transaction” as used by the government in its submission to the Foreign Intelligence Surveillance Court, filed on August 16, 2011, and provide all information supporting that understanding. *See [Redacted]*, 2011 WL 10945618, at *9 (FISC Oct. 3, 2011).

OBJECTION: The NSA Defendants object to Interrogatory No. 8 on the grounds that 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. The NSA Defendants also object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 8 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants also object to Interrogatory No. 8 as vague and ambiguous insofar as it attributes the phrase “single communication transaction” 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 *9 (FISC Oct. 3, 2011).

The NSA Defendants further object to Interrogatory No. 8 on the grounds that its instruction to “provide all information supporting [their] understanding [of the terms ‘single communication transaction’ and ‘multi-communication transaction’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 8 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 8 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding (i) the term “single communication transaction,” when used in reference to Upstream Internet collection, meant in unclassified terms an Internet transaction that contained only a single, discrete communication, and (ii) the term “multi-communication transaction” meant, in unclassified terms, an Internet transaction that contained multiple discrete communications.

INTERROGATORY NO. 9: DESCRIBE YOUR understanding of the definitions of the terms “access” and “larger body of international communications” as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 9 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 9 on the grounds that its instruction to “provide all information supporting [their] understanding [of the terms ‘access’ and ‘larger body of international communications’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 9 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 9 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding (i) the term “larger body of international communications,” as used in the above-referenced brief when filed, meant, in unclassified terms, the body of at least one-end-foreign Internet transactions transiting the Internet backbone networks of electronic communications service providers that were screened during the

Upstream Internet collection process for the purpose of identifying those containing at least one tasked selector; and (ii) the term “access,” as used in the same brief when filed, referred in unclassified terms to the means making it possible to screen this “larger body of international communications” for those that contained at least one tasked selector. As noted above in response to Interrogatory Nos. 3-5, today Internet transactions are screened during the Upstream Internet collection process to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures.

INTERROGATORY NO. 10: DESCRIBE YOUR understanding of the definition of the term “acquired” as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 10 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 10 on the grounds that its instruction to “provide all information supporting [their] understanding [of the term ‘acquired’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 10 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 10 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify

and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term “acquired,” as used in the above-referenced brief in relation to Internet transactions, meant when filed (and still means today), in unclassified terms, ingested into Government databases after the Internet transactions have passed through the filtering and scanning processes conducted during Upstream Internet collection.

INTERROGATORY NO. 11: DESCRIBE YOUR understanding of the definition of the term “collection” as used at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 11 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 11 on the grounds that its instruction to “provide all information supporting [their] understanding [of the term ‘collection’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 11 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 11 on the grounds that it seeks information 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

object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term “collection,” as used in the above-referenced brief in relation to communications, meant when filed (and still means today), in unclassified terms, ingestion into Government databases after Internet transactions have passed through the filtering and scanning processes conducted during Upstream Internet collection.

INTERROGATORY NO. 12: DESCRIBE YOUR understanding of the definition of the term “Internet ‘backbone’” as used at page 1 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 12 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 12 on the grounds that its instruction to “provide all information supporting [their] understanding [of the term ‘Internet ‘backbone’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 12 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 12 on the grounds that it seeks information 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

object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the Internet backbone is no longer well defined due to the growth of direct peering arrangements, but may be understood as the principal high-speed, ultra-high bandwidth data-transmission lines between the large, strategically interconnected computer networks and core routers that exchange Internet traffic domestically with smaller regional networks, and internationally via terrestrial or undersea circuits.

INTERROGATORY NO. 13: DESCRIBE in detail all steps taken by the NSA to PROCESS communications in the course of Upstream surveillance.

OBJECTION: The NSA Defendants object to Interrogatory No. 13 on the grounds that 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. The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 13 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

Finally, the NSA Defendants object to Interrogatory No. 13 on the ground that it seeks information about alleged NSA intelligence activities 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 object to any instruction or purported requirement, *see* Fed. R.

Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 14: DESCRIBE the entire process by which, pursuant to Upstream surveillance, the contents of INTERNET COMMUNICATIONS are INTERACTED WITH.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 14 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous. The NSA Defendants also 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 this interrogatory incapable of reasoned response.

The NSA Defendants further object to Interrogatory No. 14 to the extent grounds that 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.

Finally, the NSA Defendants object to Interrogatory No. 14 on the ground that it seeks information about alleged NSA intelligence activities 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

Dated: December 22, 2017

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
CAROLINE J. ANDERSON
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

Pursuant to 28 U.S.C. § 1746, I, Jason D. Padgett, declare under penalty of perjury that the foregoing answers to Plaintiff Wikimedia's Interrogatories are true and correct to the best of my knowledge and belief, based on my personal knowledge and information made available to me in the course of my duties and responsibilities as an Attorney in the Office of General Counsel, National Security Agency.

Executed this 22nd day of December, 2017

A handwritten signature in black ink, appearing to read 'J. Padgett', is written over a horizontal line.

Jason D. Padgett
Attorney
Office of General Counsel
National Security Agency

Exhibit 12

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

_____)	
WIKIMEDIA FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	No. 1:15-cv-00662-TSE
)	
NATIONAL SECURITY AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	
_____)	

**OBJECTIONS BY DEFENDANTS NATIONAL
SECURITY AGENCY AND ADM. MICHAEL S. ROGERS,
DIRECTOR, TO PLAINTIFF’S SECOND SET OF INTERROGATORIES**

Pursuant to Rule 33 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 as follows to Plaintiff Wikimedia Foundation’s Second Set of Interrogatories, dated March 17, 2018.

**GENERAL OBJECTIONS AND
OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS**

1. The NSA Defendants object to Plaintiff’s Interrogatories to the extent, as set forth in response to specific interrogatories below, that they seek information regarding the intelligence activities of the NSA, which is absolutely protected from disclosure by the statutory privilege under 50 U.S.C. § 3605(a).

2. The NSA Defendants object to Plaintiff’s Interrogatories to the extent, as set forth in response to specific interrogatories 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.

3. As set forth in response to each interrogatory below, the NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

4. As set forth in response to specific interrogatories 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 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 “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.

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

6. As set forth in response to specific interrogatories below, the NSA Defendants object to the definition of the term “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 the specific interrogatories in which it is used incapable of reasoned response.

7. As set forth in response to specific interrogatories below, the NSA Defendants object to Plaintiff's Interrogatories 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).

8. As set forth in response to specific interrogatories below, the NSA Defendants object to Instruction No. 3 in Plaintiff's Interrogatories to the extent that identification or description of each document or oral communication as to which privilege is claimed would itself divulge privileged information.

9. The NSA Defendants object to Plaintiff's Interrogatories as seeking irrelevant information, to the extent that they seek information not involving the NSA's Upstream Internet acquisition techniques as authorized by Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1881a. In formulating these answers, the NSA Defendants have limited the scope of their inquiry of knowledgeable persons, as well as their searches of appropriate records, to those persons and records reasonably calculated to possess information involving the NSA's Upstream Internet acquisition techniques as authorized by Section 702 of the FISA.

10. 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.

11. Nothing contained in the following objections and responses shall be construed as a waiver of any applicable objection or privilege as to any interrogatory 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 TO INTERROGATORIES

INTERROGATORY NO. 15: DESCRIBE any and all statements or facts YOU contend are inaccurate concerning Upstream surveillance in pages 7-10, 22, 32-33, 35-41 & n.157, 79, 111 n.476, 119-26, and 143-45 of the Privacy and Civil Liberties Oversight Board's Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014), based on Upstream surveillance as it was conducted on the date the report was publicly released.

OBJECTION: The NSA Defendants object to Interrogatory No. 15 on the grounds that 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. The NSA Defendants also object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 15 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 15 on the grounds that it is compound, unduly burdensome and oppressive, as it purports to require that NSA Defendants review and verify hundreds of factual assertions stated throughout more than 26 pages of a document that NSA Defendants did not author. The NSA Defendants also object to this interrogatory on the ground that the PCLOB is an independent agency within the Executive Branch, and the NSA Defendants may not have information regarding what that entity intended by statements made within its report or may not have information that allows it to verify the accuracy of certain statements. NSA Defendants reserve the right to supplement their objections as needed to address particular statements of the PCLOB 702 Report after the NSA Defendants have had an opportunity to adequately review the sections of the report identified by this interrogatory. Furthermore, to the extent that the PCLOB 702 Report contains statements that

are not factual assertions, such as statements of opinion, which can be neither accurate nor inaccurate, the NSA Defendants object to responding with respect to those statements.

Finally, to the extent that Interrogatory No. 15 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 15 on the ground that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 16: DESCRIBE the approximate percentage of CIRCUITS carrying Internet communications into or out of the United States (not CIRCUITS carrying solely telephonic or private network communications) that were monitored in the course of Upstream surveillance in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 16 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 16 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 17: DESCRIBE the approximate percentage of international submarine cables carrying Internet communications into or out of the United States (not international submarine cables carrying solely telephonic or private network communications) that were monitored in the course of Upstream surveillance in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 17 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 17 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 18: DESCRIBE, by any metric commonly used in the telecommunications industry, such as bytes or packets, the approximate amount of Internet traffic that was subject to filtering in the course of Upstream surveillance, prior to retaining Internet communications that contain a selector, in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 18 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 18 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 19: DESCRIBE, by any metric commonly used in the telecommunications industry, such as bytes or packets, the approximate amount of Internet traffic that was screened in the course of Upstream surveillance, prior to retaining Internet communications that contain a selector, in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 19 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 19 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 20: If YOU contend, for the purpose of contesting jurisdiction in this matter, that encryption bears in any way on the interception, accessing, COPYING, filtering, REVIEWING, ingestion, or RETENTION of WIKIMEDIA’S COMMUNICATIONS in the course of Upstream surveillance, DESCRIBE the protocols used to encrypt INTERNET COMMUNICATIONS or INTERNET TRANSACTIONS subject to

Upstream surveillance for which the NSA has the ability to decrypt, decipher, or render intelligible the contents of those COMMUNICATIONS.

OBJECTION: The NSA Defendants object to the definition of the term “Review” as compound, unduly burdensome and oppressive, and so vague and ambiguous as to render the specific interrogatories in which it is used incapable of reasoned response. The NSA Defendants also object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 20 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 20 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

Dated: March 22, 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. HEIMAN
OLIVIA HUSSEY-SCOTT
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 13

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.

3. 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.

4. 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.

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

6. As set forth in response to specific requests below, the NSA Defendants object to the definition of the term “Interacted With” as compound, and, insofar as it incorporates the

definition of the term “Review,” also as unduly burdensome and oppressive, and so vague and ambiguous as to render the 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 Plaintiff’s Requests for Production of Documents 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).

8. As set forth in response to specific requests below, the NSA Defendants object to Instruction No. 9 in Plaintiff’s Requests for Production of Documents, regarding the preparation of a privilege log, to the extent that providing the requested information as to each document for which privilege is claimed would itself divulge privileged information.

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. The NSA Defendants object to Plaintiffs’ Requests for Production of Documents to the extent that any of them seek the production of any documents or information not specifically involving the acquisition of Internet transactions through the use of NSA’s Upstream Internet acquisition techniques pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. § 1881a. In formulating these responses to Plaintiff’s Requests for Production of Documents, the NSA Defendants have limited the scope of their inquiry of knowledgeable persons, as well as their searches of appropriate records, to those persons and records reasonably calculated to possess information and documents involving the NSA’s Upstream Internet acquisition techniques pursuant to Section 702 of FISA.

11. 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 PLAINTIFF'S FIRST SET OF REQUESTS FOR PRODUCTION OF DOCUMENTS

REQUEST FOR PRODUCTION NO. 1: All DOCUMENTS referenced, paraphrased, or summarized in YOUR answers to Interrogatories.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that they do not reference, paraphrase, or summarize any documents in their answers to Plaintiff's interrogatories. Accordingly, there are no documents in the NSA Defendants' possession, custody, or control that are responsive to this request.

REQUEST FOR PRODUCTION NO. 2: DOCUMENTS sufficient to show or estimate the average number of optical fibers within the international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Production No. 2 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. The NSA Defendants also object to Request for Production No. 2 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The NSA Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that unclassified documents responsive to this request in their possession, custody, or control are produced at production numbers NSA-WIKI 00001–00134. (The NSA Defendants have not independently verified the accuracy of the documents being produced.)

REQUEST FOR PRODUCTION NO. 3: All DOCUMENTS listing, depicting, tallying, or describing the international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Production No. 3 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. The NSA Defendants also object to Request for Production No. 3 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The NSA Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that unclassified documents responsive to this request in their possession, custody, or control are produced at production numbers NSA-WIKI 00001–00148. (The NSA Defendants have not independently verified the accuracy of the documents being produced.)

The NSA Defendants further object to this Request insofar as it purports to require them to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and to describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

The NSA Defendants note further that the Federal Communications Commission, which issues licenses to own and operate submarine cables and associated cable landing stations located in the United States, recently issued a report enumerating the privately owned trans-ocean fiber

optic cables (also referred to in the report as cable systems) landing in the United States or its territories that were in service as of December 31, 2015. The report, Federal Communications Commission, International Bureau Report, 2015 International Circuit Capacity Data (August 2017), is available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-346376A2.pdf. A map purporting to depict the international submarine cables connecting the United States with other nations as of December 11, 2017, prepared by the telecommunications market research and consulting firm Telegeography, is available at <https://www.submarinecablemap.com>. Telegeography also publishes an online Submarine Cable Landing Directory, <https://www.telegeography.com/telecom-resources/submarine-cable-landing-directory>, which purports to identify the privately owned international undersea cable systems landing in the United States or its territories. These documents are just as accessible to Plaintiff as they are to the NSA Defendants. The NSA Defendants have not independently verified the accuracy of these documents.

REQUEST FOR PRODUCTION NO. 4: All DOCUMENTS listing, depicting, tallying, or describing the points at which international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES arrive at or depart from the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Production No. 4 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. The NSA Defendants also object to Request for Production No. 4 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The NSA Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that unclassified documents responsive to this request in their possession, custody, or control are produced at production numbers NSA-WIKI 00001–00148. (The NSA Defendants have not independently verified the accuracy of the documents being produced.)

The NSA Defendants further object to this Request insofar as it purports to require them to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and to describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

The NSA Defendants note further that the Federal Communications Commission, which issues licenses to own and operate submarine cables and associated cable landing stations located in the United States, recently issued a report enumerating the privately owned trans-ocean fiber optic cables (also referred to in the report as cable systems) landing in the United States or its territories that were in service as of December 31, 2015. The report, Federal Communications Commission, International Bureau Report, 2015 International Circuit Capacity Data (August 2017), is available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-346376A2.pdf. A map purporting to depict the international submarine cables connecting the United States with other nations as of December 11, 2017, prepared by the telecommunications market research and consulting firm Telegeography, is available at <https://www.submarinecablemap.com>. Telegeography also publishes an online Submarine Cable Landing Directory, <https://www.telegeography.com/telecom-resources/submarine-cable-landing-directory>, which purports to identify the privately owned international undersea cable systems landing in the United

States or its territories. These documents are just as accessible to Plaintiff as they are to the NSA Defendants. The NSA Defendants have not independently verified the accuracy of these documents.

REQUEST FOR PRODUCTION NO. 5: All DOCUMENTS listing, depicting, tallying, or describing the terrestrial cables that are part of the INTERNET BACKBONE within the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Production No. 5 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. The NSA Defendants also object to Request for Production No. 5 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The NSA Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that they have been unable to locate unclassified documents responsive to this request within their possession, custody, or control.

The NSA Defendants further object to this Request insofar as it purports to require them to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and to describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 6: DOCUMENTS sufficient to show or estimate the number of persons TARGETED for Upstream surveillance pursuant to 50 U.S.C. § 1881a in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The NSA Defendants object to Request for Production No. 6 on the grounds that 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, and which do not include Plaintiff's "dragnet" theory of standing rejected by the Fourth Circuit, *see Wikimedia Found. v. NSA*, 857 F.3d 193, 213-16 (4th Cir. 2017). The NSA Defendants also object to Request for Production No. 6 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The NSA Defendants further object to Request for Production 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the Office of the Director of National Intelligence (ODNI) has published Statistical Transparency Reports Regarding Use of National Security Authorities for calendar years 2013, 2014, 2015, and 2016, which include estimates of the numbers of targets of the U.S. Government's surveillance authority, including but not limited to Section 702 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a. These reports are available, and are equally accessible to Plaintiff as they are to the NSA Defendants, at the following Internet addresses:

- https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY_2013.pdf
- <https://www.dni.gov/files/icotr/CY%20Statistical%20Transparency%20Report.pdf>
- https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015

- https://www.dni.gov/files/icotr/ic_transparency_report_cy2016_5_2_17.pdf

The NSA Defendants further respond that documents responsive to this request are being withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege. The NSA Defendants further object to this request to the extent it purports to require them to describe the nature of the documents withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 7: DOCUMENTS sufficient to show or estimate the number of SELECTORS used in conducting Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The NSA Defendants object to Request for Production No. 7 on the grounds that 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, and which do not include Plaintiff's "dragnet" theory of standing rejected by the Fourth Circuit, *see Wikimedia Found. v. NSA*, 857 F.3d 193, 213-16 (4th Cir. 2017). The NSA Defendants also object to Request for Production No. 7 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The NSA Defendants further object to Request for Production No. 7 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that documents responsive to this request are being withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege. The NSA Defendants further object to this request to the extent it purports to require them to describe the nature of the documents withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 8: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS COPIED using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The NSA Defendants object to Request for Production No. 8 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The NSA Defendants also object to the definition of the term "Internet Transaction" as vague and ambiguous insofar as it is meant, by its reference to 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.

The NSA Defendants further object to Request for Production No. 8 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).

The NSA Defendants further object to Request for Production No. 8 insofar as it purports to require them to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and to describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 9: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS REVIEWED for SELECTORS using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The NSA Defendants object to Request for Production No. 9 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The NSA Defendants also object to Request for Production No. 9 on the grounds that the definition of the term "Internet Transaction" is vague and ambiguous insofar as it is meant, by its reference to 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.

Furthermore, the NSA Defendants object to Request for Production No. 9 on the grounds that the term "Review," as defined by Plaintiff, encompasses so many fundamentally different actions that as used herein it renders this request compound, unduly burdensome and

oppressive, vague and ambiguous, and particularly when viewed in the context of the phrase, “reviewed for selectors,” incapable of reasoned response.

Finally, the NSA Defendants object to Request for Production No. 9 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants state that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 10: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS RETAINED using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The NSA Defendants object to Request for Production No. 10 on the grounds that 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. The NSA Defendants also object to Request for Production No. 10 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to 2010.

The NSA Defendants further object to Request for Production No. 10 on the grounds that the definition of the term “Internet Transaction” is vague and ambiguous insofar as it is meant, by its reference to 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.

Finally, the NSA Defendants object to Request for Production 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). In particular, the NSA Defendants object to this request to the extent it means to call for the production of repositories in which communications collected during Upstream surveillance are stored, as unduly burdensome and oppressive and calling for information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, unclassified documents arguably responsive to this request for the year 2011 are produced at production numbers NSA-WIKI 00149–00297. Repositories of communications collected during Upstream surveillance are being withheld for the reasons stated in the objections, above. Other responsive documents and information are being withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege. The NSA Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 11: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS RETAINED using Upstream surveillance that are to, from, or about “U.S. persons,” in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The NSA Defendants object to Request for Production No. 11 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to 2010.

The NSA Defendants also object to Request for Production No. 11 on the grounds that the definition of the term “Internet Transaction” is vague and ambiguous insofar as it is meant, by its reference to 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.

Furthermore, the NSA Defendants object to Request for Production No. 11 on the grounds that 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.

Finally, the NSA Defendants object to Request for Production No. 11 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). In particular, the NSA Defendants object to this request to the extent it means to call for the production of repositories in which communications collected during Upstream surveillance are stored, as

unduly burdensome and oppressive and calling for information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants state that apart from the arguably responsive repositories of communications withheld for the reasons stated above, they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 12: DOCUMENTS sufficient to show or estimate the average number of discrete INTERNET COMMUNICATIONS contained in a multi-communication transaction.

OBJECTION: The NSA Defendants object to Request for Production No. 12 on the grounds that 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. The NSA Defendants object to Request for Production No. 12 as vague and ambiguous insofar as it fails to specify the universe of communications for which the “average number” in a multi-communication transaction is requested. The NSA Defendants also object to Request for Production No. 12 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The NSA Defendants further object to this request to the extent it means to call for the production of repositories in which communications collected during Upstream surveillance are stored, as unduly burdensome and oppressive and calling for information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants state that apart from the arguably responsive repositories of communications

withheld for the reasons stated above, they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 13: DOCUMENTS sufficient to show or estimate the number of CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The NSA Defendants object to Request for Production No. 13 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The NSA Defendants also object to Request for Production No. 13 on the grounds that the definition of the term "Circuit" is 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 "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 it is understood by the NSA Defendants.

Finally, the NSA Defendants object to Request for Production No. 13 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).

RESPONSE: Documents and information responsive to this request are being withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege. The NSA Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. Civ. P. 26(b)(5)(A), as unduly

burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 14: DOCUMENTS sufficient to show or estimate the combined bandwidth of the CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The NSA Defendants object to Request for Production No. 14 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The NSA Defendants also object to Request for Production No. 14 on the grounds that 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 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 it is understood by the NSA Defendants.

Finally, the NSA Defendants object to Request for Production No. 14 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).

RESPONSE: Documents and information responsive to this request are being withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege. The NSA Defendants object to this request to the extent it purports to require them to describe

the nature of the materials withheld on these grounds, *see* Fed. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 15: DOCUMENTS sufficient to show or estimate the number of “international Internet link[s]”—as that term was 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 (F.I.S.C. Oct. 3, 2011)—monitored using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The NSA Defendants object to Request for Production No. 15 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to 2010.

The NSA Defendants also object to Request for Production No. 15 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 (“FISC”) 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).

Finally, the NSA Defendants object to Request for Production 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).

RESPONSE: In light of the objection stated above regarding the phrase “international Internet link,” for purposes of responding to this request the NSA Defendants construe that phrase to mean “location.” So construing the request, the NSA Defendants respond that documents and information responsive to this request are being withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege. The NSA Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 16: DOCUMENTS sufficient to show the number of Internet “chokepoints” or “choke points” (as that term is used by YOU) inside the UNITED STATES through which INTERNATIONAL COMMUNICATIONS enter and leave the UNITED STATES and where the NSA has established Upstream surveillance collection or PROCESSING capabilities.

OBJECTION: The NSA Defendants object to Request for Production No. 16 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The NSA Defendants also object to Request for Production No. 16 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).

Finally, the NSA Defendants object to Request for Production No. 16 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).

RESPONSE: In light of the objection stated above regarding the terms “chokepoints” and “choke points,” for purposes of responding to this request the NSA Defendants construe those terms to mean “location.” So construing the request, the NSA Defendants respond that documents and information responsive to this request are being withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege. The NSA Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 17: All DOCUMENTS defining or describing the meaning of the term “Internet transaction.”

OBJECTION: The NSA Defendants object to Request for Production No. 17 on the grounds that 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. The NSA Defendants also object to Request for Production No. 17 as unduly

burdensome and oppressive insofar as it seeks “all documents” defining or describing the meaning of the term “Internet transaction,” rather than documents sufficient to define that term.

Finally, the NSA Defendants object to Request for Production No. 17 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the term “Internet transaction” is defined in the NSA’s 2011, 2014, 2015, and 2016 Section 702 Minimization Procedures, and in [*Caption Redacted*], Government’s Response to the Court’s Order of May 9, 2011 (F.I.S.C. June 1, 2011), all of which are respectively available (in redacted form) and equally accessible to Plaintiff as they are to the NSA Defendants, at the following Internet addresses:

- <https://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf>
- [https://www.dni.gov/files/documents/icotr/ NYT/ Government's%20Amendment%20to%20Section%20702%20Certification%20and%20Amended%20Minimization%20Procedures%20Q\(October%2031,%202011\).pdf](https://www.dni.gov/files/documents/icotr/ NYT/ Government's%20Amendment%20to%20Section%20702%20Certification%20and%20Amended%20Minimization%20Procedures%20Q(October%2031,%202011).pdf)
- <https://www.dni.gov/files/documents/092812014%20NSA%20702%20Minimization%20Procedures.pdf>
- https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf
- https://www.dni.gov/files/documents/icotr/51117/2016_NSA_Section_702_Minimization_Procedures_Sep_26_2016.pdf
- https://www.dni.gov/files/documents/icotr/51117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf
- [https://www.dni.gov/files/documents/icotr/ NYT/ Government's%20Response%20to%20May%209,%202011%20Briefing%20Order%20\(June%201,%202011\).pdf](https://www.dni.gov/files/documents/icotr/ NYT/ Government's%20Response%20to%20May%209,%202011%20Briefing%20Order%20(June%201,%202011).pdf)

The NSA Defendants further respond that documents responsive to this request are being withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege. The NSA Defendants further object to this request to the extent it purports to require them to describe the nature of the documents withheld or the information redacted from the documents referenced above on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 18: All Foreign Intelligence Surveillance Court-approved targeting procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance.

OBJECTION: The NSA Defendants object to Request for Production No. 18 on the grounds that 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. The NSA Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The NSA Defendants further object to Request for Production No. 18 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants state that the NSA's 2014 and 2016 Section 702 Targeting Procedures are

available (in redacted form) and equally accessible to Plaintiff as they are to the NSA

Defendants, at the following Internet addresses:

- http://www.dni.gov/files/documents/icotr/51117/2016_NSA_702_Targeting_Procedures_Mar30_17.pdf;
- <http://www.dni.gov/files/documents/icotr/702/Bates%20365-373.pdf>.

The NSA's Section 702 Targeting Procedures for the years 2009, 2010, 2011, 2012, 2013 and 2015 are being withheld in full.

The NSA Defendants further object to this request, insofar as it purports to require them to describe the nature of the information redacted from these documents, and the nature of the classified information contained in the NSA's Section 702 Targeting Procedures for the years 2009, 2010, 2011, 2012, 2013 and 2015, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 19: All Foreign Intelligence Surveillance Court-approved minimization procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance.

OBJECTION: The NSA Defendants object to Request for Production No. 19 on the grounds that 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. The NSA Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The NSA Defendants further object to Request for Production No. 19 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants state that the NSA's 2011, 2014, 2015, and 2016 Section 702 Minimization Procedures, are respectively available (in redacted form) and equally accessible to Plaintiff as they are to the NSA Defendants, at the Internet addresses given above in response to Request for Production No. 17; the NSA's Section 702 Minimization Procedures for the years 2009, 2010, 2012 and 2013 are being withheld in full. The NSA Defendants further object to this request, insofar as it purports to require them to describe the nature of the information redacted from these documents, and the nature of the classified information contained in the NSA's Section 702 Minimization Procedures for the years 2009, 2010, 2012, and 2013, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 20: Any supplemental procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance.

OBJECTION: The NSA Defendants object to Request for Production No. 20 on the grounds that 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. The NSA Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The NSA Defendants further object to Request for Production No. 20 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).

RESPONSE: On the basis of the foregoing objections, documents responsive to this request will not be produced. The NSA Defendants further object to this request insofar as it purports to require them to describe the nature of the materials withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking information protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 21: All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court orders and opinions CONCERNING Upstream surveillance.

OBJECTION: The NSA Defendants object to Request for Production No. 21 on the grounds that 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. The NSA Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The NSA Defendants further object to Request for Production No. 21 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants state that neither the Foreign Intelligence Surveillance Court of Review nor the

Supreme Court has issued any orders or opinions concerning NSA's Upstream Internet surveillance. With regard to FISC orders or opinions concerning Upstream surveillance, many of those orders and opinions are already publicly available in redacted form as a result of declassification pursuant to the USA FREEDOM Act, disclosures in response to Freedom of Information Act ("FOIA") requests, and disclosures pursuant to the Transparency Initiative.

First, in accordance with section 402 of the USA-FREEDOM Act, Pub. L. 114-23, 129 Stat. 268, 281-82, codified at 50 U.S.C. § 1872, all FISC opinions and orders issued on or after June 2, 2015, that include a significant construction or interpretation of any provision of law, including FISA Section 702, 50 U.S.C. § 1881a, are now publicly available (in redacted form as appropriate) and equally accessible to Plaintiff as they are to the NSA Defendants, at various locations on the ODNI public website.

Second, the Government has disclosed in redacted form (as appropriate) to the Electronic Frontier Foundation in response to a FOIA request "all decisions, orders, or opinions of the FISC or the FISC-R submitted to Congress by the Attorney General pursuant to section 6002 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. section 1871(a)(5)); 50 U.S.C. sections 1871(c)(1) & (2); and 50 U.S.C. section 1881f(b)(1)(D) between July 1, 2003 and June 1, 2015, which have not been previously declassified and made public (to include those decisions, orders, or opinions previously identified by [DOJ] to the Brennan Center, https://www.brennancenter.org/sites/default/files/publications/The_New_Era_of_Secret_Law.pdf), that remain classified." Those documents are now publicly available (in redacted form) and equally accessible to Plaintiff as they are to the NSA Defendants, at various locations on the ODNI public website.

Third, the Government has also disclosed (in redacted form as appropriate) other FISC opinions and orders concerning Upstream surveillance pursuant to other FOIA requests and those opinions and orders can also be found at various locations on the ODNI public website.

Finally, the Government has also disclosed (in redacted form as appropriate) other FISC opinions and orders concerning Upstream surveillance pursuant to the Transparency Initiative. Those FISC opinions and orders can also be found at various locations on the ODNI public website.

Unredacted versions of the above-referenced documents, and other FISC orders and opinions concerning Upstream surveillance not referenced above, if any, are in the custody or control of the NSA Defendants, are being withheld on the basis of the objections stated above. The NSA Defendants further object to this request insofar as it purports to require them to describe the nature of the materials withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 22: All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court submissions CONCERNING Upstream surveillance.

OBJECTION: The NSA Defendants object to Request for Production No. 22 on the grounds that 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. The NSA Defendants also object to this request as unduly burdensome and

oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The NSA Defendants further object to Request for Production No. 22 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).

RESPONSE: To the extent not produced in response to Plaintiff's other Requests for Production herein, any responsive documents the NSA Defendants may have would be a subset of those in the possession, custody, and control of the DOJ Defendants, and are being withheld on the basis of the objections stated above. The NSA Defendants further object to this request insofar as it purports to require them to describe the nature of the documents and information withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

**OBJECTIONS AND RESPONSES TO PLAINTIFF'S SECOND
SET OF REQUESTS FOR PRODUCTION OF DOCUMENTS**

REQUEST FOR PRODUCTION NO. 23: Any INTERNET COMMUNICATION of WIKIMEDIA that any DEFENDANT INTERACTED WITH in connection Upstream surveillance.

OBJECTION: The NSA Defendants object to Request for Production No. 23 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The NSA Defendants also object to Request for Production No. 23 to the extent 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).

The NSA Defendants further object to Request for Production No. 23 insofar as it purports to require them (i) to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and (ii) to describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 24: Any DOCUMENTS CONCERNING any INTERACTION WITH the INTERNET COMMUNICATIONS of WIKIMEDIA in connection with Upstream surveillance.

OBJECTION: The NSA Defendants object to Request for Production No. 24 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The NSA Defendants also object to Request for Production No. 24 to the extent 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).

The NSA Defendants further object to Request for Production No. 24 insofar as it purports to require them (i) to state whether there exist responsive materials that they are

withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and (ii) to describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

Date: January 8, 2018

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Director

/s/ James J. Gilligan

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
Trial Attorneys

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

Counsel for the NSA Defendants

Exhibit 14

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

_____)	
WIKIMEDIA FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	No. 1:15-cv-00662-TSE
)	
NATIONAL SECURITY AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	
_____)	

**OBJECTIONS AND RESPONSES BY DEFENDANTS
DEPARTMENT OF JUSTICE AND ATTORNEY GENERAL JEFFERSON B.
SESSIONS, III, 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 Department of Justice (“DOJ”) and Jefferson B. Sessions, III, in his official capacity as Attorney General (together, the “DOJ 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 DOJ 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 DOJ 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 National Security Agency (“NSA”), which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

3. The DOJ 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 DOJ 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 DOJ 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 DOJ Defendants.

5. As set forth in response to specific requests below, the DOJ 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 DOJ Defendants. The PCLOB is an independent agency within the Executive Branch, and the DOJ 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 DOJ Defendants.

6. As set forth in response to specific requests below, the DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ Defendants further object to Request for Admission No. 1 as unduly burdensome insofar as it requests that the DOJ Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the DOJ Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA and Adm. Michael S. Rogers, in his official capacity as Director of the NSA (together, the “NSA Defendants”), and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 DOJ 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 DOJ Defendants further object to Request for Admission No. 2 as unduly burdensome and oppressive insofar as it requests that DOJ Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the DOJ Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 DOJ 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 DOJ Defendants further object to Request for Admission No. 3 as unduly burdensome and oppressive insofar as it requests that DOJ Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the DOJ Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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

OBJECTION: The DOJ 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 DOJ Defendants further object to Request for Admission No. 4 as unduly burdensome and oppressive insofar as it requests that DOJ Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the DOJ Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 DOJ 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 DOJ 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 DOJ 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 DOJ Defendants further object to Request for Admission No. 6 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).

The DOJ 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 DOJ Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the

knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 DOJ 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 DOJ 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 DOJ 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 DOJ Defendants further object to Request for Admission No. 8 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).

The DOJ 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 DOJ Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 DOJ 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 DOJ 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 DOJ 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 DOJ Defendants further object to Request for Admission No. 10 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).

The DOJ 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 DOJ Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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

OBJECTION: The DOJ 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 DOJ 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 DOJ Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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

OBJECTION: The DOJ 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 DOJ 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 DOJ 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 DOJ 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 (“FISC”) 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 DOJ 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 DOJ 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 DOJ 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 DOJ Defendants allegedly used 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 DOJ Defendants object to this Request for Admission as implicitly seeking information (which can be neither confirmed nor denied) regarding the authenticity of the purported slide, and which is also absolutely protected from disclosure by 50 U.S.C. § 3605(a), the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ Defendants admit that Exhibit 1 to the NSA Defendants’ responses to these requests 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 DOJ 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: Subject to the objection stated above, and without waiving it, the DOJ Defendants admit that the 2014 NSA Section 702 Minimization Procedures, Exhibit 1 to the NSA Defendants' responses to these requests, 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 DOJ 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: Subject to the objection stated above, and without waiving it, the DOJ Defendants admit that the 2014 NSA Section 702 Minimization Procedures, Exhibit 1 to the NSA Defendants' responses to these requests, 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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 DOJ 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

JAMES J. GILLIGAN
Special Litigation Counsel

/s/ Rodney Patton
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) 305-7919
Fax: (202) 616-8470
Email: rodney.patton@usdoj.gov

*Counsel for Defendants Department of Justice
and Attorney General Jefferson B. Sessions, III,
in His Official Capacity*

Exhibit 15

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

_____)	
WIKIMEDIA FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	No. 1:15-cv-00662-TSE
)	
NATIONAL SECURITY AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	
_____)	

**OBJECTIONS AND RESPONSES BY DEFENDANTS
DEPARTMENT OF JUSTICE AND ATTORNEY GENERAL JEFFERSON B.
SESSIONS, III,
TO PLAINTIFF’S INTERROGATORIES**

Pursuant to Rule 33 of the Federal Rules of Civil Procedure and District of Maryland Local Rule 104, Defendants Department of Justice (“DOJ”) and Jefferson B. Sessions, III, in his official capacity as Attorney General (together, the “DOJ Defendants”), by their undersigned attorneys, object and respond as follows to Plaintiff Wikimedia Foundation’s Interrogatories, dated November 7, 2017.

**GENERAL OBJECTIONS AND
OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS**

1. The DOJ Defendants object to Plaintiff’s Interrogatories to the extent, as set forth in response to specific interrogatories below, that they seek information regarding the activities of the National Security Agency (“NSA”), which is absolutely protected from disclosure by the statutory privilege under 50 U.S.C. § 3605(a).

2. The DOJ Defendants object to Plaintiff’s Interrogatories to the extent, as set forth in response to specific interrogatories 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.

3. As set forth in response to each interrogatory below, the DOJ Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants’ narrative statement]” on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

4. As set forth in response to specific interrogatories below, the DOJ 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 DOJ 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 DOJ Defendants.

5. As set forth in response to specific interrogatories below, the DOJ 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 DOJ Defendants. The PCLOB is an independent agency within the Executive Branch, and the DOJ 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 DOJ Defendants.

6. As set forth in response to specific interrogatories below, the DOJ Defendants object to the definition of the term “Review” as compound, unduly burdensome and oppressive,

and so vague and ambiguous as to render the specific requests in which it is used incapable of reasoned response.

7. As set forth in response to specific interrogatories below, the DOJ Defendants object to the definition of the term “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 the specific interrogatories in which it is used incapable of reasoned response.

8. As set forth in response to specific interrogatories below, the DOJ Defendants object to Plaintiff’s Interrogatories 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. As set forth in response to specific interrogatories below, the DOJ Defendants object to Instruction No. 3 in Plaintiff’s Interrogatories to the extent that identification or description of each document or oral communication as to which privilege is claimed would itself divulge privileged information.

10. The DOJ Defendants object to Plaintiff’s Interrogatories to the extent that they seek information not involving the NSA’s Upstream Internet acquisition techniques as authorized by Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. § 1881a. In formulating these answers, the DOJ Defendants have limited the scope of their inquiry of knowledgeable persons, as well as their searches of appropriate records, to those persons and records reasonably calculated to possess information involving the NSA’s Upstream Internet acquisition techniques as authorized by Section 702 of the FISA.

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

12. Nothing contained in the following objections and responses shall be construed as a waiver of any applicable objection or privilege as to any interrogatory 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 INTERROGATORIES

INTERROGATORY NO. 1: DESCRIBE YOUR understanding of the definition of the term “international Internet link” as 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)—and provide all information supporting that understanding.

OBJECTION: The DOJ Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 1 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants also object to Interrogatory No. 1 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 DOJ Defendants further object to Interrogatory No. 1 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the

term ‘international Internet link’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 1 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 1 on the ground that it seeks information 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 2: DESCRIBE YOUR understanding of the definition of the term “circuit” as used at pages 36 to 37 of the PCLOB Report, and provide all information supporting that understanding, including but not limited to all information furnished by DEFENDANTS to the Privacy and Civil Liberties Oversight Board concerning this term.

OBJECTION: The DOJ Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants’ narrative statement]” in response to Interrogatory No. 2 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants also object to Interrogatory No. 2 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘circuit’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

The DOJ Defendants further object to this interrogatory on the ground that the PCLOB is an independent agency within the Executive Branch, and the DOJ 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 DOJ Defendants.

Finally, to the extent that Interrogatory No. 2 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 2 on the grounds that it seeks information 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that set forth in the NSA Defendants' answer to this interrogatory or the PCLOB's Section 702 Report itself. Thus, the DOJ Defendants refer Plaintiff to the PCLOB's Section 702 Report and to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 3: DESCRIBE YOUR understanding of the definition of the term "filtering mechanism" as used at pages 10 and 47–48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The DOJ Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants' narrative statement]" in response to Interrogatory No. 3 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants further object to Interrogatory No. 3 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘filtering mechanism’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 3 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 3 on the grounds that it seeks information 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified terms, can state no more than is set forth in the NSA Defendants’ answer to this interrogatory. Thus, the DOJ Defendants refer Plaintiff to the NSA Defendants’ response to this interrogatory.

INTERROGATORY NO. 4: DESCRIBE YOUR understanding of the definition of the term “scanned” as used at page 10 of the Memorandum in Support of Defendants’ Motion to Dismiss the First Amended Complaint, *Wikimedia Foundation v. NSA*, No. 15-cv-662-TSE (D. Md. Aug. 6, 2015), and provide all information supporting that understanding.

OBJECTION: The DOJ Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants’ narrative statement]” in response to Interrogatory No. 4 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants further object to Interrogatory No. 4 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘scanned’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 4 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 4 on the grounds that it seeks information 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified terms, can state no more than is set forth in the NSA Defendants’ answer to this interrogatory. Thus, the DOJ Defendants refer Plaintiff to the NSA Defendants’ response to this interrogatory.

INTERROGATORY NO. 5: DESCRIBE YOUR understanding of the definition of the term “screen” as used at page 48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The DOJ Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants’ narrative statement]” in response to Interrogatory No. 5 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants further object to Interrogatory No. 5 on the grounds that its instruction to “provide all information supporting [their] understanding [of the definition of the term ‘screen’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 5 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 5 on the grounds that it seeks information 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified terms, can state no more than is set forth in the NSA Defendants’ answer to this interrogatory. Thus, the DOJ Defendants refer Plaintiff to the NSA Defendants’ response to this interrogatory.

INTERROGATORY NO. 6: DESCRIBE YOUR understanding of the definition of the term “discrete communication” as used in the 2014 NSA Minimization Procedures, and provide all information supporting that understanding.

OBJECTION: The DOJ Defendants object to Interrogatory No. 6 on the grounds that 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. The DOJ Defendants also object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants’

narrative statement]” in response to Interrogatory No. 6 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants further object to Interrogatory No. 6 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘discrete communication’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 6 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 6 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). The DOJ Defendants also object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that set forth in the NSA Defendants’ answer to this interrogatory. Thus, the DOJ Defendants refer Plaintiff to the NSA Defendants’ response to this interrogatory.

INTERROGATORY NO. 7: DESCRIBE YOUR understanding of all features that a series of INTERNET PACKETS comprising an “Internet transaction” has in common, as the term “Internet transaction” is used in at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding. For example, the INTERNET PACKETS comprising an “Internet transaction” might share source and destination IP addresses, source and destination ports, and protocol type (albeit with the source and destination IP addresses and ports reversed for packets flowing in the opposite direction).

OBJECTION: DOJ Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants’ narrative statement]” in response to Interrogatory No. 7 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants further object to Interrogatory No. 7 on the grounds that its instruction to “provide all information supporting [their] understanding [of the ‘features that a series of Internet packets comprising an “Internet transaction” has in common’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, the DOJ Defendants object to Interrogatory No. 7 on the ground that it seeks classified information about alleged NSA intelligence activities 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 8: DESCRIBE YOUR understanding of the definitions of the terms “single communication transaction” and “multi-communication transaction” as used by the government in its submission to the Foreign Intelligence Surveillance Court, filed on August 16, 2011, and provide all information supporting that understanding. *See* [Redacted], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011).

OBJECTION: The DOJ Defendants object to Interrogatory No. 8 on the grounds that 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. The DOJ Defendants also object to the definition of the term “Describe” to the extent it calls for

“identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants’ narrative statement]” in response to Interrogatory No. 8 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants also object to Interrogatory No. 8 as vague and ambiguous insofar as it attributes the phrase “single communication transaction” 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 *9 (FISC Oct. 3, 2011).

The DOJ Defendants further object to Interrogatory No. 8 on the grounds that its instruction to “provide all information supporting [their] understanding [of the terms ‘single communication transaction’ and ‘multi-communication transaction’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 8 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 8 on the grounds that it seeks information 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 DOJ Defendants also object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that set forth in the NSA Defendants’ answer to

this interrogatory. Thus, the DOJ Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 9: DESCRIBE YOUR understanding of the definitions of the terms “access” and “larger body of international communications” as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The DOJ Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants' narrative statement]” in response to Interrogatory No. 9 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants further object to Interrogatory No. 9 on the grounds that its instruction to “provide all information supporting [their] understanding [of the terms ‘access’ and ‘larger body of international communications’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 9 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 9 on the grounds that it seeks information 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified

terms, can state no more than is set forth in the NSA Defendants' answer to this interrogatory.

Thus, the DOJ Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 10: DESCRIBE YOUR understanding of the definition of the term “acquired” as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The DOJ Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants' narrative statement]” in response to Interrogatory No. 10 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants further object to Interrogatory No. 10 on the grounds that its instruction to “provide all information supporting [their] understanding [of the term ‘acquired’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 10 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 10 on the grounds that it seeks information 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome or oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified

terms, can state no more than is set forth in the NSA Defendants' answer to this interrogatory.

Thus, the DOJ Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 11: DESCRIBE YOUR understanding of the definition of the term "collection" as used at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The DOJ Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants' narrative statement]" in response to Interrogatory No. 11 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants further object to Interrogatory No. 11 on the grounds that its instruction to "provide all information supporting [their] understanding [of the term 'collection']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 11 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 11 on the grounds that it seeks information 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified

terms, can state no more than is set forth in the NSA Defendants' answer to this interrogatory.

Thus, the DOJ Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 12: DESCRIBE YOUR understanding of the definition of the term "Internet "backbone"" as used at page 1 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The DOJ Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants' narrative statement]" in response to Interrogatory No. 12 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The DOJ Defendants further object to Interrogatory No. 12 on the grounds that its instruction to "provide all information supporting [their] understanding [of the term 'Internet 'backbone']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 12 seeks classified information about alleged NSA intelligence activities, the DOJ Defendants object to Interrogatory No. 12 on the grounds that it seeks information 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 DOJ Defendants also object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that set forth in the NSA Defendants' answer to

this interrogatory. Thus, the DOJ Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 13: DESCRIBE in detail all steps taken by the NSA to PROCESS communications in the course of Upstream surveillance.

OBJECTION: The DOJ Defendants object to Interrogatory No. 13 on the grounds that 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. The DOJ Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants' narrative statement]" in response to Interrogatory No. 13 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

Finally, the DOJ Defendants object to Interrogatory No. 13 on the ground that it seeks information about alleged NSA intelligence activities 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 14: DESCRIBE the entire process by which, pursuant to Upstream surveillance, the contents of INTERNET COMMUNICATIONS are INTERACTED WITH.

OBJECTION: The DOJ Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the DOJ Defendants' narrative statement]" in response to Interrogatory No. 14 on the grounds that it is

unduly burdensome and oppressive, and vague and ambiguous. The DOJ Defendants also 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 this interrogatory incapable of reasoned response.

The DOJ Defendants further object to Interrogatory No. 14 to the extent grounds that 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.

Finally, the DOJ Defendants object to Interrogatory No. 14 on the ground that it seeks information about alleged NSA intelligence activities 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 DOJ Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

Dated: January 8, 2018

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

/s/ Rodney Patton
RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
CAROLINE J. ANDERSON
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) 305-7919
Fax: (202) 616-8470
Email: rodney.patton@usdoj.gov

*Counsel for Defendants Department of Justice
and Attorney General Jefferson B. Sessions, III,
in His Official Capacity*

Pursuant to 28 U.S.C. § 1746. I, G. BRADLEY WEINSHEIMER, declare under penalty of perjury that the foregoing answers to Plaintiff Wikimedia's Interrogatories are true and correct to the best of my knowledge and belief, based on my personal knowledge and information made available to me in the course of my duties and responsibilities as the Acting Chief of Staff and the Director of Risk Management and Strategy for the National Security Division, United States Department of Justice.

Executed this 2^d day of January, 2018

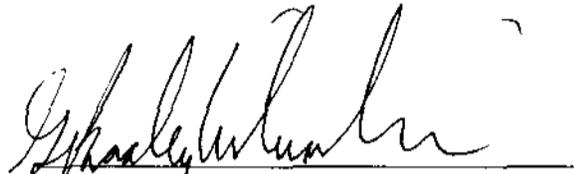

G. BRADLEY WEINSHEIMER
Acting Chief of Staff and Director of
Risk Management and Strategy
National Security Division
United States Department of Justice

Exhibit 16

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

_____)	
WIKIMEDIA FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	No. 15-cv-00662-TSE
)	
NATIONAL SECURITY AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	
_____)	

**OBJECTIONS AND RESPONSES OF DEFENDANTS
DEPARTMENT OF JUSTICE AND JEFFERSON B. SESSIONS, III, TO PLAINTIFF'S
FIRST AND SECOND SETS OF REQUESTS FOR PRODUCTION OF DOCUMENTS**

Pursuant to Rule 34 of the Federal Rules of Civil Procedure and District of Maryland Local Rule 104, Defendants Department of Justice (“DOJ”) and Jefferson B. Sessions, III, in his official capacity as Attorney General (together, the “DOJ Defendants”), by their undersigned attorneys, object and respond as follows to Plaintiff Wikimedia Foundation’s Request for Production of Documents and Second Set of Requests for Production of Documents, dated November 7 and 29, 2017, respectively.

GENERAL OBJECTIONS AND OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS

1. The DOJ Defendants object to Plaintiff’s Requests for Production of Documents to the extent, as set forth in response to specific requests below, that they seek information regarding the intelligence activities of the National Security Agency (“NSA”), which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

2. The DOJ Defendants object to Plaintiff’s Requests for Production of Documents 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.

3. As set forth in response to specific requests below, the DOJ 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 DOJ 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 DOJ Defendants.

4. As set forth in response to specific requests below, the DOJ 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 DOJ Defendants. The PCLOB is an independent agency within the Executive Branch, and the DOJ 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 DOJ Defendants.

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

6. As set forth in response to specific requests below, the DOJ 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 in the context

of specific requests as to render the specific requests in which it is used incapable of reasoned response.

7. As set forth in response to specific requests below, the DOJ Defendants object to Plaintiff's Requests for Production of Documents 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).

8. As set forth in response to specific requests below, the DOJ Defendants object to Instruction No. 9 in Plaintiff's Requests for Production of Documents, regarding the preparation of a privilege log, to the extent that providing the requested information as to each document for which privilege is claimed would itself divulge privileged information.

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

10. The DOJ Defendants object to Plaintiff's Requests for Production of Documents to the extent that any of them seeks the production of any documents or information not specifically involving the acquisition of Internet transactions through the use of NSA's Upstream Internet acquisition techniques pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1881a. In formulating these responses to Plaintiff's Requests for Production of Documents, the DOJ Defendants have limited the scope of their inquiry of knowledgeable persons, as well as their searches of appropriate records, to those persons and records reasonably calculated to possess information and documents specifically involving the acquisition of Internet transactions through the use of NSA's Upstream Internet acquisition techniques pursuant to Section 702 of the FISA.

11. 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 PLAINTIFF'S FIRST SET OF REQUESTS
FOR PRODUCTION OF DOCUMENTS**

REQUEST FOR PRODUCTION NO. 1: All DOCUMENTS referenced, paraphrased, or summarized in YOUR answers to Interrogatories.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they do not reference, paraphrase, or summarize any documents in their answers to Plaintiff's interrogatories. Accordingly, there are no documents in the DOJ Defendants' possession, custody, or control that are responsive to this request.

REQUEST FOR PRODUCTION NO. 2: DOCUMENTS sufficient to show or estimate the average number of optical fibers within the international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

OBJECTION: The DOJ Defendants object to Request for Production No. 2 as unduly burdensome and oppressive insofar as it requests that the DOJ Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the DOJ Defendants from public sources. The DOJ Defendants also object to Request for Production No. 2 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The DOJ Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 3: All DOCUMENTS listing, depicting, tallying, or describing the international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

OBJECTION: The DOJ Defendants object to Request for Production No. 3 as unduly burdensome and oppressive insofar as it requests that the DOJ Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the DOJ Defendants from public sources. The DOJ Defendants also object to Request for Production No. 3 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The DOJ Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 4: All DOCUMENTS listing, depicting, tallying, or describing the points at which international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES arrive at or depart from the UNITED STATES.

OBJECTION: The DOJ Defendants object to Request for Production No. 4 as unduly burdensome and oppressive insofar as it requests that the DOJ Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the DOJ Defendants from public sources. The DOJ Defendants also object to Request for Production No. 4 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The DOJ Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 5: All DOCUMENTS listing, depicting, tallying, or describing the terrestrial cables that are part of the INTERNET BACKBONE within the UNITED STATES.

OBJECTION: The DOJ Defendants object to Request for Production No. 5 as unduly burdensome and oppressive insofar as it requests that the DOJ Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the DOJ Defendants from public sources. The DOJ Defendants also object to Request for Production No. 5 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The DOJ Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 6: DOCUMENTS sufficient to show or estimate the number of persons TARGETED for Upstream surveillance pursuant to 50 U.S.C. § 1881a in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The DOJ Defendants object to Request for Production No. 6 on the grounds that 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, and which do not include Plaintiff's "dragnet" theory of standing rejected by the Fourth Circuit, *see Wikimedia Found. v. NSA*, 857 F.3d 193, 213-16 (4th Cir. 2017). The DOJ Defendants also object to Request for Production No. 6 as unduly burdensome and oppressive and

irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The DOJ Defendants further object to Request for Production 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control; but the DOJ Defendants refer Plaintiff to the NSA Defendants' response to this request.

REQUEST FOR PRODUCTION NO. 7: DOCUMENTS sufficient to show or estimate the number of SELECTORS used in conducting Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The DOJ Defendants object to Request for Production No. 7 on the grounds that 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, and which do not include Plaintiff's "dragnet" theory of standing rejected by the Fourth Circuit, *see Wikimedia Found. v. NSA*, 857 F.3d 193, 213-16 (4th Cir. 2017). The DOJ Defendants also object to Request for Production No. 7 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The DOJ Defendants further object to Request for Production No. 7 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have identified approximately ninety documents within their possession, custody, or control arguably responsive to this request. These documents are classified, and are being withheld in full on the basis of the objections stated above. The DOJ Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 8: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS COPIED using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The DOJ Defendants object to Request for Production No. 8 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The DOJ Defendants also object to the definition of the term "Internet Transaction" as vague and ambiguous insofar as it is meant, by its reference to the PCLOB Section 702 Report, to assign the term "Internet Transaction" a meaning other than that understood by the DOJ Defendants. The PCLOB is an independent agency within the Executive Branch, and the DOJ 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 DOJ Defendants.

The DOJ Defendants further object to Request for Production No. 8 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).

The DOJ Defendants further object to Request for Production No. 8 insofar as it purports to require them to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and to describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as itself seeking disclosures of information that is protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 9: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS REVIEWED for SELECTORS using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The DOJ Defendants object to Request for Production No. 9 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The DOJ Defendants also object to Request for Production No. 9 on the grounds that the definition of the term "Internet Transaction" is vague and ambiguous insofar as it is meant, by its reference to the PCLOB Section 702 Report, to assign the term "Internet Transaction" a meaning other than that understood by the DOJ Defendants. The PCLOB is an independent agency within the Executive Branch, and the DOJ 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 DOJ Defendants.

Furthermore, the DOJ Defendants object to Request for Production No. 9 on the grounds that the term "Review," as defined by Plaintiff, encompasses so many fundamentally different actions that as used herein it renders this request compound, unduly burdensome and

oppressive, vague and ambiguous, and particularly when viewed in the context of the phrase, “reviewed for selectors,” incapable of reasoned response.

Finally, the DOJ Defendants object to Request for Production No. 9 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 10: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS RETAINED using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The DOJ Defendants object to Request for Production No. 10 on the grounds that 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. The DOJ Defendants also object to Request for Production No. 10 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to 2010.

The DOJ Defendants further object to Request for Production No. 10 on the grounds that the definition of the term “Internet Transaction” is vague and ambiguous insofar as it is meant, by its reference to the PCLOB Section 702 Report, to assign the term “Internet Transaction” a meaning other than that understood by the DOJ Defendants. The PCLOB is an independent agency within the Executive Branch, and the DOJ 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 DOJ Defendants.

Finally, the DOJ Defendants object to Request for Production 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have identified five documents in their possession, custody, or control that contain information that are, in part, arguably responsive to this request. Redacted versions of three of these five documents showing all arguably responsive information are attached as Attachment A. Unredacted versions of these three documents, as well as the unredacted versions of the two documents being withheld in full, are being withheld on the basis of the objections stated above. The DOJ Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 11: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS RETAINED using Upstream surveillance that are to, from, or about “U.S. persons,” in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The DOJ Defendants object to Request for Production No. 11 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to 2010.

The DOJ Defendants also object to Request for Production No. 11 on the grounds that the definition of the term “Internet Transaction” is vague and ambiguous insofar as it is meant, by its reference to the PCLOB Section 702 Report, to assign the term “Internet Transaction” a meaning other than that understood by the DOJ Defendants. The PCLOB is an independent agency within the Executive Branch, and the DOJ 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 DOJ Defendants.

Furthermore, the DOJ Defendants object to Request for Production No. 11 on the grounds that 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.

Finally, the DOJ Defendants object to Request for Production No. 11 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 12: DOCUMENTS sufficient to show or estimate the average number of discrete INTERNET COMMUNICATIONS contained in a multi-communication transaction.

OBJECTION: The DOJ Defendants object to Request for Production No. 12 on the grounds that 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. The DOJ Defendants object to Request for Production No. 12 as vague and ambiguous insofar as it fails to specify the universe of communications for which the “average number” in a multi-communication transaction is requested. The DOJ Defendants also object to Request for Production No. 12 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 13: DOCUMENTS sufficient to show or estimate the number of CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The DOJ Defendants object to Request for Production No. 13 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to 2010.

The DOJ Defendants also object to Request for Production No. 13 on the grounds that the definition of the term “Circuit” is 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 “Circuit” a meaning other than its ordinary meaning in the telecommunications industry. The PCLOB is an independent agency within the Executive Branch, and the DOJ Defendants do not have information regarding what, if anything, that agency intended by the term “Circuit” beyond the ordinary meaning of that term within the telecommunications industry as it is understood by the DOJ Defendants.

Finally, the DOJ Defendants object to Request for Production No. 13 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 14: DOCUMENTS sufficient to show or estimate the combined bandwidth of the CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The DOJ Defendants object to Request for Production No. 14 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The DOJ Defendants also object to Request for Production No. 14 on the grounds that the definition of the term "Circuit" is 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 "Circuit" a meaning other than its ordinary meaning in the telecommunications industry. The PCLOB is an independent agency within the Executive Branch, and the DOJ 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 it is understood by the DOJ Defendants.

Finally, the DOJ Defendants object to Request for Production No. 14 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 15: DOCUMENTS sufficient to show or estimate the number of “international Internet link[s]”—as that term was 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 (F.I.S.C. Oct. 3, 2011)—monitored using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The DOJ Defendants object to Request for Production No. 15 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to 2010. The DOJ Defendants also object to Request for Production No. 15 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 (“FISC”) 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).

Finally, the DOJ Defendants object to Request for Production 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).

RESPONSE: In light of the objection stated above regarding the phrase “international Internet link,” for purposes of responding to this request, the DOJ Defendants construe that phrase to mean “location.” So construing the request, the DOJ Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 16: DOCUMENTS sufficient to show the number of Internet “chokepoints” or “choke points” (as that term is used by YOU) inside the UNITED STATES through which INTERNATIONAL COMMUNICATIONS enter and leave the UNITED STATES and where the NSA has established Upstream surveillance collection or PROCESSING capabilities.

OBJECTION: The DOJ Defendants object to Request for Production No. 16 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The DOJ Defendants also object to Request for Production No. 16 as vague and ambiguous insofar as it does not specify where or in what context the DOJ 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 DOJ Defendants object to this Request for Production 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 by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

Finally, the DOJ Defendants object to Request for Production No. 16 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).

RESPONSE: In light of the objection stated above regarding the terms “chokepoints” and “choke points,” for purposes of responding to this request, the DOJ Defendants construe those terms to mean “location.” So construing the request, the DOJ Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 17: All DOCUMENTS defining or describing the meaning of the term “Internet transaction.”

OBJECTION: The DOJ Defendants object to Request for Production No. 17 on the grounds that 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. The DOJ Defendants also object to Request for Production No. 17 as unduly burdensome and oppressive insofar as it seeks “all documents” defining or describing the meaning of the term “Internet transaction,” rather than documents sufficient to define that term.

The DOJ Defendants further object to Request for Production No. 17 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants refer Plaintiff to the NSA Defendants’ response to this request. In addition, the DOJ Defendants have identified four documents in their possession, custody, or control arguably responsive to this request. Redacted versions of three of these four documents are attached as Attachment B. A fourth responsive document is being withheld in full. Unredacted versions of

all four documents are being withheld on the basis of the objections stated above. The DOJ Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 18: All Foreign Intelligence Surveillance Court-approved targeting procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance.

OBJECTION: The DOJ Defendants object to Request for Production No. 18 on the grounds that 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. The DOJ Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The DOJ Defendants further object to Request for Production No. 18 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants refer Plaintiff to the NSA Defendants' response to this request, identifying the following two responsive documents publicly available in redacted form: 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, adopted by the Attorney General July 24, 2014 and submitted to the Foreign Intelligence Surveillance Court on or about July 25, 2014; and 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, adopted by the Attorney General March 29, 2017 and submitted to the Foreign Intelligence Surveillance Court on or about March 30, 2017. All other sets of relevant NSA Targeting Procedures are being withheld in full. The DOJ Defendants further object to this request, insofar as it purports to require them to describe the nature of the information redacted from these documents, and the nature of the classified information contained in other sets of relevant NSA Section 702 Targeting Procedures, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 19: All Foreign Intelligence Surveillance Court-approved minimization procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance.

OBJECTION: The DOJ Defendants object to Request for Production No. 19 on the grounds that 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. The DOJ Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The DOJ Defendants further object to Request for Production No. 19 to the extent that it seeks information 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants refer Plaintiff to the NSA Defendants' response to this request, identifying the following responsive documents publicly available in redacted form: 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, adopted by the Attorney General on October 31, 2011 and submitted to the Foreign Intelligence Surveillance Court on or about October 31, 2011; 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, adopted by the Attorney General on July 24, 2014 and submitted to the Foreign Intelligence Surveillance Court on or about July 28, 2014; 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, adopted by the Attorney General on July 10, 2015 and submitted to the Foreign Intelligence Surveillance Court on or about July 15, 2015; and 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, adopted by the Attorney General on March 29, 2017 and submitted to the Foreign Intelligence Surveillance Court on or about March 30, 2017. All other relevant sets of NSA Minimization

Procedures are being withheld in full. The DOJ Defendants further object to this request, insofar as it purports to require them to describe the nature of the information redacted from these documents, and the nature of the classified information contained in all other relevant sets of NSA Section 702 Minimization Procedures, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 20: Any supplemental procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance.

OBJECTION: The DOJ Defendants object to Request for Production No. 20 on the grounds that 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. The DOJ Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The DOJ Defendants further object to Request for Production No. 20 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants respond that they have identified three documents in their possession, custody, or control arguably responsive to this request. A redacted version of one of these documents is attached as Attachment C. An unredacted version of this document, as well as the other two classified documents withheld in full, are being withheld on the basis of the objections stated

above. The DOJ Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 21: All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court orders and opinions CONCERNING Upstream surveillance.

OBJECTION: The DOJ Defendants object to Request for Production No. 21 on the grounds that 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. The DOJ Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The DOJ Defendants further object to Request for Production No. 21 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the DOJ Defendants state that neither the Foreign Intelligence Surveillance Court of Review nor the Supreme Court has issued any orders or opinions concerning NSA's Upstream Internet surveillance. With regard to FISC orders or opinions concerning Upstream surveillance, many of those orders and opinions are already publicly available in redacted form as a result of

declassification pursuant to the USA FREEDOM Act, disclosures in response to Freedom of Information Act (“FOIA”) requests, and disclosures pursuant to the Transparency Initiative.

First, in accordance with section 402 of the USA-FREEDOM Act, Pub. L. 114-23, 129 Stat. 268, 281-82, codified at 50 U.S.C. § 1872, all FISC opinions and orders issued on or after June 2, 2015, that include a significant construction or interpretation of any provision of law, including FISA Section 702, 50 U.S.C. § 1881a, are now publicly available (in redacted form as appropriate) and equally accessible to Plaintiff as they are to the DOJ Defendants, at various locations on the ODNI public website.

Second, the Government has disclosed in redacted form (as appropriate) to the Electronic Frontier Foundation in response to a FOIA request “all decisions, orders, or opinions of the FISC or the FISC-R submitted to Congress by the Attorney General pursuant to section 6002 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. section 1871(a)(5)); 50 U.S.C. sections 1871(c)(1) & (2); and 50 U.S.C. section 1881f(b)(1)(D) between July 1, 2003 and June 1, 2015, which have not been previously declassified and made public (to include those decisions, orders, or opinions previously identified by the Department of Justice to the Brennan Center,

https://www.brennancenter.org/sites/default/files/publications/The_New_Era_of_Secret_Law.pdf), that remain classified.” Those documents are now publicly available (in redacted form) and equally accessible to Plaintiff as they are to the DOJ Defendants, at various locations on the ODNI public website.

Third, the Government has also disclosed (in redacted form as appropriate) other FISC opinions and orders concerning Upstream surveillance pursuant to other FOIA requests and those opinions and orders can also be found at various locations on the ODNI public website.

Finally, the Government has also disclosed (in redacted form as appropriate) other FISC opinions and orders concerning Upstream surveillance pursuant to the Transparency Initiative. Those FISC opinions and orders can also be found at various locations on the ODNI public website.

Unredacted versions of the above-referenced documents, and any other FISC orders and opinions concerning Upstream surveillance not referenced above, are being withheld on the basis of the objections stated above. The DOJ Defendants object to this request insofar as it purports to require them to describe the nature of the materials withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 22: All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court submissions CONCERNING Upstream surveillance.

OBJECTION: The DOJ Defendants object to Request for Production No. 22 on the grounds that 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. The DOJ Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The DOJ Defendants further object to Request for Production No. 22 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).

RESPONSE: To the extent not produced in response to Plaintiff's other Requests for Production herein, the DOJ Defendants have identified between 10,000 and 15,000 pages of responsive documents to this request and can state that all documents responsive to this request are being withheld on the basis of the objections stated above. The DOJ Defendants object to this request insofar as it purports to require them to describe the nature of the materials withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

**OBJECTIONS AND RESPONSES TO PLAINTIFF'S SECOND
SET OF REQUESTS FOR PRODUCTION OF DOCUMENTS**

REQUEST FOR PRODUCTION NO. 23: Any INTERNET COMMUNICATION of WIKIMEDIA that any DEFENDANT INTERACTED WITH in connection Upstream surveillance.

OBJECTION: The DOJ Defendants object to Request for Production No. 23 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The DOJ Defendants also object to Request for Production No. 23 to the extent 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).

The DOJ Defendants further object to this Request for Production No. 23 insofar as it purports to require them (i) to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and (ii) to describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 24: Any DOCUMENTS CONCERNING any INTERACTION WITH the INTERNET COMMUNICATIONS of WIKIMEDIA in connection with Upstream surveillance.

OBJECTION: The DOJ Defendants object to Request for Production No. 24 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The DOJ Defendants also object to Request for Production No. 24 to the extent 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).

The DOJ Defendants further object to this Request for Production insofar as it purports to require them (i) to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and (ii) to describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and

oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

DATED: January 8, 2018

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

/s/ Rodney Patton
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 Avenue, N.W., Room 7320
Washington, D.C. 20001
E-mail: rodney.patton@usdoj.gov
Phone: (202) 305-7919
Fax: (202) 616-8470

Counsel for the DOJ Defendants

Exhibit 17

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

_____)	
WIKIMEDIA FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	No. 1:15-cv-00662-TSE
)	
NATIONAL SECURITY AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	
_____)	

**OBJECTIONS AND RESPONSES BY DEFENDANTS OFFICE
OF THE DIRECTOR OF NATIONAL INTELLIGENCE AND DANIEL
COATS, DIRECTOR OF NATIONAL INTELLIGENCE, 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 Office of the Director of National Intelligence (“ODNI”) and Daniel Coats, in his official capacity as the Director of National Intelligence (together, the “ODNI 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 ODNI 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 ODNI 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 National Security Agency (“NSA”), which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

3. The ODNI 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 ODNI 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 ODNI 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 ODNI Defendants.

5. As set forth in response to specific requests below, the ODNI 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 ODNI Defendants. The PCLOB is an independent agency within the Executive Branch, and the ODNI 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 ODNI Defendants.

6. As set forth in response to specific requests below, the ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI Defendants further object to Request for Admission No. 1 as unduly burdensome and oppressive insofar as it requests that the ODNI Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the ODNI Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA, and on that basis admit for purposes of this action the response of defendants NSA and Adm. Michael S. Rogers, in his official capacity as Director of the NSA (together, the “NSA Defendants”), to this request for admission.

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 ODNI 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 ODNI Defendants further object to Request for Admission No. 2 as unduly burdensome and oppressive insofar as it requests that the ODNI Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the ODNI Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 ODNI 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 ODNI Defendants further object to Request for Admission No. 3 as unduly burdensome and oppressive insofar as it requests that the ODNI Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the ODNI Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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

OBJECTION: The ODNI 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 ODNI Defendants further object to Request for Admission No. 4 as unduly burdensome and oppressive insofar as it requests that the ODNI Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the ODNI Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 ODNI 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 ODNI 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 ODNI 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 ODNI Defendants further object to Request for Admission No. 6 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).

The ODNI 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 ODNI Defendants state based on reasonable inquiry that they have no knowledge or readily

obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 ODNI 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 ODNI 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 ODNI 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 ODNI Defendants further object to Request for Admission No. 8 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).

The ODNI 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 ODNI Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 ODNI 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 ODNI 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 ODNI 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 ODNI Defendants further object to Request for Admission No. 10 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).

The ODNI 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 ODNI Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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

OBJECTION: The ODNI 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 ODNI 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 ODNI Defendants state based on reasonable inquiry that they have no knowledge or readily obtainable information concerning the subject matter of this request that is independent of the knowledge and information possessed by the NSA Defendants, and on that basis admit for purposes of this action the response of the NSA Defendants to this request for admission.

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

OBJECTION: The ODNI 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 ODNI 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 ODNI 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 ODNI 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 (“FISC”) 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 ODNI 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 ODNI 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 ODNI 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 ODNI Defendants allegedly used 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 ODNI Defendants object to this Request for Admission 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI Defendants admit that Exhibit 1 to the NSA Defendants’ responses to these requests 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 ODNI 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: Subject to the objection stated above, and without waiving it, the ODNI Defendants admit that the 2014 NSA Section 702 Minimization Procedures, Exhibit 1 to the NSA Defendants' responses to these requests, 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 ODNI 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: Subject to the objection stated above, and without waiving it, the ODNI Defendants admit that the 2014 NSA Section 702 Minimization Procedures, Exhibit 1 to the NSA Defendants' responses to these requests, 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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 ODNI 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

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

/s/ Timothy A. Johnson
JULIA A. BERMAN
TIMOTHY A. JOHNSON
Trial Attorneys

U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7322
Washington, D.C. 20001
Phone: (202) 514-1359
Fax: (202) 616-8470
Email: timothy.johnson4@usdoj.gov

Counsel for the ODNI Defendants

Exhibit 18

3. As set forth in response to each interrogatory below, the ODNI Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants’ narrative statement]” on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

4. As set forth in response to specific interrogatories below, the ODNI 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 ODNI 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 ODNI Defendants.

5. As set forth in response to specific interrogatories below, the ODNI 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 ODNI Defendants. The PCLOB is an independent agency within the Executive Branch, and the ODNI 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 ODNI Defendants.

6. As set forth in response to specific interrogatories below, the ODNI Defendants object to the definition of the term “Review” as compound, unduly burdensome and oppressive,

and so vague and ambiguous as to render the specific interrogatories in which it is used incapable of reasoned response.

7. As set forth in response to specific interrogatories below, the ODNI Defendants object to the definition of the term “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 the specific interrogatories in which it is used incapable of reasoned response.

8. As set forth in response to specific interrogatories below, the ODNI Defendants object to Plaintiff’s Interrogatories 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. As set forth in response to specific interrogatories below, the ODNI Defendants object to Instruction No. 3 in Plaintiff’s Interrogatories to the extent that identification or description of each document or oral communication as to which privilege is claimed would itself divulge privileged information.

10. The ODNI Defendants object to Plaintiff’s Interrogatories to the extent that they seek information not involving the NSA’s Upstream Internet acquisition techniques as authorized by Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. § 1881a. In formulating these answers, the ODNI Defendants have limited the scope of their inquiry of knowledgeable persons, as well as their searches of appropriate records, to those persons and records reasonably calculated to possess information involving the NSA’s Upstream Internet acquisition techniques as authorized by Section 702 of the FISA.

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

12. Nothing contained in the following objections and responses shall be construed as a waiver of any applicable objection or privilege as to any interrogatory 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 INTERROGATORIES

INTERROGATORY NO. 1: DESCRIBE YOUR understanding of the definition of the term “international Internet link” as 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)—and provide all information supporting that understanding.

OBJECTION: The ODNI Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 1 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants also object to Interrogatory No. 1 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 ODNI Defendants further object to Interrogatory No. 1 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the

term ‘international Internet link’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 1 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 1 on the ground that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 2: DESCRIBE YOUR understanding of the definition of the term “circuit” as used at pages 36 to 37 of the PCLOB Report, and provide all information supporting that understanding, including but not limited to all information furnished by DEFENDANTS to the Privacy and Civil Liberties Oversight Board concerning this term.

OBJECTION: The ODNI Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants’ narrative statement]” in response to Interrogatory No. 2 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants also object to Interrogatory No. 2 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘circuit’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

The ODNI Defendants further object to this interrogatory on the ground that the PCLOB is an independent agency within the Executive Branch, and the ODNI 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 ODNI Defendants.

Finally, to the extent that Interrogatory No. 2 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 2 on the grounds that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that set forth in the NSA Defendants’ answer to this interrogatory or the PCLOB’s Section 702 Report itself. Thus, the ODNI Defendants refer Plaintiff to the PCLOB’s Section 702 Report and to the NSA Defendants’ response to this interrogatory.

INTERROGATORY NO. 3: DESCRIBE YOUR understanding of the definition of the term “filtering mechanism” as used at pages 10 and 47–48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The ODNI Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants’ narrative statement]” in response to Interrogatory No. 3 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants further object to Interrogatory No. 3 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘filtering mechanism’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 3 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 3 on the grounds that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified terms, can state no more than is set forth in the NSA Defendants’ answer to this interrogatory. Thus, the ODNI Defendants refer Plaintiff to the NSA Defendants’ response to this interrogatory.

INTERROGATORY NO. 4: DESCRIBE YOUR understanding of the definition of the term “scanned” as used at page 10 of the Memorandum in Support of Defendants’ Motion to Dismiss the First Amended Complaint, *Wikimedia Foundation v. NSA*, No. 15-cv-662-TSE (D. Md. Aug. 6, 2015), and provide all information supporting that understanding.

OBJECTION: The ODNI Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants’ narrative statement]” in response to Interrogatory No. 4 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants further object to Interrogatory No. 4 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘scanned’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 4 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 4 on the grounds that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified terms, can state no more than is set forth in the NSA Defendants’ answer to this interrogatory. Thus, the ODNI Defendants refer Plaintiff to the NSA Defendants’ response to this interrogatory.

INTERROGATORY NO. 5: DESCRIBE YOUR understanding of the definition of the term “screen” as used at page 48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The ODNI Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants’ narrative statement]” in response to Interrogatory No. 5 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants further object to Interrogatory No. 5 on the grounds that its instruction to “provide all information supporting [their] understanding [of the definition of the term ‘screen’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 5 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 5 on the grounds that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified terms, can state no more than is set forth in the NSA Defendants’ answer to this interrogatory. Thus, the ODNI Defendants refer Plaintiff to the NSA Defendants’ response to this interrogatory.

INTERROGATORY NO. 6: DESCRIBE YOUR understanding of the definition of the term “discrete communication” as used in the 2014 NSA Minimization Procedures, and provide all information supporting that understanding.

OBJECTION: The ODNI Defendants object to Interrogatory No. 6 on the grounds that 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. The ODNI Defendants also object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI

Defendants' narrative statement]” in response to Interrogatory No. 6 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants further object to Interrogatory No. 6 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘discrete communication’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 6 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 6 on the grounds that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that set forth in the NSA Defendants' answer to this interrogatory. Thus, the ODNI Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 7: DESCRIBE YOUR understanding of all features that a series of INTERNET PACKETS comprising an “Internet transaction” has in common, as the term “Internet transaction” is used in at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding. For example, the INTERNET PACKETS comprising an “Internet transaction” might share source and destination IP addresses, source and destination ports, and protocol type (albeit with the source and destination IP addresses and ports reversed for packets flowing in the opposite direction).

OBJECTION: ODNI Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants’ narrative statement]” in response to Interrogatory No. 7 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants further object to Interrogatory No. 7 on the grounds that its instruction to “provide all information supporting [their] understanding [of the ‘features that a series of Internet packets comprising an “Internet transaction” has in common’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, the ODNI Defendants object to Interrogatory No. 7 on the ground that it seeks classified information about alleged NSA intelligence activities 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 8: DESCRIBE YOUR understanding of the definitions of the terms “single communication transaction” and “multi-communication transaction” as used by the government in its submission to the Foreign Intelligence Surveillance Court, filed on August 16, 2011, and provide all information supporting that understanding. *See [Redacted]*, 2011 WL 10945618, at *9 (FISC Oct. 3, 2011).

OBJECTION: The ODNI Defendants object to Interrogatory No. 8 on the grounds that 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. The ODNI Defendants also object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants’ narrative statement]” in response to Interrogatory No. 8 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants also object to Interrogatory No. 8 as vague and ambiguous insofar as it attributes the phrase “single communication transaction” 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 *9 (FISC Oct. 3, 2011).

The ODNI Defendants further object to Interrogatory No. 8 on the grounds that its instruction to “provide all information supporting [their] understanding [of the terms ‘single communication transaction’ and ‘multi-communication transaction’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 8 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 8 on the grounds that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state that they do not have any additional knowledge or information regarding

the subject matter of this interrogatory beyond that set forth in the NSA Defendants' answer to this interrogatory. Thus, the ODNI Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 9: DESCRIBE YOUR understanding of the definitions of the terms “access” and “larger body of international communications” as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The ODNI Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants' narrative statement]” in response to Interrogatory No. 9 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants further object to Interrogatory No. 9 on the grounds that its instruction to “provide all information supporting [their] understanding [of the terms ‘access’ and ‘larger body of international communications’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 9 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 9 on the grounds that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they do not have any additional knowledge or information

regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified terms, can state no more than is set forth in the NSA Defendants' answer to this interrogatory. Thus, the ODNI Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 10: DESCRIBE YOUR understanding of the definition of the term “acquired” as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The ODNI Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants' narrative statement]” in response to Interrogatory No. 10 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants further object to Interrogatory No. 10 on the grounds that its instruction to “provide all information supporting [their] understanding [of the term ‘acquired’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 10 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 10 on the grounds that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified terms, can state no more than is set forth in the NSA Defendants' answer to this interrogatory. Thus, the ODNI Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 11: DESCRIBE YOUR understanding of the definition of the term "collection" as used at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The ODNI Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants' narrative statement]" in response to Interrogatory No. 11 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants further object to Interrogatory No. 11 on the grounds that its instruction to "provide all information supporting [their] understanding [of the term 'collection']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 11 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 11 on the grounds that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that possessed by the NSA, and, in unclassified terms, can state no more than is set forth in the NSA Defendants' answer to this interrogatory. Thus, the ODNI Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 12: DESCRIBE YOUR understanding of the definition of the term "Internet 'backbone'" as used at page 1 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The ODNI Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants' narrative statement]" in response to Interrogatory No. 12 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The ODNI Defendants further object to Interrogatory No. 12 on the grounds that its instruction to "provide all information supporting [their] understanding [of the term 'Internet 'backbone']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 12 seeks classified information about alleged NSA intelligence activities, the ODNI Defendants object to Interrogatory No. 12 on the grounds that it seeks information 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state that they do not have any additional knowledge or information regarding the subject matter of this interrogatory beyond that set forth in the NSA Defendants' answer to this interrogatory. Thus, the ODNI Defendants refer Plaintiff to the NSA Defendants' response to this interrogatory.

INTERROGATORY NO. 13: DESCRIBE in detail all steps taken by the NSA to PROCESS communications in the course of Upstream surveillance.

OBJECTION: The ODNI Defendants object to Interrogatory No. 13 on the grounds that 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. The ODNI Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants' narrative statement]" in response to Interrogatory No. 13 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

Finally, the ODNI Defendants object to Interrogatory No. 13 on the ground that it seeks information about alleged NSA intelligence activities 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 14: DESCRIBE the entire process by which, pursuant to Upstream surveillance, the contents of INTERNET COMMUNICATIONS are INTERACTED WITH.

OBJECTION: The ODNI Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the ODNI Defendants’ narrative statement]” in response to Interrogatory No. 14 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous. The ODNI Defendants also 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 this interrogatory incapable of reasoned response.

The ODNI Defendants further object to Interrogatory No. 14 to the extent grounds that 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.

Finally, the ODNI Defendants object to Interrogatory No. 14 on the ground that it seeks information about alleged NSA intelligence activities 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 ODNI Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

Dated: December 22, 2017

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTION
Senior Trial Counsel

/s/ Timothy A. Johnson

JULIA A. BERMAN
CAROLINE J. ANDERSON
TIMOTHY A. JOHNSON
Trial Attorneys

U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7322
Washington, D.C. 20001
Phone: (202) 514-1359
Fax: (202) 616-8470
Email: timothy.johnson4@usdoj.gov

Counsel for the ODNI Defendants

Pursuant to 28 U.S.C. § 1746. I, Alyssa McCarthy, declare under penalty of perjury that the foregoing answers to Plaintiff Wikimedia's Interrogatories are true and correct to the best of my knowledge and belief, based on my personal knowledge and information made available to me in the course of my duties and responsibilities of Associate General Counsel, Office of the General Counsel.

Executed this 22nd day of December, 2017

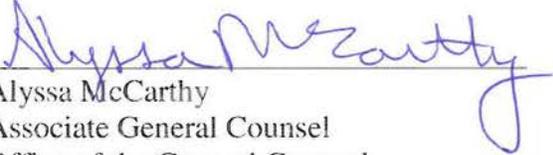

Alyssa McCarthy
Associate General Counsel
Office of the General Counsel
Office of the Director of National Intelligence

Exhibit 19

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	No. 15-cv-00662-TSE
)	
NATIONAL SECURITY AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	

**REVISED OBJECTIONS AND RESPONSES OF DEFENDANTS OFFICE OF THE
DIRECTOR OF NATIONAL INTELLIGENCE, AND DANIEL COATS,
DIRECTOR OF NATIONAL INTELLIGENCE, TO PLAINTIFF’S FIRST
AND SECOND SETS OF REQUESTS FOR PRODUCTION OF DOCUMENTS**

Pursuant to Rule 34 of the Federal Rules of Civil Procedure and District of Maryland Local Rule 104, Defendants Office of the Director of National Intelligence (“ODNI”), and Daniel Coats, in his official capacity as the Director of National Intelligence (together, the “ODNI Defendants”), by their undersigned attorneys, object and respond as follows to Plaintiff Wikimedia Foundation’s Request for Production of Documents and Second Set of Requests for Production of Documents, dated November 7 and 29, 2017, respectively.¹

**GENERAL OBJECTIONS AND
OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS**

1. The ODNI Defendants object to Plaintiff’s Requests for Production of Documents to the extent, as set forth in response to specific requests below, that they seek information regarding the intelligence activities of the National Security Agency (“NSA”), which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

¹ These Revised Objections and Responses supersede and replace the ODNI Defendants’ Objections and Responses dated January 8, 2018.

2. The ODNI Defendants object to Plaintiff's Requests for Production of Documents 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.

3. As set forth in response to specific requests below, the ODNI 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 ODNI 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 ODNI Defendants.

4. As set forth in response to specific requests below, the ODNI 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 ODNI Defendants. The PCLOB is an independent agency within the Executive Branch, and the ODNI 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 ODNI Defendants.

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

6. As set forth in response to specific requests below, the ODNI 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 the specific requests in which it is used incapable of reasoned response.

7. As set forth in response to specific requests below, the ODNI Defendants object to Plaintiff’s Requests for Production of Documents 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).

8. As set forth in response to specific requests below, the ODNI Defendants object to Instruction No. 9 in Plaintiff’s Requests for Production of Documents, regarding the preparation of a privilege log, to the extent that providing the requested information as to each document for which privilege is claimed would itself divulge privileged information.

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

10. The ODNI Defendants object to Plaintiff’s Requests for Production of Documents to the extent that any of them seeks the production of any documents or information not specifically involving the acquisition of Internet transactions through the use of NSA’s Upstream Internet acquisition techniques pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. § 1881a. In formulating these responses to Plaintiff’s Requests for Production of Documents, the ODNI Defendants have limited the scope of their inquiry of knowledgeable persons, as well as their searches of appropriate records, to those persons and records reasonably calculated to possess information and documents specifically involving the acquisition of Internet

transactions through the use of NSA's Upstream Internet acquisition techniques pursuant to Section 702 of the FISA.

11. 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 PLAINTIFF'S FIRST SET OF REQUESTS FOR PRODUCTION OF DOCUMENTS

REQUEST FOR PRODUCTION NO. 1: All DOCUMENTS referenced, paraphrased, or summarized in YOUR answers to Interrogatories.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they do not reference, paraphrase, or summarize any documents in their answers to Plaintiff's interrogatories. Accordingly, there are no documents in the ODNI Defendants' possession, custody, or control that are responsive to this request.

REQUEST FOR PRODUCTION NO. 2: DOCUMENTS sufficient to show or estimate the average number of optical fibers within the international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

OBJECTION: The ODNI Defendants object to Request for Production No. 2 as unduly burdensome and oppressive insofar as it requests that the ODNI Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the ODNI Defendants from public sources. The ODNI Defendants also object to Request for Production No. 2 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The ODNI Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 3: All DOCUMENTS listing, depicting, tallying, or describing the international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

OBJECTION: The ODNI Defendants object to Request for Production No. 3 as unduly burdensome and oppressive insofar as it requests that the ODNI Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the ODNI Defendants from public sources. The ODNI Defendants also object to Request for Production No. 3 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The ODNI Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 4: All DOCUMENTS listing, depicting, tallying, or describing the points at which international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES arrive at or depart from the UNITED STATES.

OBJECTION: The ODNI Defendants object to Request for Production No. 4 as unduly burdensome and oppressive insofar as it requests that the ODNI Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the ODNI Defendants from public sources. The ODNI Defendants also object to Request for Production No. 4 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to

seek prospective relief insofar as it seeks information dating back to July 8, 2008. The ODNI Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 5: All DOCUMENTS listing, depicting, tallying, or describing the terrestrial cables that are part of the INTERNET BACKBONE within the UNITED STATES.

OBJECTION: The ODNI Defendants object to Request for Production No. 5 as unduly burdensome and oppressive insofar as it requests that the ODNI Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the ODNI Defendants from public sources. The ODNI Defendants also object to Request for Production No. 5 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008. The ODNI Defendants further object to this request to the extent it seeks information that is protected from disclosure by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 6: DOCUMENTS sufficient to show or estimate the number of persons TARGETED for Upstream surveillance pursuant to 50 U.S.C. § 1881a in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The ODNI Defendants object to Request for Production No. 6 on the grounds that 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, and which do not include Plaintiff's "dragnet" theory of standing rejected by the Fourth Circuit, *see Wikimedia Found. v. NSA*, 857 F.3d 193, 213-16 (4th Cir. 2017). The ODNI Defendants also object to Request for Production No. 6 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The ODNI Defendants further object to Request for Production 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).

RESPONSE: Subject to the objections stated above, and without waiving them, ODNI has published Statistical Transparency Reports Regarding Use of National Security Authorities for calendar years 2013, 2014, 2015, and 2016, which include estimates of the numbers of targets affected by the U.S. Government's use of surveillance authority, including but not limited to section 702 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a. These reports are available, and are equally accessible to Plaintiff as they are to the ODNI Defendants, at the following Internet addresses:

- https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY_2013.pdf
- <https://www.dni.gov/files/icotr/CY%20Statistical%20Transparency%20Report.pdf>
- https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015
- https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf

Other than the above-referenced documents, the ODNI Defendants have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 7: DOCUMENTS sufficient to show or estimate the number of SELECTORS used in conducting Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The ODNI Defendants object to Request for Production No. 7 on the grounds that 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, and which do not include Plaintiff's "dragnet" theory of standing rejected by the Fourth Circuit, *see Wikimedia Found. v. NSA*, 857 F.3d 193, 213-16 (4th Cir. 2017). The ODNI Defendants also object to Request for Production No. 7 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The ODNI Defendants further object to Request for Production No. 7 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have identified twenty-three documents within their possession, custody, or control arguably responsive to this request. These documents are classified and are being withheld in full on the basis of the objections stated above. The ODNI Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole.

REQUEST FOR PRODUCTION NO. 8: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS COPIED using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The ODNI Defendants object to Request for Production No. 8 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The ODNI Defendants also object to the definition of the term "Internet Transaction" as vague and ambiguous insofar as it is meant, by its reference to the PCLOB Section 702 Report, to assign the term "Internet Transaction" a meaning other than that understood by the ODNI Defendants. The PCLOB is an independent agency within the Executive Branch, and the ODNI 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 ODNI Defendants.

The ODNI Defendants further object to Request for Production No. 8 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).

The ODNI Defendants further object to Request for Production No. 8 insofar as it purports to require them to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and to describe the nature of the materials withheld, if any, on the basis of the 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking disclosures of information that is itself protected by 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 9: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS REVIEWED for SELECTORS using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The ODNI Defendants object to Request for Production No. 9 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The ODNI Defendants also object to Request for Production No. 9 on the grounds that the definition of the term "Internet Transaction" is vague and ambiguous insofar as it is meant, by its reference to the PCLOB Section 702 Report, to assign the term "Internet Transaction" a meaning other than that understood by the ODNI Defendants. The PCLOB is an independent agency within the Executive Branch, and the ODNI 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 ODNI Defendants.

Furthermore, the ODNI Defendants object to Request for Production No. 9 on the grounds that the term "Review," as defined by Plaintiff, encompasses so many fundamentally different actions that as used herein it renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and particularly when viewed in the context of the phrase, "reviewed for selectors," incapable of reasoned response.

Finally, the ODNI Defendants object to Request for Production No. 9 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 10: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS RETAINED using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The ODNI Defendants object to Request for Production No. 10 on the grounds that 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. The ODNI Defendants also object to Request for Production No. 10 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The ODNI Defendants further object to Request for Production No. 10 on the grounds that the definition of the term "Internet Transaction" is vague and ambiguous insofar as it is meant, by its reference to the PCLOB Section 702 Report, to assign the term "Internet Transaction" a meaning other than that understood by the ODNI Defendants. The PCLOB is an independent agency within the Executive Branch, and the ODNI 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 ODNI Defendants.

Finally, the ODNI Defendants object to Request for Production 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have identified two documents in their possession, custody, or control arguably responsive to this request. A redacted version of one of these documents, which reflects the arguably responsive information, is available at the following Internet address:

- [https://www.dni.gov/files/icotr/ NYT/ Government%20Supplement%20to%20June%20201%20and%20June%2028,%202011%20Submissions%20\(August%2016,%202011\).pdf](https://www.dni.gov/files/icotr/ NYT/ Government%20Supplement%20to%20June%20201%20and%20June%2028,%202011%20Submissions%20(August%2016,%202011).pdf)

An unredacted version of this document, as well as the other classified document withheld in full, are being withheld on the basis of the objections stated above. The ODNI Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole.

REQUEST FOR PRODUCTION NO. 11: DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS RETAINED using Upstream surveillance that are to, from, or about “U.S. persons,” in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The ODNI Defendants object to Request for Production No. 11 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to 2010.

The ODNI Defendants also object to Request for Production No. 11 on the grounds that the definition of the term “Internet Transaction” is vague and ambiguous insofar as it is meant, by its reference to the PCLOB Section 702 Report, to assign the term “Internet Transaction” a meaning other than that understood by the ODNI Defendants. The PCLOB is an independent agency within the Executive Branch, and the ODNI 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 ODNI Defendants.

Furthermore, the ODNI Defendants object to Request for Production No. 11 on the grounds that 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.

Finally, the ODNI Defendants object to Request for Production No. 11 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 12: DOCUMENTS sufficient to show or estimate the average number of discrete INTERNET COMMUNICATIONS contained in a multi-communication transaction.

OBJECTION: The ODNI Defendants object to Request for Production No. 12 on the grounds that 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. The ODNI Defendants object to Request for Production No. 12 as vague and ambiguous insofar as it fails to specify the universe of communications for which the “average number” in a multi-communication transaction is requested. The ODNI Defendants also object to Request for Production No. 12 as unduly burdensome and oppressive and irrelevant to

Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 13: DOCUMENTS sufficient to show or estimate the number of CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The ODNI Defendants object to Request for Production No. 13 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The ODNI Defendants also object to Request for Production No. 13 on the grounds that the definition of the term "Circuit" is 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 "Circuit" a meaning other than its ordinary meaning in the telecommunications industry. The PCLOB is an independent agency within the Executive Branch, and the ODNI 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 ODNI Defendants.

Finally, the ODNI Defendants object to Request for Production No. 13 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 14: DOCUMENTS sufficient to show or estimate the combined bandwidth of the CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The ODNI Defendants object to Request for Production No. 14 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to 2010.

The ODNI Defendants also object to Request for Production No. 14 on the grounds that the definition of "Circuit" 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 "Circuit" a meaning other than its ordinary meaning in the telecommunications industry. The PCLOB is an independent agency within the Executive Branch, and the ODNI 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 ODNI Defendants.

Finally, the ODNI Defendants object to Request for Production No. 14 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 15: DOCUMENTS sufficient to show or estimate the number of “international Internet link[s]”—as that term was 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 (F.I.S.C. Oct. 3, 2011)—monitored using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.

OBJECTION: The ODNI Defendants object to Request for Production No. 15 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to 2010. The ODNI Defendants also object to Request for Production No. 15 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 (“FISC”) 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 neither be confirmed nor denied) that is protected from disclosure by the state secrets privilege and statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

Finally, the ODNI Defendants object to Request for Production 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).

RESPONSE: In light of the objection stated above regarding the phrase “international Internet link,” for the purposes of responding to this request, the ODNI Defendants construe this phrase to mean “location.” So construing this request, the ODNI Defendants respond that they

have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 16: DOCUMENTS sufficient to show the number of Internet “chokepoints” or “choke points” (as that term is used by YOU) inside the UNITED STATES through which INTERNATIONAL COMMUNICATIONS enter and leave the UNITED STATES and where the NSA has established Upstream surveillance collection or PROCESSING capabilities.

OBJECTION: The ODNI Defendants object to Request for Production No. 16 as unduly burdensome and oppressive and irrelevant to Plaintiff’s standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The ODNI Defendants also object to Request for Production No. 16 as vague and ambiguous insofar as it does not specify where or in what context the ODNI 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 ODNI Defendants object to this Request for Production 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).

Finally, the ODNI Defendants object to Request for Production No. 16 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).

RESPONSE: In light of the objection stated above regarding the terms “chokepoints” and “choke points,” for the purposes of responding to this request, the ODNI Defendants construe those terms to mean “location.” So construing this request, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 17: All DOCUMENTS defining or describing the meaning of the term “Internet transaction.”

OBJECTION: The ODNI Defendants object to Request for Production No. 17 on the grounds that 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. The ODNI Defendants also object to Request for Production No. 17 as unduly burdensome and oppressive insofar as it seeks “all documents” defining or describing the meaning of the term “Internet transaction,” rather than documents sufficient to define that term. The ODNI Defendants further object to Request for Production No. 17 to the extent it seeks documents protected by the deliberative process privilege.

Finally, the ODNI Defendants object to Request for Production No. 17 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants refer Plaintiff to the response of defendants NSA and Adm. Michael S. Rogers, in his official capacity as Director of the NSA (together, the “NSA Defendants”), to this request identifying the responsive documents publicly available in redacted form. In addition, the ODNI Defendants have identified documents in their possession, custody, or control arguably

responsive to this request. Redacted versions of three of these documents are available at the following Internet addresses:

- [https://www.dni.gov/files/icotr/ NYT/Government's%20Supplement%20to%20June%20201%20and%20June%2028,%202011%20Submissions%20\(August%2016,%202011\).pdf](https://www.dni.gov/files/icotr/ NYT/Government's%20Supplement%20to%20June%20201%20and%20June%2028,%202011%20Submissions%20(August%2016,%202011).pdf)
- <https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>
- <https://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf>

Unredacted versions of these documents, as well as the other documents withheld in full, are being withheld on the basis of the objections stated above. The ODNI Defendants object to this request to the extent it purports to require them to describe the nature of the materials withheld on these grounds, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole.

REQUEST FOR PRODUCTION NO. 18: All Foreign Intelligence Surveillance Court-approved targeting procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance.

OBJECTION: The ODNI Defendants object to Request for Production No. 18 on the grounds that 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. The ODNI Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The ODNI Defendants further object to Request for Production No. 18 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants refer Plaintiff to the NSA Defendants' response to this request, identifying the following two responsive documents publicly available in redacted form: 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, adopted by the Attorney General July 24, 2014, and submitted to the Foreign Intelligence Surveillance Court on or about July 25, 2014; and 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, adopted by the Attorney General March 29, 2017, and submitted to the Foreign Intelligence Surveillance Court on or about March 30, 2017. All other sets of relevant NSA Targeting Procedures are being withheld in full. The ODNI Defendants further object to this request, insofar as it purports to require them to describe the nature of the information redacted from these documents, and the nature of the classified information contained in other sets of relevant NSA Section 702 Targeting Procedures, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 19: All Foreign Intelligence Surveillance Court-approved minimization procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance.

OBJECTION: The ODNI Defendants object to Request for Production No. 19 on the grounds that 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. The ODNI Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The ODNI Defendants further object to Request for Production No. 19 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants refer Plaintiff to the NSA Defendants' response to this request, identifying the following responsive documents publicly available in redacted form: 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, adopted by the Attorney General on October 31, 2011, and submitted to the Foreign Intelligence Surveillance Court on or about October 31, 2011; 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, adopted by the Attorney General on July 24, 2014, and submitted to the Foreign Intelligence Surveillance Court on or about July 28, 2014; 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, adopted by the Attorney General on July 10, 2015, and submitted to the Foreign Intelligence Surveillance Court on or about July 15, 2015; and 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, adopted by the Attorney General on March 29, 2017, and submitted to the Foreign Intelligence Surveillance Court on or about March 30, 2017. All other relevant sets of NSA Minimization Procedures are being withheld in full. The ODNI Defendants further object to this request, insofar as it purports to require them to describe the nature of the information redacted from these documents, and the nature of the classified information contained in all other relevant sets of NSA Section 702 Minimization Procedures, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 20: Any supplemental procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance.

OBJECTION: The ODNI Defendants object to Request for Production No. 20 on the grounds that 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. The ODNI Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The ODNI Defendants further object to Request for Production No. 20 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants respond that they have been unable to locate documents responsive to this request within their possession, custody, or control.

REQUEST FOR PRODUCTION NO. 21: All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court orders and opinions CONCERNING Upstream surveillance.

OBJECTION: The ODNI Defendants object to Request for Production No. 21 on the grounds that 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. The ODNI Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The ODNI Defendants further object to Request for Production No. 21 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).

RESPONSE: Subject to the objections stated above, and without waiving them, the ODNI Defendants state that neither the Foreign Intelligence Surveillance Court of Review nor the Supreme Court has issued any orders or opinions concerning NSA's Upstream Internet surveillance. With regard to FISC orders or opinions concerning Upstream surveillance, many of those orders and opinions are already publicly available in redacted form as a result of

declassification pursuant to the USA FREEDOM Act, disclosures in response to Freedom of Information Act (“FOIA”) requests, and disclosures pursuant to the Transparency Initiative.

First, in accordance with section 402 of the USA FREEDOM Act, Pub. L. 114-23, 129 Stat. 268, 281-82, codified at 50 U.S.C. § 1872, all FISC opinions and orders issued on or after June 2, 2015, that include a significant construction or interpretation of any provision of law, including FISA Section 702, 50 U.S.C. § 1881a, are now publicly available (in redacted form as appropriate) and equally accessible to Plaintiff as they are to the ODNI Defendants, at various locations on the ODNI public website.

Second, the Government has disclosed in redacted form (as appropriate) to the Electronic Frontier Foundation in response to a FOIA request “all decisions, orders, or opinions of the FISC or the FISC-R submitted to Congress by the Attorney General pursuant to section 6002 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. section 1871(a)(5)); 50 U.S.C. sections 1871(c)(1) & (2); and 50 U.S.C. section 1881f(b)(1)(D) between July 1, 2003 and June 1, 2015, which have not been previously declassified and made public (to include those decisions, orders, or opinions previously identified by the Department of Justice to the Brennan Center, https://www.brennancenter.org/sites/default/files/publications/The_New_Era_of_Secret_Law.pdf), that remain classified.” Those documents are now publicly available (in redacted form) and equally accessible to Plaintiff as they are to the ODNI Defendants, at various locations on the ODNI public website.

Third, the Government has also disclosed (in redacted form as appropriate) other FISC opinions and orders concerning Upstream surveillance pursuant to other FOIA requests and those opinions and orders can also be found at various locations on the ODNI public website.

Finally, the Government has also disclosed (in redacted form as appropriate) other FISC opinions and orders concerning Upstream surveillance pursuant to the Transparency Initiative. Those FISC opinions and orders can also be found at various locations on the ODNI public website.

Unredacted versions of the above-referenced documents, and other FISC orders and opinions concerning Upstream surveillance not referenced above, if any, are being withheld on the basis of the objections stated above. The ODNI Defendants further object to this request insofar as it purports to require them to describe the nature of the materials withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 22: All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court submissions CONCERNING Upstream surveillance.

OBJECTION: The ODNI Defendants object to Request for Production No. 22 on the grounds that 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. The ODNI Defendants also object to this request as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The ODNI Defendants further object to Request for Production No. 22 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).

RESPONSE: To the extent not produced in response to Plaintiff's other Requests for Production herein, any responsive documents the ODNI Defendants may have would be a subset of those in the possession, custody, and control of defendants Department of Justice ("DOJ") and Jefferson B. Sessions, III, in his official capacity as Attorney General (together, the "DOJ Defendants"), and are being withheld on the basis of the objections stated above. The ODNI Defendants further object to this request insofar as it purports to require them to describe the nature of the materials withheld on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking information protected from disclosure by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

**OBJECTIONS AND RESPONSES TO PLAINTIFF'S SECOND
SET OF REQUESTS FOR PRODUCTION OF DOCUMENTS**

REQUEST FOR PRODUCTION NO. 23: Any INTERNET COMMUNICATION of WIKIMEDIA that any DEFENDANT INTERACTED WITH in connection Upstream surveillance.

OBJECTION: The ODNI Defendants object to Request for Production No. 23 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The ODNI Defendants also object to Request for Production No. 23 to the extent 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).

The ODNI Defendants further object to Request for Production No. 23 insofar as it purports to require them (i) to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and (ii) to describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking the disclosure of information that is itself protected by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

REQUEST FOR PRODUCTION NO. 24: Any DOCUMENTS CONCERNING any INTERACTION WITH the INTERNET COMMUNICATIONS of WIKIMEDIA in connection with Upstream surveillance.

OBJECTION: The ODNI Defendants object to Request for Production No. 24 as unduly burdensome and oppressive and irrelevant to Plaintiff's standing to seek prospective relief insofar as it seeks information dating back to July 8, 2008.

The ODNI Defendants also object to Request for Production No. 24 to the extent 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).

The ODNI Defendants further object to Request for Production No. 24 insofar as it purports to require them (i) to state whether there exist responsive materials that they are withholding on the basis of the foregoing objections, *see* Fed. R. Civ. P. 34(b)(2)(C), and (ii) to

describe the nature of the materials withheld, if any, on the basis of 50 U.S.C. § 3024(i)(1), 50 U.S.C. § 3605(a), and/or the state secrets privilege, *see* Fed. R. Civ. P. 26(b)(5)(A), as unduly burdensome and oppressive in the context of these requests as a whole, and as seeking the disclosure of information that is itself protected by 50 U.S.C. § 3024(i), 50 U.S.C. § 3605(a), and/or the state secrets privilege.

Dated: February 5, 2018

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

/s/ Timothy A. Johnson

JULIA A. BERMAN
TIMOTHY A. JOHNSON
Trial Attorneys
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7322
Washington, D.C. 20530
Tel: (202) 514-1359
Email: timothy.johnson4@usdoj.gov

Counsel for the ODNI Defendants

Exhibit 20

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
NSA Privilege Log
(March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
1.	6, 7	Database[s] containing information concerning NSA's SIGINT targets	TS//SI (at a minimum)	(i) sources and methods of authorized collection; (ii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; and (iii) operational information concerning intelligence activities	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
2.	10, 11, 12	Preserved 702 data collected pursuant to the upstream internet collection technique on or before March 17, 2017	TS//SI//NF	(i) sources and methods of authorized collection; (ii) raw SIGINT collected pursuant to FISA § 702; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; and (iv) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~Classified By: [REDACTED]
Derived From: NSA/CSSM 1-52
Dated: 20180110
Declassify On: 20430301~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
3.	10, 11, 12	702 data collected pursuant to the upstream internet collection technique after March 17, 2017	TS//SI//NF	(i) sources and methods of authorized collection; (ii) raw SIGINT collected pursuant to FISA § 702; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; and (iv) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
4.	13, 15, 16, 17	Classified Declaration of Admiral Michael S. Rogers, Director, National Security Agency, dated February [16], 2018, filed <i>ex parte</i> , <i>in camera</i> in <i>Jewel v. National Security Agency</i> , No. 4:08-cv-4373-JSW	TS//STLW//SI- [REDACTED]//OC/NF	(i) sources and methods of authorized collection; (ii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iii) operational information concerning NSA intelligence activities; (iv) identities of assisting electronic communications service providers; and (v) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

**Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
NSA Privilege Log
(March 19, 2018)**

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
5.	13, 14, 15, 16	Documents identifying one [or more than one] circuit on which NSA conducted Upstream surveillance for periods during the years 2015, 2016 and the first six months of 2017.	TS//SI//NF (at a minimum)	(i) sources and methods of authorized collection; (ii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iii) operational information concerning NSA intelligence activities; and (iv) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
6.	15, 16	Word document prepared by counsel on or about February 1, 2018, in connection with ongoing litigation in <i>Jewel v. National Security Agency</i> , No. 4:08-cv-4373-JSW, containing, among other things, the location[s] where Upstream surveillance occurs.	TS//SI-██████//NF	(i) sources and methods of authorized collection; (ii) operational information concerning NSA intelligence activities; (iii) identities of assisting electronic communications service providers; (iv) memorialization of communication between attorney and client concerning information requested by counsel to provide legal advice	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1); Attorney-Client Communication Privilege; Attorney Work Product Privilege
7.	15, 16	Power point presentation, last modified on or about October 2016, containing information concerning, among other things, Upstream infrastructure.	TS//SI//OC/NF	(i) sources and methods of authorized collection; and (ii) operational information concerning NSA intelligence activities	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
NSA Privilege Log
(March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
8.	19	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702, dated August 5, 2008	TS//SI/NF	(i) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; (ii) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
9.	19	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702, dated [REDACTED], 2009	S//SI/NF	(i) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; (ii) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
10.	19	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702, dated [REDACTED], 2010	TS//SI/NF	(i) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; (ii) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
11.	17, 19	Amended Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702, dated October 31, 2011	TS//SI/NF	(i) types of communications collected; (ii) sources and methods of authorized collection; (iii) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; (iv) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
12.	17, 19	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702, dated August 24, 2012	TS//SI/NF	(i) types of communications collected; (ii) sources and methods of authorized collection; (iii) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; (iv) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)*

NSA Privilege Log

(March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
13.	17, 19	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702, dated November 13, 2013	TS//SI//NF	(i) types of communications collected; (ii) sources and methods of authorized collection; (iii) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
14.	17, 19	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702, dated July 28, 2014	TS//SI//NF	(i) types of communications collected; (ii) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
15.	17, 19	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702, dated July 10, 2015	TS//SI//NF	(i) types of communications collected; (ii) sources and methods of authorized collection; and (iii) procedures regarding the retention, dissemination, and use of attorney-client communications acquired pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
16.	17, 19	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702, dated September 26, 2016	TS//SI//NF	(i) types of communications collected; (ii) sources and methods of authorized collection; (iii) extent to which acquired communications may be used or disclosed; and (iv) procedures regarding the retention, dissemination, and use of attorney-client communications acquired pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
17.	17, 19	Amended Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702, dated March 30, 2017	TS//SI//NF	(i) types of communications collected; (ii) sources and methods of authorized collection; (iii) extent to which acquired communications may be used or disclosed; and (iv) procedures regarding the retention, dissemination, and use of attorney-client communications acquired pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
18.	18	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702, dated August 5, 2008	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; (iv) sources and methods of authorized collection; (v) descriptions of government systems; and (vi) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
19.	18	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702, dated [REDACTED], 2009	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are non-United States persons reasonably believed to be located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; (iv) sources and methods of authorized collection; (v) descriptions of government systems; and (vi) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
20.	18	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702, dated [REDACTED], 2010	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are non-United States persons reasonably believed to be located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; (iv) sources and methods of authorized collection; (v) descriptions of government systems; and (vi) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D. Md.)

NSA Privilege Log

(March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
21.	18	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702, dated April 20/22, 2011	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are non-United States persons reasonably believed to be located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; (iv) sources and methods of authorized collection; (v) descriptions of government systems; and (vi) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
NSA Privilege Log
(March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
22.	18	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702, dated August 24, 2012	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection ; (iv) sources and methods of authorized collection; (v) descriptions of government systems; and (vi) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)*

NSA Privilege Log

(March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
23.	18	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702, dated July 31, 2013	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; (iv) sources and methods of authorized collection; (v) descriptions of government systems; and (vi) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
24.	18	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702, dated July 28, 2014	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) descriptions of government systems; (iv) types of communications collected; (v) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; and (vi) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
25.	18	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702, dated Jul 10, 2015.	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) descriptions of government systems; (iv) types of communications collected; (v) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; and (vi) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D. Md.)

NSA Privilege Log

(March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
26.	18	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702, dated September 26, 2016	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) descriptions of government systems; (iv) types of communications collected; (v) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; and (vi) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
27.	18	Amended procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702, dated March 30, 2017	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; and (iv) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
28.	17	FISC Memorandum Opinion and Order (J. Bates) dated October 3, 2011	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) types of communications collected; (iv) identities of assisting electronic communications service providers; (v) categories of information and analytic techniques used, and procedures followed, to assess whether a target is a non-United States person reasonably believed to be outside the United States; (vi) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; (vii) descriptions of government systems; (viii) detailed technical and operational information concerning intelligence activities	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
 NSA Privilege Log
 (March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
29.	17	Government's Response to the FISC's May 9, 2011 Briefing Order dated June 1, 2011	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) types of communications collected; (iv) identities of assisting electronic communications service providers; (v) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; (vi) descriptions of government systems; (vii) detailed technical and operational information concerning intelligence activities; (viii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D. Md.)

NSA Privilege Log

(March 19, 2018)

Entry	RFP #s	Description	Overall Classification	Nature of Privileged Information	Basis for Withholding
30.	21	Copies of Foreign intelligence Surveillance Court orders concerning upstream collection under Foreign Intelligence Surveillance Act § 702	The NSA Defendants refer Plaintiff to the DOJ Defendants' privilege log	With regard to Request for Production 21, the NSA Defendants refer Plaintiff to the DOJ Defendants' privilege log entries for this request. Any responsive documents the NSA Defendants have are a duplicative of those in the possession, custody, and control of the DOJ Defendants, and any information being withheld in those documents is withheld by NSA on the same basis as indicated in the DOJ Defendants' privilege log.	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
31.	22	Copies of submissions by the United States Government to the Foreign Intelligence Surveillance concerning upstream collection under Foreign Intelligence Surveillance Act § 702	The NSA Defendants refer Plaintiff to the DOJ Defendants' privilege log	With regard to Request for Production 22, the NSA Defendants refer Plaintiff to the DOJ Defendants' privilege log entries for this request. Any responsive documents the NSA Defendants have are a duplicative of those in the possession, custody, and control of the DOJ Defendants, and any information being withheld in those documents is withheld by NSA on the same basis as indicated in the DOJ Defendants' privilege log.	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

Exhibit 21

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log¹
(March 19, 2018)

Entry	RFP	Date Issued	Description of Order	Classification	Nature of Privileged Information	Basis for Withholding
1.	21	██████ 2009	Order by Foreign Intelligence Surveillance Court ("FISC") granting motion to extend time limit for review of Certification of the Director of National Intelligence and the Attorney General pursuant to § 702(g) of the Foreign Intelligence Surveillance Act of 1978 ("DNI/AG 702(g) Certification")	S	(i) subject matter and scope of collection authorized under § 702 of the Foreign Intelligence Surveillance Act of 1978 ("FISA § 702")	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
2.	21	██████ 2009	Order granting motion to extend time limit for review of DNI/AG 702(g) Certification	S	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
3.	21	██████ 2009	FISC Order finding no court action required with respect to 2008 DNI/AG 702(g) Certifications following compliance incident described in order in light of Government's remedial efforts	TS//SI//OC/NF	(i) subject matter and scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
4.	21	██████ 2010	FISC order approving amended DNI/AG 702(g) Certification and revised minimization procedures	S	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
5.	21	██████ 2010	FISC order approving amended DNI/AG 702(g) Certification and revised minimization procedures	S	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

¹ In accordance with the parties' discussions following the DOJ Defendants' service of their objections to Plaintiff's document requests, the DOJ Defendants are logging (i) only those FISC opinions and orders responsive to Plaintiff's request no. 21 that have not previously been publicly released by the Government at least in part, and (ii) only those submissions, responsive to Plaintiff's request no. 22, that were filed by the Government in connection with specified FISC opinions issued on April 26, 2017, [REDACTED] 2014, August 26, 2014, September 20, 2012, November 30 and October 3, 2011, April 7, 2009, and September 4, 2008. (The parties have not yet reached agreement on a term search of documents responsive to request no. 22, and so no documents reflective of such a search are included in this log.) During the parties' discussions Plaintiff did not take issue with the DOJ Defendants' objections to preparing a privilege log for request nos. 7, 10, and 17-20. Accordingly, the documents withheld by the DOJ Defendants in response to those requests on the basis of privilege are not included in this log.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)*

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date Issued	Description of Order	Classification	Nature of Privileged Information	Basis for Withholding
6.	21	██████ 2010	FISC order approving amended DNI/AG 702(g) Certification and revised minimization procedures.	S	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
7.	21	██████ 2010	FISC order approving amended DNI/AG 702(g) Certification and revised minimization procedures	S	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
8.	21	██████ 2010	FISC order approving amended DNI/AG 702(g) Certification and revised minimization procedures	S	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
9.	21	05/09/2011	FISC orders granting motion to extend time limits for review of DNI/AG § 702 Certifications	TS//SI//NF	(i) subject matter and scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
10.	21	07/14/2011	FISC orders granting motion to extend the time limit for review of DNI/AG 702(g) Certifications	S	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
11.	21	07/14/2011	FISC notices informing assisting electronic communications service providers of 07/14/2011 extension	TS//SI//NF	(i) subject matter and scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

2

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)*DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date Issued	Description of Order	Classification	Nature of Privileged Information	Basis for Withholding
12.	21	09/14/2011	FISC orders granting motion to extend the time limit for review of DNI/AG 702(g) certifications	TS//SI//NF	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
13.	21	09/14/2011	FISC notices informing assisting electronic communications service providers of 09/14/2011 extension	TS//SI//NF	(i) subject matter and scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
14.	21	10/05/2011	FISC secondary orders informing assisting electronic communications service providers of nature and time limits on collection authorized under FISA § 702	TS//SI//NF	(i) subject matter and scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
15.	21	11/01/2011	FISC notices of continued acquisition authority, informing assisting electronic communications service providers that Upstream acquisition of Internet communications remained authorized pending court action on Government's amendments to 2011 DNI/AG § 702(g) Certifications	TS//SI//NF	(i) subject matter and scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

3

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~
Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)
 DOJ Privilege Log
 (March 19, 2018)

Entry	RFP	Date Issued	Description of Order	Classification	Nature of Privileged Information	Basis for Withholding
16.	21	09/20/2012	FISC order approving amended DNI/AG § 702(g) Certifications and revised targeting and minimization procedures	S	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
17.	21	11/08/2013	FISC order granting motion to extend the time limit for review of DNI/AG 702(g) Certifications following compliance incident described in order	S	(i) subject matter and scope of collection authorized under FISA § 702; and (ii) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
18.	21	06/27/2014	FISC order requiring the Government to provide details pertaining to a compliance incident concerning a single, named target	TS [REDACTED] SI// OC/NF	(i) subject matter and scope of collection under FISA § 702; (ii) sources and methods and operational details of authorized collection; and (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
19.	21	07/07/2015	FISC order requiring Government to explain whether extension of time to review 2015 DNI/AG § 702(g) Certifications to allow meaningful amicus assistance would be consistent with national security	S	(i) subject matter and scope of collection under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
20.	21	07/23/2015	FISC order extending time to review 2015 DNI/AG § 702(g) certifications to allow for participation of amicus curiae	S	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
21.	21	10/14/2015	FISC order requiring the Government to describe the basis for the retention of certain information in specific NSA repositories discussed in order	TS//SI//NF	(i) subject matter and scope of collection authorized under FISA § 702; (ii) NSA analytic techniques; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

4

Classified By: Chief, Operations Section, OI, NSD USA GOV
 Derived From: DOJ/NSI-SCG 1 INT dated 20120701, NSA-SCG dated 20130930
 Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date Issued	Description of Order	Classification	Nature of Privileged Information	Basis for Withholding
22.	21	11/09/2015	FISC order approving amended DNI/AG 702(g) Certification and revised minimization procedures	S	(i) subject matter and scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
23.	21	12/30/2015	Supplemental FISC order requiring the Government to provide details pertaining to compliance incident concerning a single, named target	S//OC/NF	(i) subject matter and scope of collection under FISA § 702; (ii) sources and methods of authorized collection; and (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
24.	21	10/26/2016	FISC order extending time to review 2016 DNI/AG § 702(g) certifications	S	(i) subject matter and scope of collection under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
25.	21	01/27/2017	FISC order granting further extension of period for review of 2016 DNI/AG § 702(g) Certifications	TS//SI//NF	(i) subject matter and scope of collection under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
26.	21	01/27/2017	FISC notices of 01/27/2017 extension to assisting electronic communications service providers	TS//SI//NF	(i) subject matter and scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
27.	21	04/26/2017	FISC order approving amended 2016 DNI/AG § 702(g) Certifications and revised minimization procedures.	S	(i) subject matter and scope of collection under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

5

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~
Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)
 DOJ Privilege Log
 (March 19, 2018)

Entry	RFP	Date Issued	Description of Order	Classification	Nature of Privileged Information	Basis for Withholding
28.	21	04/26/2017	FISC order approving 2016 DNI/AG § 702(g) Certifications and targeting and minimization procedures.	S	(i) subject matter and scope of collection under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
29.	21	07/25/2017	Supplemental FISC order requiring the Government to provide details pertaining to a compliance incident concerning a single, named target.	TS//SI-G// OC/NF/FISA	(i) subject matter and scope of collection under FISA § 702; (ii) sources and methods of authorized collection; and (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
30.	22	08/05/2008	Government's Ex Parte Submission of Replacement Certification and Related Procedures and Request for an Order Approving Such Certification and Procedures, including a proposed Order for the Foreign Intelligence Surveillance Court ("FISC").	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under § 702 of the Foreign Intelligence Surveillance Act of 1978 ("FISA § 702")	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
31.	22	08/05/2008	Certification of the Director of National Intelligence and the Attorney General pursuant to § 702(g) of the Foreign Intelligence Surveillance Act of 1978 ("DNI/AG 702(g) Certification")	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

6

Classified By: Chief, Operations Section, OI, NSD USA GOV
 Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930
 Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
32.	22	08/05/2008	Affidavit of the Director, National Security Agency ("NSA"), in support of DNI/AG 702(g) Certification	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) sources and methods of authorized collection; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
33.	22	08/05/2008	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; (iv) sources and methods of authorized collection; (v) descriptions of government systems; and (vi) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

7

Classified By: Chief, Operations Section, OI, NSD USA GOV
Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930
Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
34.	22	08/05/2008	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702	TS//SI/NF	(i) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; and (ii) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
35.	22	08/05/2008	Exhibit listing entities concerning which the NSA seeks to acquire intelligence information under DNI/AG 702(g) Certification	TS//SI//OC/NF	(i) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
36.	22	08/26/2008	Government's Preliminary Responses to Certain Questions Posed by the Court	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) procedures followed to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (iv) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (v) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; and (iv) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

8

Classified By: Chief, Operations Section, OI, NSD USA GOV
 Derived From: DOJ/NSISCG 1 INT dated 20120701, NSA SCG dated 20130930
 Declassify On: 20430301

~~SECRET//NOFORN~~
Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)
 DOJ Privilege Log
 (March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
37.	22	08/28/2008	Notice of Filing Concerning 50 U.S.C. § 1806(i)	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
38.	22	09/02/2008	Notice of Clarification and Correction	S//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) categories of information and analytic techniques used, and procedures followed to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States.	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
39.	22	12/23/2008	Notice of compliance incident regarding collection pursuant to Section 702 of the FISA Amendments Act of 2008	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iv) identities of assisting electronic communications service providers; (v) types of communications collected; and (vi) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

9

Classified By: Chief, Operations Section, OI, NSD USA GOV
 Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930
 Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
40.	22	02/05/2009	Notice of compliance incident regarding collection pursuant to Section 702 of the FISA Amendments Act of 2008	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iv) identities of assisting electronic communications service providers; (v) types of communications collected; (vi) sources and methods of authorized collection; (vii) descriptions of government systems; and (viii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
41.	22	02/05/2009	Motion for an Order Extending Time Limit Pursuant to 50 U.S.C. § 1881a(j)(2)	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

10

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~
 Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)
 DOJ Privilege Log
 (March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
42.	22	03/17/2009	Government's supplement to its response to the Court's order of [REDACTED] 2009	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iv) identities of assisting electronic communications service providers; (v) types of communications collected; (vi) sources and methods of authorized collection; (vii) descriptions of government systems; and (viii) extent of authorized dissemination of acquired communications within the IC	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
43.	22	04/02/2009	Government's Second Supplement to its Response to the Court's Order of [REDACTED] 2009	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iv) identities of assisting electronic communications service providers; (v) types of communications collected; (vi) sources and methods of authorized collection; (vii) descriptions of government systems; (viii) extent of authorized dissemination of acquired communications within the IC; and (ix) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
44.	22	[REDACTED] 2009	Government's Ex Parte Submission of Replacement Certification and Related Procedures and Request for an Order Approving Such Certification and Procedures, including a proposed Order for the FISC.	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
45.	22	[REDACTED] 2009	DNI/AG 702(g) Certification	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(j)(1)

~~SECRET//NOFORN~~

12

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG-1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
46.	22	██████ 2009	Affidavit of the Director. NSA, in support of DNI/AG 702(g) Certification	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) sources and methods of authorized collection; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
47.	22	██████ 2009	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; (iv) sources and methods of authorized collection; (v) descriptions of government systems; and (vi) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

13

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
48.	22	██████ 2009	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702	S//SI/NF	(i) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; and (ii) extent to which acquired communications may be used or disclosed	State Secrets Privilege: 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
49.	22	██████ 2009	Government's Ex Parte Statement Concerning DNI/AG 702(g) Certification	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) extent to which acquired communications may be used or disclosed; and (iii) identities of assisting electronic communications service providers	State Secrets Privilege: 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

14

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
50.	22	██████ 2009	Government's Response to the Court's Order of ████████ 2009	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iv) identities of assisting electronic communications service providers; (v) types of communications collected; (vi) sources and methods of authorized collection; (vii) descriptions of government systems; (viii) extent of authorized dissemination of acquired communications within the IC; and (ix) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
51.	22	04/19/2011	Preliminary Notice of Compliance Incidents Regarding Collection Pursuant to Section 702	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) descriptions of government systems; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

15

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG-1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
52.	22	04/20/2011 04/22/2011	Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures. Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications, including proposed orders for the FISC	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
53.	22	04/20/2011 04/22/2011	DNI/AG 702(g) Certifications	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
54.	22	04/20/2011 04/22/2011	Affidavits of the Director, NSA, in support of DNI/AG 702(g) Certifications	TS//SI/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) sources and methods of authorized collection; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

16

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)*DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
55.	22	04/20/2011 04/22/2011	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; (iv) sources and methods of authorized collection; (v) descriptions of government systems; and (vi) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

17

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

SECRET//NOFORN*Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)***DOJ Privilege Log****(March 19, 2018)**

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
56.	22	05/02/2011	Clarification of National Security Agency's Upstream Collection Pursuant to Section 702 of FISA	TS//SI/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) descriptions of government systems; (iv) types of communications collected; (v) identities of assisting electronic communications service providers; and (vi) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
57.	22	05/05/2011	Motion for Orders Extending Time Limits Pursuant to 50 U.S.C. § 1881a(j)(2), and proposed orders for the FISC	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) descriptions of government systems; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

SECRET//NOFORN

18

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
58.	22	06/01/2011	Notice of Filing of Government's Response to the Court's Briefing Order of May 9, 2011	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) descriptions of government systems; (iv) types of communications collected; (v) identities of assisting electronic communications service providers; and (vi) nature or identity of specific individual(s) targeted or facilities tasked pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
59.	22	06/28/2011	Notice of Filing of Government's Response to the Court's Supplemental Questions of June 17, 2011	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) descriptions of government systems; (iv) types of communications collected; (v) identities of assisting electronic communications service providers; and (vi) nature or identity of specific individual(s) targeted or facilities tasked pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

19

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
60.	22	07/14/2011	Motion for Orders Extending Time Limits Pursuant to 50 U.S.C. § 1881a(j)(2)	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) descriptions of government systems; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
61.	22	08/16/2011	Notice of Filing of Government's Supplement to its Submissions of June 1 st and June 28 th , 2011	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) descriptions of government systems; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
62.	22	08/30/2011	Notice of Clarifications regarding four clarifications for the record concerning certain statements made in documents previously submitted to the FISC and how the NSA will apply its section 702 minimization procedures to certain communications	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) descriptions of government systems; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

20

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
63.	22	09/09/2011	Letter to FISC providing certain additional information related to questions raised by the Court and discussed during the September 7, 2011 hearing	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) descriptions of government systems; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
64.	22	09/13/2011	Letter to the FISC providing supplemental information to the September 9, 2011 correspondence to the Court	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
65.	22	10/05/2011	Motion for Secondary Orders to Certain Electronic Communications Service Providers	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) types of communications collected; and (iv) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
66.	22	10/31/2011	Government's Ex Parte Request for Issuance of Notices, including proposed notices for Continued Acquisition Authority for the FISC to review	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) types of communications collected; and (iv) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

21

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)*

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
67.	22	10/31/2011	Government's Ex Parte Submission of Amendment to Certifications and Related Procedures, Ex Parte Submission of Amended Minimization Procedures, including proposed orders for the FISC	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
68.	22	10/31/2011	Amended DNI/AG 702(g) Certifications	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
69.	22	10/31/2011	Amended Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702	TS//SI//NF	(i) types of communications collected; (ii) sources and methods of authorized collection; (iii) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; and (iv) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
70.	22	11/04/2011	Motion to Extend Time to file memorandum in response to the Court's Briefing Order of October 13, 2011, including proposed order for the FISC.	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

22

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
71.	22	11/15/2011	Notice of Filing of Government's Responses to FISC Questions Re: Amended 2011 Section 702 Certifications	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) types of communications collected; (iii) procedures followed to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (iv) procedures regarding the retention, dissemination, and use of communications acquired pursuant to FISA § 702; (v) types of communications collected; and (vi) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
72.	22	11/22/2011	Government's Response to the Court's Briefing Order of October 13, 2011	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature or identity of specific individual(s) targeted or facilities tasked pursuant to FISA § 702; and (iii) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
73.	22	11/23/2011	Preliminary Notice of Compliance Incident Regarding Collection Pursuant to Section 702	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) types of communications collected; and (iii) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

23

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

SECRET//NOFORN*Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)***DOJ Privilege Log****(March 19, 2018)**

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
74.	22	11/29/2011	Notice concerning NSA's application of amended NSA section 702 minimization procedures to certain transactions	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
75.	22	08/24/2012	Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications, including proposed orders for FISC	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) descriptions of government systems; (iii) types of communications collected; and (iv) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
76.	22	08/24/2012	DNI/AG 702(g) Certifications	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
77.	22	08/24/2012	Affidavits of the Acting Director, NSA, in support of DNI/AG 702(g) Certifications	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) sources and methods of authorized collection; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

SECRET//NOFORN

24

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~
Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)
 DOJ Privilege Log
 (March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
78.	22	08/24/2012	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) descriptions of government systems; (iv) types of communications collected; (v) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; and (vi) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
79.	22	08/24/2012	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702	TS//SI//NF	(i) types of communications collected; (ii) sources and methods of authorized collection; (iii) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; and (iv) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

25

Classified By: Chief, Operations Section, OI, NSD USA GOV
 Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930
 Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
80.	22	08/24/2012	Exhibits listing entities concerning which the NSA seeks to acquire foreign intelligence information under DNI/AG 702(g) Certifications	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
81.	22	08/28/2012	Letter to the FISC and attachment, a memorandum from NSA entitled, [REDACTED]	TS//SI//NF	(i) procedures followed to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) extent to which acquired communications may be used or disclosed; (iii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; and (iv) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
82.	22	09/12/2012	Supplement to the Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) descriptions of government systems; (iii) types of communications collected; (iv) sources and methods of authorized collection; and (v) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
83.	22	03/18/2014	Notice of NSA's Assessment of Purge Practices and Discovery of Incomplete Purges	S	(i) descriptions of government systems; and (ii) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

26

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
84.	22	05/29/2014	Supplemental Notice of NSA's Assessment of Purge Practices and Discovery of Incomplete Purges	S//REL TO USA, FVEY	(i) descriptions of government systems; (ii) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
85.	22	07/18/2014	Verified Report in Response to Order of June 27, 2014	TS [REDACTED] SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) descriptions of government systems; (iii) types of communications collected; (iv) sources and methods of authorized collection; (v) nature or identity of specific individuals targeted and/or facilities tasked pursuant to FISA § 702; (vi) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (vii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; and (viii) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

27

Classified By: Chief, Operations Section, OI, NSD USA GOV
Derived From: DOJ/NSI SCG-1 INT dated 20120701, NSA SCG dated 20130930
Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
86.	22	07/25/2014	Notice Regarding NSA Purge Practices	TS//SI//NF	(i) descriptions of government systems; (ii) extent to which acquired communications may be used or disclosed; and (iii) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
87.	22	07/28/2014	Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) descriptions of government systems; (iii) types of communications collected; (iv) sources and methods of authorized collection; and (v) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (vi) extent to which acquired communications may be used or disclosed; and (vii) nature or identity of specific individuals targeted and/or facilities tasked pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
88.	22	07/28/2014	DNI/AG 702(g) Certifications	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

28

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG-1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
89.	22	07/28/2014	Affidavits of the Acting Director, NSA, in support of DNI/AG 702(g) Certifications	TS//SI/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) sources and methods of authorized collection; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
90.	22	07/28/2014	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702	TS//SI/NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) descriptions of government systems; (iv) types of communications collected; (v) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; and (vi) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

29

Classified By: Chief, Operations Section, OI, NSD USA GOV
Derived From: DOJ/NSI-SCG 1 INT dated 20120701, NSA SCG dated 20130930
Declassify On: 20430301

SECRET//NOFORN*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)**DOJ Privilege Log
(March 19, 2018)**

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
91.	22	07/28/2014	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702	TS//SI//NF	(i) types of communications collected; and (ii) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
92.	22	07/28/2014	Exhibits listing entities concerning which the NSA seeks to acquire foreign intelligence information under DNI/AG 702(g) Certifications	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
93.	22	07/30/2014	Update Regarding Compliance Incidents Reported in the December 2013, March 2014, and June 2014 Section 702 Quarterly Reports	TS//SI//NF	(i) descriptions of government systems; (ii) nature or identity of specific individuals targeted and/or facilities tasked pursuant to FISA § 702; (iii) procedures followed to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (iv) procedures regarding the retention, dissemination, and use of attorney-client communications acquired pursuant to FISA § 702; (v) types of communications collected; (vi) extent to which acquired communications may be used or disclosed; and (vii) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

SECRET//NOFORN

30

Classified By: Chief, Operations Section, OI, NSD USA GOV
 Derived From: DOJ/NSI-SCG 1 INT dated 20120701, NSA SCG dated 20130930
 Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
94.	22	09/18/15	Preliminary Notice of Compliance Incident Regarding the Querying of Section 702-Acquired Data	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
95.	22	11/10/15	Preliminary Notice of Possible Compliance Incident Regarding the Dissemination of FISA-acquired Information	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) types of communications collected; (iv) extent of authorized dissemination of acquired communications within the IC; and (v) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
96.	22	12/22/15	Supplemental Notice of Compliance Incident Regarding [] Improper Queries	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) types of communications collected; (iv) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; (v) extent of authorized dissemination of acquired communications within the IC; and (vi) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

31

Classified By: Chief, Operations Section, OI, NSD-USA-GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20120930

Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
97.	22	12/29/15	Notice Regarding the Scope of Section 702 Pre-Tasking Review of [Certain Information]	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) types of communications collected; (iv) descriptions of government systems; and (v) procedures followed to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
98.	22	06/28/2016	Preliminary Notice of Compliance Incident Regarding Collection Pursuant to Section 702	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) types of communications collected; (iv) descriptions of government systems; and (v) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

32

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG-1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
99.	22	06/29/16	Notice of Compliance Incidents Regarding Improper Queries	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) sources and methods of authorized collection; (iv) types of communications collected; (v) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons; (vi) descriptions of government systems; and (vii) nature or identity of specific individual(s) or facility(ies) tasked pursuant to FISA	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

33

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
100.	22	08/24/2016	Update Regarding the Scope of Section 702 Pre-Tasking Review of [Certain Information]	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iv) sources and methods of authorized collection; (v) types of communications collected; (vi) extent of authorized dissemination of acquired communications within the IC; (vii) descriptions of government systems; and (viii) procedures followed to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

34

Classified By: Chief, Operations Section, OI, NSD-USA-GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
101.	22	09/13/2016	Update Regarding Post-Targeting Content Reviews	S//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iv) sources and methods of authorized collection; (v) types of communications collected; (vi) identities of assisting electronic communications service providers; (vii) descriptions of government systems; and (viii) procedures followed to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

35

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)
DOJ Privilege Log
 (March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
102.	22	09/21/2016	Preliminary Notice of Compliance Incident Regarding [a Specified Number of] Section 702-Tasked Facilities	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iv) sources and methods of authorized collection; (v) types of communications collected; (vi) identities of assisting electronic communications service providers; (vii) extent of authorized dissemination of acquired communications within the IC; (viii) descriptions of government systems communications service providers; (ix) procedures followed to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; and (x) procedures followed to ensure that information acquired through lawful collection is retained, used, and disseminated in a manner that protects the privacy of United States persons	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)*DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
103.	22	09/26/2016	Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iv) sources and methods of authorized collection; (v) types of communications collected; (vi) identities of assisting electronic communications service providers; (vii) extent of authorized dissemination of acquired communications within the IC; and (viii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
104.	22	09/26/2016	DNI/AG 702(g) Certifications	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

37

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
105.	22	09/26/2016	Affidavits of the Director, NSA, in support of DNI/AG 702(g) Certifications	TS//SI/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) sources and methods of authorized collection; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
106.	22	09/26/2016	Procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702	TS//SI/NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) descriptions of government systems; (iv) types of communications collected; (v) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; and (vi) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

38

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG-1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)*DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
107.	22	09/26/2016	Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702	TS//SI//NF	(i) types of communications collected; (ii) sources and methods of authorized collection; (iii) extent to which acquired communications may be used or disclosed; and (iv) procedures regarding the retention, dissemination, and use of attorney-client communications acquired pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
108.	22	09/26/2016	Exhibits listing entities concerning which the NSA seeks to acquire foreign intelligence information under DNI/AG 702(g) Certifications	TS//SI//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
109.	22	09/30/2016	Final Notice of Compliance Incidents Regarding Improper Queries	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA; (iv) sources and methods of authorized collection; and (v) types of communications collected	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

39

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
110.	22	09/30/2016	Supplemental Notice of Compliance Incident Regarding Collection Pursuant to Section 702	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) sources and methods of authorized collection; (iv) types of communications collected; and (v) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
111.	22	10/26/2016	Preliminary and Supplemental Notice of Compliance Incidents Regarding the Querying of Section 702-Acquired Data	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
112.	22	01/03/2017	Supplemental Notice of Compliance Incidents Regarding the Querying of Section 702-Acquired Data	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; and (iv) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

40

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

SECRET//NOFORN*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)**DOJ Privilege Log
(March 19, 2018)**

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
113.	22	01/27/2017	In re: DNI/AG 702(g) Certifications [], and their predecessor Certifications. Docket Numbers 702(i)-[]	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; and (iv) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
114.	22	01/27/2017	Notice of Extension	S	(i) subject matter and/or scope of collection authorized under FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
115.	22	02/24/2017	Supplemental Notice Regarding the National Security Agency's (NSA) Signals Intelligence (SIGINT) Information Storage Taxonomy and Purge Process for FISA-Acquired Information	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) sources and methods of authorized collection; (iv) types of communications collected; and (v) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

SECRET//NOFORN

41

Classified By: Chief, Operations Section, OI, NSD USA GOV
 Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930
 Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
116.	22	03/13/2017	Supplemental Letter Regarding Post-Targeting Content Reviews	S//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) types of communications collected; and (iv) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
117.	22	03/30/2017	Cover Filing for Amended DNI/AG 702(g) Certifications	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) types of communications collected; and (iv) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
118.	22	03/30/2017	Amended DNI/AG 702(g) Certifications	S//OC/NF	(i) subject matter and/or scope of collection authorized under FISA § 702; and (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
119.	22	03/30/2017	Affidavits of the Director, NSA, in support of Amended DNI/AG 702(g) Certifications	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) nature and/or identities of entities concerning which the NSA seeks to acquire foreign intelligence information; (iii) sources and methods of authorized collection; (iv) types of communications collected; and (v) identities of assisting electronic communications service providers	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

42

Classified By: Chief, Operations Section, OI, NSD USA GOV
Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930
Declassify On: 20420301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
120.	22	03/30/2017	Amended procedures used by the NSA for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to FISA § 702	TS//SI//NF	(i) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be non-United States persons located outside the United States; (ii) categories of information and analytic techniques used, and procedures followed, to assess whether a target is expected to possess, receive, and/or is likely to communicate foreign intelligence information; (iii) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection; and (iv) sources and methods of authorized collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
121.	22	03/30/2017	Amended Minimization Procedures used by the NSA in connection with acquisitions of foreign intelligence information pursuant to FISA § 702	TS//SI//NF	(i) types of communications collected; (ii) sources and methods of authorized collection; (iii) extent to which acquired communications may be used or disclosed; and (iv) procedures regarding the retention, dissemination, and use of attorney-client communications acquired pursuant to FISA § 702	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

43

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

~~SECRET//NOFORN~~

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log
(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
122.	22	04/03/2017	Supplemental Notice of Compliance Incidents Regarding Improper Queries	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
123.	22	04/07/2017	Preliminary Notice of Potential Compliance Incidents Regarding Improper Queries	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
124.	22	04/12/2017	Preliminary Notice of Potential Compliance Incidents Regarding Improper Queries	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
125.	22	06/15/2017	Section 702-Acquired Internet Transactions Existing in NSA's [Systems]	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
126.	22	07/13/2017	Supplemental Notice of Compliance Incidents Regarding Improper Queries	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

44

Classified By: Chief, Operations Section, OI, NSD USA GOV
 Derived From: DOJ/NSI SCG-1 INT dated 20120701, NSA SCG dated 20120930
 Declassify On: 20430301

~~SECRET//NOFORN~~*Wikimedia Foundation v. NSA*, No. 1:15-cv-00662-TSE (D.Md.)

DOJ Privilege Log

(March 19, 2018)

Entry	RFP	Date of Submission	Description of Document(s)	Classification	Nature of Privileged Information	Basis for Withholding
127.	22	07/13/2017	Notice of Compliance Incident Regarding Improper Queries	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection.	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
128.	22	07/25/2017	Government's First Update Regarding Information Acquired on or Before March 17, 2017, Pursuant to NSA's Section 702 Upstream Internet Collection	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
129.	22	10/23/2017	Government's Second Update Regarding Information Acquired on or Before March 17, 2017, Pursuant to NSA's Section 702 Upstream Internet Collection	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
130.	22	01/19/18	Government's Third Update Regarding Information Acquired on or Before March 17, 2017, Pursuant to NSA's Section 702 Upstream Internet Collection	TS//SI//NF	(i) subject matter and/or scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; and (iii) descriptions of government systems	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

~~SECRET//NOFORN~~

45

Classified By: Chief, Operations Section, OI, NSD USA GOV

Derived From: DOJ/NSI SCG 1 INT dated 20120701, NSA SCG dated 20130930

Declassify On: 20430301

Exhibit 22

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
ODNI Privilege Log
(March 19, 2018)

Entry	RFP	Description of Documents	Overall Classification	Nature of Privileged Information	Basis for Withholding
1.	7	Semi-annual joint assessments of the Director of National Intelligence and Attorney General pursuant to the Foreign Intelligence Surveillance Act (“FISA”) § 702(I)(1), 2015-2017	TS//SI//NF	(i) subject matter and scope of collection authorized under FISA § 702; (ii) sources and methods of authorized collection; (iii) Intelligence Community (“IC”) analytic techniques; (iv) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be located outside the United States; (v) extent of authorized dissemination of acquired communications within the IC; (vi) identification of IC repositories and systems; and (vii) extent to which acquired communications may be used or disclosed	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
2.	7	Annual reviews of the Director of the National Security Agency (“NSA”) pursuant to FISA § 702(I)(3), 2015-2017	TS//SI//NF/FISA	(i) subject matter and scope of collection authorized under FISA § 702; (ii) nature and identities of targets; (iii) sources and methods of authorized collection; (iv) NSA analytic techniques; (v) categories of information and analytic techniques used, and procedures followed, to ensure that persons targeted under FISA § 702 are reasonably believed to be located outside the United States; and (vi) extent of authorized dissemination of acquired communications within the IC	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
ODNI Privilege Log
(March 19, 2018)

Entry	RFP	Description of Documents	Overall Classification	Nature of Privileged Information	Basis for Withholding
3.	13, 15, 16, 17	Classified Declaration of Admiral Michael S. Rogers, Director, National Security Agency, dated February [16], 2018, filed <i>ex parte, in camera</i> in <i>Jewel v. National Security Agency</i> , No. 4:08-cv-4373-JSW	TS//STLW//SI-ECI AMB//OC/NF	(i) sources and methods of authorized collection; (ii) nature or identity of specific individual(s) targeted or facility(ies) tasked pursuant to FISA § 702; (iii) operational information concerning NSA intelligence activities; (iv) identities of assisting electronic communications service providers; and (v) information if disclosed that could be used by a foreign intelligence target to escape collection or minimize the likelihood of collection	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
3.	17	Copies of NSA minimization procedures approved by the Foreign Intelligence Surveillance Court (“FISC”), 2008-2017	TS//SI/NF	With regard to Request for Production 17, the ODNI Defendants refer Plaintiff to the NSA Defendants’ privilege log entries for this request numbered 8-17 which log copies of NSA minimization procedures. Any responsive documents the ODNI Defendants have are the same as or a subset of those in the possession, custody, and control of the NSA Defendants, and any information being withheld in those documents is withheld by ODNI on the same basis as indicated in the NSA Defendants’ privilege log.	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

**Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
ODNI Privilege Log
(March 19, 2018)**

Entry	RFP	Description of Documents	Overall Classification	Nature of Privileged Information	Basis for Withholding
4.	18	Copies of NSA targeting procedures approved by the FISC, 2008-2017	TS//SI/NF	With regard to Request for Production 18, the ODNI Defendants refer Plaintiff to the NSA Defendants' privilege log entries for this request numbered 18-27. Any responsive documents the ODNI Defendants have are the same as or a subset of those in the possession, custody, and control of the NSA Defendants, and any information being withheld in those documents is withheld by ODNI on the same basis as indicated in the NSA Defendants' privilege log.	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
5.	19	Copies of NSA minimization procedures approved by the FISC, 2008-2017	TS//SI/NF	With regard to Request for Production 19, the ODNI Defendants refer Plaintiff to the NSA Defendants' privilege log entries for this request numbered 8-17. Any responsive documents the ODNI Defendants have are the same as or a subset of those in the possession, custody, and control of the NSA Defendants, and any information being withheld in those documents is withheld by ODNI on the same basis as indicated in the NSA Defendants' privilege log.	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

Wikimedia Foundation v. NSA, No. 1:15-cv-00662-TSE (D. Md.)
ODNI Privilege Log
(March 19, 2018)

Entry	RFP	Description of Documents	Overall Classification	Nature of Privileged Information	Basis for Withholding
6.	21	Copies of FISC orders concerning upstream collection under FISA § 702, 2009-2017	The ODNI Defendants refer Plaintiff to the DOJ Defendants' privilege log	With regard to Request for Production 21, the ODNI Defendants refer Plaintiff to the DOJ Defendants' privilege log entries for this request numbered 1-29. Any responsive documents the ODNI Defendants have are the same as or a subset of those in the possession, custody, and control of the DOJ Defendants, and any information being withheld in those documents is withheld by ODNI on the same basis as indicated in the DOJ Defendants' privilege log.	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)
7	22	Copies of submissions by the United States Government to the FISC concerning upstream collection under FISA § 702, 2008-2018	The ODNI Defendants refer Plaintiff to the DOJ Defendants' privilege log	With regard to Request for Production 22, the ODNI Defendants refer Plaintiff to the DOJ Defendants' privilege log entries for this request numbered 30-130. Any responsive documents the ODNI Defendants have are the same as or a subset of those in the possession, custody, and control of the DOJ Defendants, and any information being withheld in those documents is withheld by ODNI on the same basis as indicated in the DOJ Defendants' privilege log.	State Secrets Privilege; 50 U.S.C. § 3605(a); 50 U.S.C. § 3024(i)(1)

Exhibit 23

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

WIKIMEDIA FOUNDATION,

*

Plaintiff,

*

v.

* **Civil Action No.: 15-cv-00662-TSE**

NATIONAL SECURITY AGENCY, *et al.*,

*

Defendants.

*

* * * * *

PLEASE TAKE NOTICE that, in accordance with Federal Rule of Civil Procedure 30(b)(6), Plaintiff Wikimedia Foundation, through its counsel, the American Civil Liberties Union Foundation, the Knight First Amendment Institute at Columbia University, and the American Civil Liberties Union Foundation of Maryland, will take the deposition on oral examination of the Designee(s) of National Security Agency (“NSA”) on April 2, 2018 at 10:00 a.m. at the offices of the American Civil Liberties Union Foundation, 125 Broad Street, New York, New York 10004, or wherever counsel shall later agree to conduct the deposition, so long as such designation is made with sufficient time to make all necessary arrangements. The deposition will be recorded by sound, sound-and-visual, or stenographic means by an officer of the court with the power to administer oaths. The deposition will continue from day to day until complete as allowed by applicable rules.

Pursuant to Federal Rule of Civil Procedure 30(b)(6), please designate the person or persons most knowledgeable and prepared to testify on the matters described in the “Topics of Examination” below, and who are known or reasonably available to you.

TOPICS OF EXAMINATION

1. The structure and functions of the Internet backbone and its component parts that transmit Internet communications subject to Upstream surveillance conducted under Section 702 of the Foreign Intelligence Surveillance Act (hereinafter, “Upstream surveillance”), including: the high-capacity submarine and terrestrial cables that transmit Internet communications directly into or directly out of the United States; the high-capacity terrestrial cables that transmit international Internet communications within the United States; the type and number of circuits carried on these Internet backbone cables; and the switches, routers, exchanges, or other points at which Internet backbone cables or circuits originate, terminate, or connect.
2. The definitions and meanings, as understood by the NSA, of terms that have been used in official public disclosures to describe Upstream surveillance, including the terms: circuit, link, Internet backbone, Internet transaction, Internet communication, international Internet link, scan, screen, filter, access, acquire, collect, ingest, filtering mechanism, screening mechanism, discrete communication, single communication transaction (“SCT”), multi-communication transaction (“MCT”), and larger body of international communications.¹
3. The ways in which the NSA or telecommunications providers acting on the NSA’s behalf access or interact with Internet communications in the course of Upstream surveillance—

¹ See, e.g., Government’s Response to the Court’s Briefing Order of May 9, 2011 (NSA-WIKI 00237–00277); [Redacted], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011); Mem. Opinion & Order, [Redacted], No. [Redacted] (FISC Apr. 26, 2017); Privacy & Civil Liberties Oversight Board (“PCLOB”), Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014); PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of FISA (2014), including pages 7–10, 12–13, 22, 30–41 & n.157, 79, 111 n.476, 119–26, 143–45; NSA targeting and minimization procedures applicable to Section 702 surveillance.

including the interception, copying, filtering, reviewing, screening, scanning, ingestion, and retention of Internet communications—and any NSA procedures relating to these activities.

4. The breadth and magnitude of Upstream surveillance, including:
 - a. The number and type of Internet communications or Internet transactions intercepted, accessed, copied, filtered, reviewed, screened, scanned, ingested, and/or retained by the NSA in the course of Upstream surveillance;
 - b. The number of targets under Upstream surveillance and Section 702 surveillance in total;
 - c. The number of selectors used by the NSA in Upstream surveillance; and
 - d. The number of circuits, international Internet links, and Internet backbone chokepoints on or at which the NSA conducts and has conducted Upstream surveillance.
5. If the NSA contends, for the purpose of contesting jurisdiction, that encryption bears in any way on the interception, accessing, copying, filtering, reviewing, screening, scanning, ingestion, or retention of Wikimedia's communications in the course of Upstream surveillance, the protocols used to encrypt communications subject to Upstream surveillance for which the NSA has the ability to decrypt, decipher, or render intelligible the contents of those communications.
6. The facts related to Upstream surveillance that the NSA has disclosed, or authorized the disclosure of, to the Foreign Intelligence Surveillance Court, the Foreign Intelligence Surveillance Court of Review, the United States Supreme Court, and/or the Privacy and Civil Liberties Oversight Board and that it has subsequently declassified.

Dated: March 17, 2018

/s/ Ashley Gorski

Ashley Gorski

Patrick Toomey

Asma Peracha

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

Exhibit 24

U.S. Department of Justice



Civil Division
Federal Programs Branch

*P.O. Box 883
Washington, D.C. 20044*

James J. Gilligan
Special Litigation Counsel

Telephone: (202) 514-3358
E-mail: james.gilligan@usdoj.gov

March 22, 2018

VIA ELECTRONIC MAIL

Patrick Toomey, Esq.
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004

Re: *Wikimedia Foundation v. National Security Agency, et al.,*
No. 1:15-cv-00662-TSE (D. Md.)

Dear Patrick:

Defendant National Security Agency (“NSA”) sets forth below its objections to Plaintiff’s notice of deposition of Defendant NSA pursuant to Federal Rule of Civil Procedure 30(b)(6). Defendant’s counsel are prepared to meet and confer with you regarding the objections set forth below at a date and time mutually convenient to all parties concerned.

SPECIFIC OBJECTIONS TO RULE 30(B)(6) DEPOSITION TOPICS

1. The structure and functions of the Internet backbone and its component parts that transmit Internet communications subject to Upstream surveillance conducted under Section 702 of the Foreign Intelligence Surveillance Act (hereinafter, “Upstream surveillance”), including: the high-capacity submarine and terrestrial cables that transmit Internet communications directly into or directly out of the United States; the high-capacity terrestrial cables that transmit international Internet communications within the United States; the type and number of circuits carried on these Internet backbone cables; and the switches, routers, exchanges, or other points at which Internet backbone cables or circuits originate, terminate, or connect.

OBJECTION: The NSA objects to a Rule 30(b)(6) deposition on this topic to the extent that it seeks to elicit information about the sources and methods and operational details of Upstream surveillance that is protected from disclosure by the state secrets privilege and the statutory privileges established under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a). To the extent that this topic seeks generic information about the “structure and functions

of the Internet backbone and its component parts” that is as available to Plaintiff as it is the Defendants, the NSA objects to this topic as unduly burdensome and oppressive and as seeking expert testimony that is not properly the subject of a Rule 30(b)(6) fact deposition. Counsel for the NSA is prepared to meet and confer with Plaintiff’s counsel, however, to ascertain whether this topic encompasses unclassified information for which a Rule 30(b)(6) deposition would be appropriate, subject to the terms and conditions stated below.

2. The definitions and meanings, as understood by the NSA, of terms that have been used in official public disclosures to describe Upstream surveillance, including the terms: circuit, link, Internet backbone, Internet transaction, Internet communication, international Internet link, scan, screen, filter, access, acquire, collect, ingest, filtering mechanism, screening mechanism, discrete communication, single communication transaction (“SCT”), multi-communication transaction (“MCT”), and larger body of international communications. [footnote omitted]

RESPONSE: The NSA objects to this topic to the extent it is meant to elicit information about the sources and methods and operational details of Upstream surveillance that is protected from disclosure by the state secrets privilege and the statutory privileges established under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a). The NSA does not object to providing unclassified deposition testimony on this topic, subject to the terms and conditions stated below, so far as it ascertainably encompasses unclassified information for which a Rule 30(b)(6) deposition would be appropriate.

3. The ways in which the NSA or telecommunications providers acting on the NSA’s behalf access or interact with Internet communications in the course of Upstream surveillance – including the interception, copying, filtering, reviewing, screening, scanning, ingestion, and retention of Internet communications – and any NSA procedures relating to these activities.

RESPONSE: The NSA objects to this topic to the extent it is meant to elicit information about the sources and methods and operational details of Upstream surveillance that is protected from disclosure by the state secrets privilege and the statutory privileges established under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a). The NSA does not object to providing unclassified deposition testimony on this topic, subject to the terms and conditions stated below, so far as it ascertainably encompasses unclassified information for which a Rule 30(b)(6) deposition would be appropriate.

4. The breadth and magnitude of Upstream surveillance, including: (a) the number and type of Internet communications or Internet transactions intercepted, accessed, copied, filtered, reviewed, screened, scanned, ingested, and/or retained by the NSA in the course of Upstream surveillance; (b) the number of targets under Upstream surveillance and Section 702 surveillance in total; (c) the number of selectors used by the NSA in Upstream surveillance; and (d) the number of circuits, international Internet links, and Internet backbone chokepoints on or at which the NSA conducts and has conducted Upstream surveillance.

OBJECTION: The NSA objects to a Rule 30(b)(6) deposition on the subjects identified in the topic above (which are also the subjects of earlier written discovery objected to by the NSA) on the grounds that “[t]he breadth and magnitude of Upstream surveillance,” including the information identified in subparts (a), (c), and (d), above, is protected from disclosure by the state secrets privilege and the statutory privileges established under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a). The NSA also objects to subpart (b), to the extent it seeks to elicit testimony regarding “the number of targets under Upstream surveillance,” on the same grounds. To the extent subpart (b) seeks testimony regarding “[t]he number of targets under . . . Section 702 surveillance in total,” the NSA objects that this information has already been publicly released by the Government, and a Rule 30(b)(6) deposition on this publicly available information would be unduly burdensome and cumulative.

5. If the NSA contends, for the purpose of contesting jurisdiction, that encryption bears in any way on the interception, accessing, copying, filtering, reviewing, screening, scanning, ingestion, or retention of Wikimedia’s communications in the course of Upstream surveillance, the protocols used to encrypt communications subject to Upstream surveillance for which the NSA has the ability to decrypt, decipher, or render intelligible the contents of those communications.

OBJECTION: The NSA objects to a Rule 30(b)(6) deposition on this topic on the grounds that it calls upon the NSA to confirm or deny the existence of “protocols used to encrypt communications subject to Upstream surveillance for which the NSA [allegedly] has the ability to decrypt, decipher, or render intelligible the contents of those communications.” The NSA cannot offer testimony concerning its ability or inability to decrypt, decipher, or render intelligible the contents of encrypted communications without revealing sources and methods of intelligence-gathering that are protected from disclosure by the state secrets privilege and the statutory privileges established under 50 U.S.C. §3024(i)(1) and 50 U.S.C. § 3605(a).

6. The facts related to Upstream surveillance that the NSA has disclosed, or authorized the disclosure of, to the Foreign Intelligence Surveillance Court, the Foreign Intelligence Surveillance Court of Review, the United States Supreme Court, and/or the Privacy and Civil Liberties Oversight Board and that it has subsequently declassified.

RESPONSE: The NSA objects to this topic to the extent it is intended to elicit information about (i) the sources and methods and operational details of Upstream surveillance that is protected from disclosure by the state secrets privilege and the statutory privileges established under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a), or (ii) matters placed under seal by the FISC. To the extent this topic seeks testimony regarding “facts related to Upstream surveillance that the NSA has disclosed, or authorized the disclosure of, . . . and that it has subsequently declassified,” the NSA objects that this information has already been publicly released by the Government, and a Rule 30(b)(6) deposition on this publicly available information would be unduly

burdensome and cumulative. The NSA does not object to providing unclassified deposition testimony on this topic, subject to the terms and conditions stated below, so far as it ascertainably encompasses unclassified information that is not under seal by the FISC for which a Rule 30(b)(6) deposition would be appropriate.

TERMS AND CONDITIONS OF DEPOSITIONS

The deposition of witnesses who possess classified information about NSA intelligence-gathering activities on subjects concerning alleged NSA surveillance presents significant risk for unauthorized disclosures of classified information that reasonably could be expected to cause exceptionally grave damage to the national security. Therefore, the NSA also objects to conducting the depositions contemplated by Plaintiff's Rule 30(b)(6) notice to the NSA, except pursuant to the following terms and conditions:

1. The depositions shall not be video- or audio-taped. If practical, the stenographer for the deposition should be cleared at the TS//SCI level and create the transcript in a manner that protects the transcript as if it contained classified information until the Government confirms that the transcript is unclassified.
2. Each deposition must take place at a location providing access to a Sensitive Compartmented Information Facility ("SCIF") where Government counsel and/or witnesses can discuss information classified up to the TS//SCI level, should the need arise to do so during the deposition in order to prevent disclosure of classified information protected by the state secrets privilege and the statutory privileges established under 50 U.S.C. § 3024(i)(1) and/or 50 U.S.C. § 3605(a) ("protected, privileged, or classified information").
3. An attorney for the U.S. Government present at a deposition may make such objections as he or she deems in good faith to be necessary to prevent the unauthorized disclosure of protected, privileged, or classified information.
4. An attorney for the U.S. Government may, at any time, direct the witness not to answer a question or to stop responding to a question if he or she deems in good faith that it is necessary to prevent the unauthorized disclosure or protected, privileged, or classified information.
5. An attorney for the U.S. Government (or the witness) may stop the deposition at any time in order to confer privately with the witness (or counsel) concerning prevention of the unauthorized disclosure of protected, privileged, or classified information.
6. Following the deposition the Government shall have a reasonable opportunity to conduct a review of the transcript for protected, privileged, or classified information, and to redact any protected, privileged, or classified information, prior to release of the transcript to Plaintiff's counsel.

7. Nothing in the testimony of a witness will constitute or be construed as a waiver of applicable protections or privileges.

Finally, the NSA objects to Plaintiff's Rule 30(b)(6) deposition notice as unduly burdensome and oppressive insofar as it purports to schedule the deposition to take place on Monday, April 2, 2018, the day after Easter Sunday, at the offices of Plaintiff's counsel in New York, New York, which is neither in the forum district nor the location of the NSA's principal place of business.

As noted above, Defendant's counsel are prepared to meet and confer with you regarding the objections set forth herein at a date and time mutually convenient to all parties concerned.

Very truly yours,

/s/ Jim Gilligan

James J. Gilligan

Exhibit 25

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~SECRET//ORCON,NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

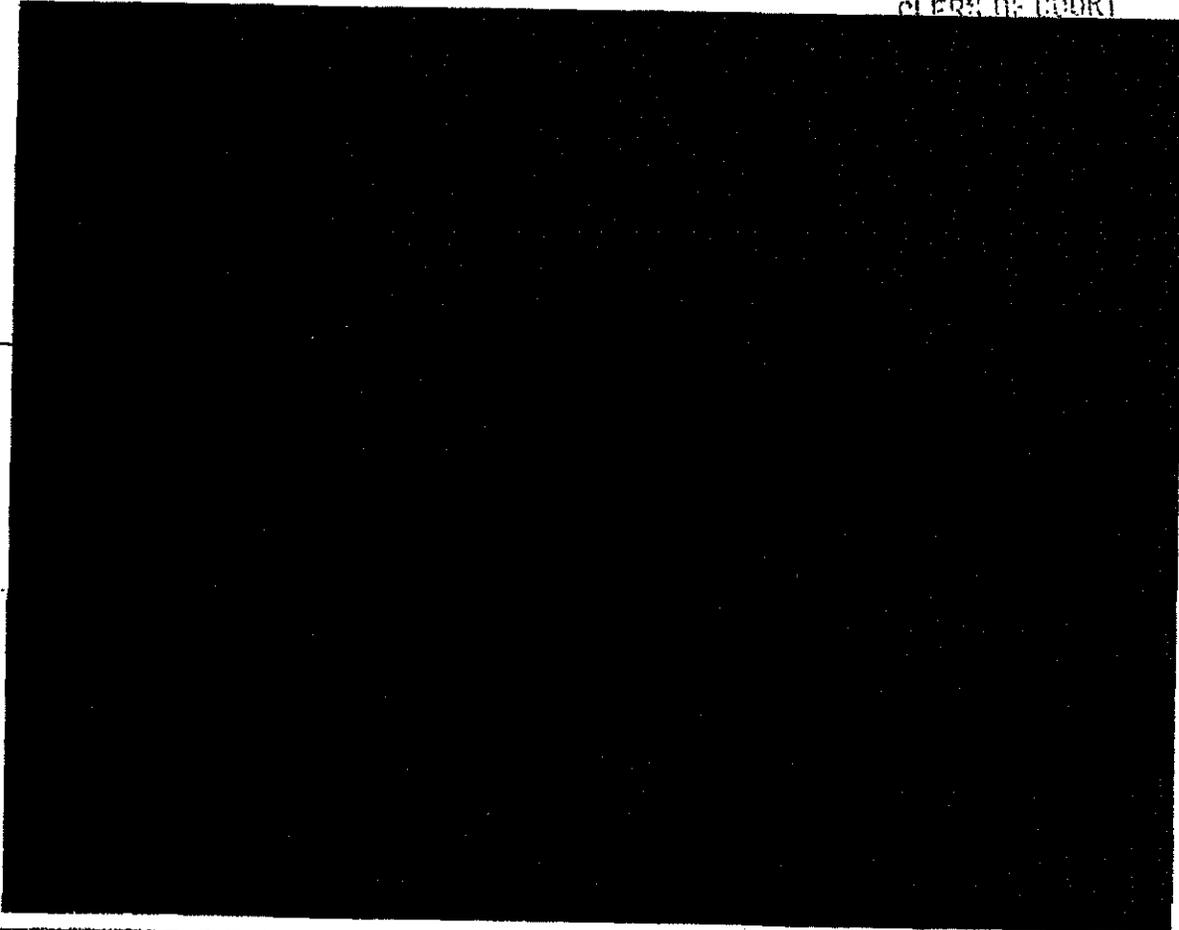
UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

2011 JUN -1 PM 4:47

WASHINGTON, D.C.

LEEANN FLYNN HALL
CLERK OF COURT



NOTICE OF FILING OF GOVERNMENT'S RESPONSE
TO THE COURT'S BRIEFING ORDER OF MAY 9, 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: ~~1 June 2036~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~SECRET//ORCON,NOFORN~~

questions posed by this Court in its Briefing Order of May 9, 2011, concerning the above-referenced matters. The Government may 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,



National Security Division
United States Department of Justice

~~SECRET//ORCON,NOFORN~~

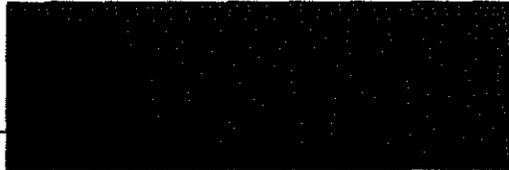
Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~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 Briefing Order of May 9, 2011, are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 1st day of June, 2011. (S)



Signals Intelligence Directorate Compliance Architect
National Security Agency

~~SECRET//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

GOVERNMENT'S RESPONSE TO THE COURT'S BRIEFING ORDER OF MAY 9, 2011

1. The government's May 2 Letter can be read to take the position that [redacted] [redacted] are communications authorized for collection under the Section 702 Certifications that have previously been approved by the Court. ~~(TS//SI//NF)~~

a. For how long has NSA been acquiring [redacted] through its upstream collection? ~~(TS//SI//NF)~~

Under the Section 702 Certifications, NSA acquires, *inter alia*, "Internet communications." *E.g.*, DNI/AG 702(g) Certification [redacted] Affidavit of General Keith B. Alexander, Director, National Security Agency (NSA), filed Apr. 20, 2011, at ¶ 4. As described by General Alexander, Internet communications "include, but are not limited to, [redacted]"

E.g., id. ~~(TS//SI//NF)~~

In the context of NSA's upstream collection techniques, NSA acquires Internet communications in the form of "transactions," which in this filing refers to 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.¹ A "transaction" might contain information or data representing either a discrete communication (e.g., an e-mail message), or multiple discrete communications [redacted]. As further described in the response to question 2 below, whenever a tasked selector is present within a transaction, NSA's "upstream" Internet collection techniques are designed to identify and acquire that transaction. ~~(TS//SI//NF)~~

¹ While the terms "Internet communication" and "transmission" have been used to describe the types of communications NSA acquires, NSA believes that, in the context of upstream collection, "transaction" is the more precise term from a technical perspective, because "transmission" could be understood to mean all data being exchanged on the Internet within a specific time period by a specific device, and an "Internet communication" may actually contain multiple logically separate communications between or among persons. ~~(TS//SI//NF)~~

The transactions discussed herein -- whether they contain single or multiple discrete communications having a commonality of a single user -- should not be confused with the two [redacted] compliance incidents initially reported to the Court on April 19, 2011, and further discussed below in the Government's response to question 6, which involved the [redacted] unrelated communications [redacted] ~~(TS//SI//NF)~~

~~Derived From: NSA/CSSM 1-52~~

~~Dated: 20070108~~

~~Declassify On: 20360501~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

At the time of acquisition, NSA's upstream Internet collection devices are, with limited exceptions further described below, not presently 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 may be to, from, or about a tasked selector.² Thus, in order to acquire transactions containing one or more communications to, from, or about a tasked selector, it has been necessary for NSA to employ these same upstream Internet collection techniques throughout the entire timeframe of all certifications authorized under Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter "FISA" or "the Act"), and the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 5, 2007) (hereinafter "PAA"). It was also necessary for NSA to employ these upstream collection techniques to implement the electronic surveillance authorized in *In re*

[REDACTED] Docket No. [REDACTED] and *In re* [REDACTED]

Docket No. [REDACTED] (~~TS//SI//NF~~)

b. According to the May 2 Letter, [REDACTED] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: (~~TS//SI//NF~~)

i. comports with the government's representations to the Court regarding the scope of upstream collection under Section 702 and the approvals granted by the Court in reliance upon those representations in Dockets 702(i) 08-01, [REDACTED] (see, e.g., Docket No. 702(i)-08-01, Aug. 27, 2008 Hearing Transcript at 19-26, 40-41 and Sept. 4, 2008 Memorandum Opinion at 15-20, 38); (~~TS//SI//NF~~)

The Government has concluded, after a careful review of the record, that its prior representations to the Court 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 collection techniques. The Government will attempt through this filing to provide the Court with a more thorough explanation of this technically complex collection. This notwithstanding, the Government respectfully submits that for the reasons set forth in its responses to questions 2.ii.,

² Specifically, as is discussed in the Government's response to questions 2(c) and (d) of the Court's briefing order, NSA does have the ability to identify and acquire discrete communications to, from, or about a tasked selector in certain cases [REDACTED]

[REDACTED] (~~TS//SI//NF~~)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

2.iii., and 5 below, NSA's prior and ongoing acquisition of information utilizing its upstream collection techniques is consistent with the Court's prior orders, meets the requirements of Section 702, and is consistent with the Fourth Amendment. ~~(TS//SI//NF)~~

b. According to the May 2 Letter, [REDACTED] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: ~~(TS//SI//NF)~~

ii. meets the requirements of Section 702, including, but not limited to, the requirement that 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 acquisition to be located in the United States"; and, ~~(TS//SI//NF)~~

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 LOCATED IN THE UNITED STATES. (S)

Under Section 702, the Government targets "persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). The Government determines whether the targeting of a person is consistent with Section 702 by applying Court-approved targeting procedures. 50 U.S.C. § 1881a(d). These targeting procedures must be "reasonably designed to (A) ensure that any acquisition authorized under subsection [702(a)] is limited to targeting persons reasonably believed to be located outside the United States; and (B) 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." 50 U.S.C. § 1881a(d)(1). (U)

A. The User of a Tasked Selector is the Person Being Targeted by all Acquisitions by NSA's Upstream Collection, Including Transactions That Contain Multiple Discrete Communications ~~(TS//SI//NF)~~

As previously explained to the Court, the Government "targets" a person by tasking for collection a "selector" (e.g., an e-mail account) believed to be used by that person. *See, e.g., In re DNI/AG Certification* [REDACTED] Docket No. 702(i)-08-01, Mem. Op. at 8 (USFISC Sept. 4, 2008) (hereinafter "[REDACTED] Mem. Op."). NSA acquires foreign intelligence information through the tasking of selectors by collecting communications to or from a selector used by a targeted person (hereinafter "to/from communications") and by collecting communications that refer to or are about a selector used by a targeted person (hereinafter "abouts communications"). *Id.*

~~(TS//SI//NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

In both of these types of acquisition, 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. Specifically, "the persons targeted by acquisition of to/from communications are the users of the tasked selectors," because "their communications are intentionally selected for acquisition." ██████████ Mem. Op. at 15. Similarly, the person being targeted by acquisition of abouts communications is also the user of the tasked selector, "because the government's purpose in acquiring abouts communications is to obtain information about that user." *Id.* at 18 (citation omitted). ~~(TS//SI//NF)~~

This remains true for all acquisitions conducted by NSA's upstream collection -- including transactions containing several discrete communications, only one of which may be to, from, or about the user of a tasked selector. As discussed above, the fact that there also may be communications to, from, or about persons other than the target in the transaction does not mean that those persons are also being targeted by the acquisition. 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 subjected to NSA's targeting procedures.³ 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.* ██████████ 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. United States v. Bin Laden*, 126 F. Supp. 2d 264, 281 (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) (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"). ~~(TS//SI//OC,NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

Id. at 4. Except in one circumstance previously reported to the Court,⁵ the Government is not aware of a case where an about collection resulted in the acquisition of a communication where both ends were inside the United States. NSA therefore continues to believe that these prior representations remain accurate. Accordingly, for the reasons described below, the Government respectfully submits that NSA's targeting procedures are reasonably designed to prevent, in the context of NSA's upstream collection, "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," including Internet communications [REDACTED] that have not been previously described to the Court. 50 U.S.C. § 1881a(d)(1)(B). ~~(TS//SI//OC,NF)~~

1. How NSA's IP Filters Work (S)

NSA acquires Internet communications by collecting the individual packets of data that make up those communications. [REDACTED]

[REDACTED]

~~(TS//SI//OC,NF)~~

[REDACTED]

5 [REDACTED]

~~(TS//SI//NF)~~

6 [REDACTED]

~~(TS//SI//NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

[REDACTED]

(TS//SI//OC,NF)

[REDACTED]

Additionally, at the time of acquisition, NSA's upstream Internet collection devices are, with limited exceptions further described below, not presently capable of distinguishing transactions containing only a single discrete communication to, from or about a targeted selector from transactions containing multiple discrete communications.⁷ Accordingly, NSA cannot prevent the acquisition of, or even mark for separate treatment, those types of transactions that may feature multiple discrete communications [REDACTED]. (TS//SI//OC,NF)

[REDACTED]

⁷ See Government's response to questions 2(c) and (d) *infra*. (U)

[REDACTED]

(TS//SI//NF)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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



¹⁰ ~~(TS//SI//OC,NF)~~

Except for the one instance noted above concerning an error by an electronic communication service provider, NSA is not aware of any instance in which its upstream collection on [redacted] or are subject to an IP filter nevertheless resulted in the acquisition of a communication as to which the sender and all intended recipients were known at the time of acquisition to be located in the United States.¹¹ This includes those situations in which NSA might collect unrelated communications when acquiring Internet communications that include multiple, discrete communications. ~~(TS//SI//NF)~~



~~(TS//SI//OC,NF)~~



~~(TS//SI//OC,NF)~~

¹¹ It is noteworthy that the provider error that resulted in the acquisition of domestic communications was first identified not by the provider, but by an NSA analyst who recognized a domestic communication in NSA's repositories, realized that such a domestic communication should not have been acquired, and properly reported the communication through NSA channels. NSA investigated this matter and found that domestic communications had been acquired not due to any theoretical limitations in its IP filter technology, but instead because [redacted]. The domestic overcollection caused by this incident represented a very small portion of NSA's collection during the time period of the overcollection, and an even smaller portion of NSA's collection since the initiation of its Section 702 acquisitions, but the error was still discovered and remedied. It is therefore particularly noteworthy that no NSA analyst has otherwise yet discovered a wholly domestic communication in NSA's repositories collected through NSA's upstream collection systems.

~~(TS//SI//OC,NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

In May 2011, NSA conducted two tests of its Section 702 upstream collection in order to determine the likelihood of collecting an Internet transaction between a user in the United States and [REDACTED]. The first test included [REDACTED]

[REDACTED]
The second test included [REDACTED]

~~(TS//SI//NF)~~

The first test sample included no records where both the sender and receiver IP addresses were in the United States [REDACTED]

[REDACTED] NSA analysis further revealed that only [REDACTED] of the more than [REDACTED] (0.028%) had characteristics consistent with a person in the United States accessing a [REDACTED]

[REDACTED] For the second dataset, NSA analysis discovered that only [REDACTED] out of more than [REDACTED] total records (0.0016%) included a non-targeted user likely accessing the Internet from an IP address in the United States. [REDACTED]

[REDACTED] NSA assesses, based on analysis of the underlying data, that this activity in fact was [REDACTED] copies of the same Internet transaction, [REDACTED]. There is no indication that NSA collected any wholly domestic communications through its acquisition of this transaction.

~~(TS//SI//NF)~~

In sum, the Government submits that the two test samples discussed above, coupled with the fact that, except as noted above, no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication collected through NSA's upstream collection systems, strongly suggests that NSA's acquisition of transactions or single Internet communications between users in the United States and [REDACTED] currently occurs only in a very small percentage of cases. Even those rare cases, moreover, won't necessarily involve a user in the United States receiving from the [REDACTED] a transaction containing a communication from a person known at the time of acquisition to be located in the United States.¹² ~~(TS//SI//NF)~~

¹² Additionally, as discussed elsewhere herein, even if the sender is located in the United States, the communication likely will not contain any reliable information that would enable NSA to determine at the time of acquisition the sender's location. ~~(TS//SI//OC,NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

2. The [REDACTED] Means by Which NSA Prevents the Intentional Acquisition of Communications as to Which the Sender and All Intended Recipients Are Known to be Located In the United States at the Time of Acquisition Are Reasonable (S)

This Court has found that NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications in which the sender and all intended recipients are known at the time of acquisition to be located in the United States. In approving DNI/AG 702(g) Certification [REDACTED], with respect to NSA's upstream collection of "abouts" communications, in particular, the Court noted that NSA "relies on [REDACTED] means of ensuring that at least one party to the communication is located outside the United States." [REDACTED] Mem. Op. at 19. As described above, those [REDACTED] means are NSA's use of "an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas" and NSA's [REDACTED] NSA

Targeting Procedures at 1-2; see also [REDACTED] Mem. Op. at 19. Relying on the Government's representations that these [REDACTED] means had prevented the acquisition of wholly domestic communications under the PAA, and recognizing that it is "theoretically possible that a wholly domestic communication could be acquired as a result of the [REDACTED]" the Court 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." [REDACTED] Mem. Op. at 20 & n.17. The Government respectfully submits that there is no aspect of NSA's upstream collection, as further described herein, that would 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)~~

Two aspects of NSA's upstream collection activity that have not been specifically addressed by the Court are discussed herein: first, the fact that NSA acquires some communications [REDACTED]

and second, the fact that NSA could acquire [REDACTED] -- whether retrieving a single, discrete communication, or a transaction containing several discrete communications -- possibly resulting in the acquisition of wholly domestic communications. ~~(TS//SI//OC,NF)~~

a. Acquisition of Communications that [REDACTED]

(S)

First, [REDACTED]

-- 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 located in the United

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

States.

[REDACTED]

(TS//SI//OC,NF)

b. **Theoretical Acquisition of Wholly Domestic Communications Through**

[REDACTED]

(TS//SI//NF)

With respect to the above-discussed theoretical cases in which NSA could acquire a [REDACTED] NSA's targeting procedures also 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 located in the United States. As discussed above, NSA assesses that [REDACTED]

[REDACTED] only in a minute percentage of cases. Yet even in those rare cases, there would be no way for NSA to know at the time of acquisition that the sender and intended recipient are located in the United States. [REDACTED]

[REDACTED] NSA cannot at that point know the location of the intended recipient, who has yet to receive the message. Likewise, [REDACTED]

[REDACTED] it is highly unlikely that the communication would contain information useful in determining the sender's true location.¹³ In any event, it is currently not possible for NSA's IP filters to [REDACTED]

[REDACTED] Because NSA's filters will be looking at the best available information, [REDACTED] it cannot be said that the sender and all intended recipients of those communications are known at the time of acquisition to be located in the United States. Similarly, in the case of NSA's [REDACTED]

13

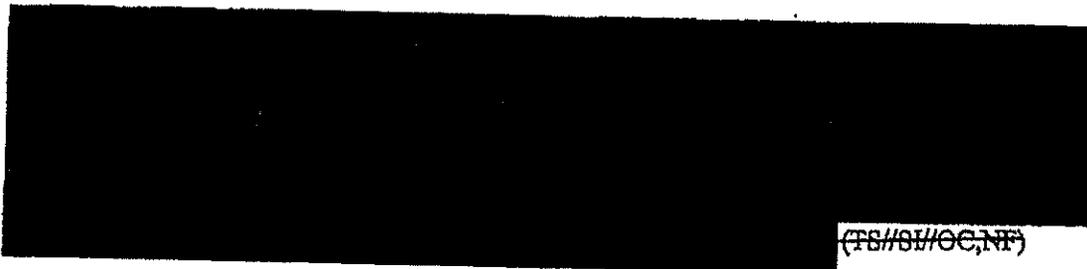
(TS//SI//OC,NF)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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



Accordingly, NSA has designed its systems so that it should never intentionally acquire a communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States. To the extent that NSA does unintentionally acquire such communications, NSA must treat those communications in accordance with its minimization procedures -- just as it must for other types of communications that it is prohibited from intentionally collecting under subsection 702(b), but nevertheless sometimes does unintentionally acquire, such as communications acquired from a target while that target is located inside the United States. ~~(TS//SI//OC,NF)~~

c. Conclusion (U)

Although for different reasons than those discussed above, the Court has recognized that it is "theoretically possible that a wholly domestic communication could be acquired" through NSA's upstream collection of "abouts" communications. ~~Mem. Op. at 20 n.17.~~ For the reasons outlined above, the Government respectfully submits that, despite the theoretical scenarios under which NSA could acquire communications through its upstream collection as to which the sender and all intended recipients are located in the United States, NSA's targeting procedures are reasonably designed to prevent such acquisitions where the location of the sender and all intended recipients is known at the time of acquisition. ~~(TS//SI//OC,NF)~~

The remainder of this page intentionally left blank.

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

b. According to the May 2 Letter, [REDACTED] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: ~~(TS//SI//NF)~~

iii. is consistent with the Fourth Amendment. ~~(TS//SI//NF)~~

NSA's ACQUISITION OF TRANSACTIONS CONTAINING MULTIPLE DISCRETE COMMUNICATIONS IS CONSISTENT WITH THE FOURTH AMENDMENT.
~~(TS//SI//NF)~~

Section 702 requires the Attorney General (AG) and the Director of National Intelligence (DNI) to execute a certification attesting, among other things, that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(g)(2)(A)(iv). In reviewing a certification, Section 702 in turn requires the Court to enter an order approving the certification and the use of the targeting and minimization procedures if the Court finds, among other things, that those procedures are consistent with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A). 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. *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008) (hereinafter "*In re Directives*"). ~~(TS//SI//NF)~~

The Fourth Amendment protects the right "to be secure . . . against unreasonable searches and seizures" and directs that "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." U.S. Const. amend. IV. As demonstrated below, the Fourth Amendment requires no warrant here, and the upstream collection conducted by NSA is a reasonable exercise of governmental power that satisfies the Fourth Amendment. ~~(TS//SI//NF)~~

A. The Warrant Requirement Does Not Apply to NSA's Acquisition of Transactions Containing Multiple Discrete Communications. ~~(TS//SI//NF)~~

The Supreme Court has recognized exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal quotations omitted); see also *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (quoting *Griffin*). The Foreign Intelligence Surveillance Court of Review, in upholding the Government's implementation of the PAA, held that a foreign intelligence exception exists "when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

believed to be located outside the United States." *In re Directives*, 551 F.3d at 1012. See also *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002) ("[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."). ~~(TS//SI//NF)~~

In approving a previous Section 702 certification, this Court has found that Section 702 acquisitions "fall within the exception recognized by the Court of Review" in that they "target persons reasonably believed to be located outside the United States who will have been assessed by NSA to possess and/or to be likely to communicate foreign intelligence information concerning a foreign power authorized for acquisition under the Certification" and are "conducted for national security purposes." ~~██████████~~ Mem. Op. at 35 (citations omitted). Specifically, this Court recognized that the Court of Review's rationale for applying a foreign intelligence exception "appl[ies] with equal force" to Section 702 acquisitions, in that the Government's purpose in conducting Section 702 acquisitions goes well beyond a normal law enforcement objective and involves "the acquisition from overseas foreign agents of foreign intelligence to help protect national security," a circumstance ~~in which the government's interest is particularly intense.~~ *Id.* at 35-36 (quoting *In re Directives*, 551 F.3d at 1011). In addition, this Court, noting the likely volume of Section 702 acquisitions and the fact that those acquisitions involve targets who are attempting to conceal their communications, found that "[s]ubjecting ~~██████████~~ number of targets to a warrant process inevitably would result in delays and, at least occasionally, in failures to obtain perishable foreign intelligence information, to the detriment of national security." ~~██████████~~ Mem. Op. at 36; see also *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) ("attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy" such that "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, [and] in some cases delay executive response to foreign intelligence threats..."). The Court's previous finding that the foreign intelligence exception applies to Section 702 acquisitions remains equally applicable here. ~~(TS//SI//NF)~~

B. NSA's Acquisition of Transactions Containing Multiple Discrete Communications is Reasonable Under the Fourth Amendment. ~~(TS//SI//NF)~~

Where, as here, the foreign intelligence exception applies, "governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement." *In re Directives*, 551 F.3d at 1012. In evaluating the reasonableness of the Government's action, a court must consider the totality of the circumstances, see *United States v. Knights*, 534 U.S. 112, 118 (2001), taking into account "the nature of the government intrusion and how the intrusion is implemented." *In re Directives*, 551 F.3d at 1012 (citing *Tennessee v. Garner*, 471 U.S. 1, 8 (1985) and *United States v. Place*, 462 U.S. 696, 703 (1983)). In balancing these interests, the Court of Review has observed that "[t]he more important the government's interest, the greater the intrusion that may be constitutionally tolerated." *In re Directives*, 551 F.3d at 1012 (citing *Michigan v. Summers*, 452 U.S. 692, 701-05 (1981)). "If the protections that are in place for individual privacy interests are sufficient in light of the governmental interests at stake, the constitutional scales will tilt in favor of upholding the government's actions." *Id.* ~~(TS//SI//NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

1. NSA's Acquisition of Transactions Containing Multiple Discrete Communications Implicates Fourth Amendment-Protected Interests.

~~(TS//SI//NF)~~

Although targeting under Section 702 is limited to non-United States persons reasonably believed to be located outside the United States, who are not entitled to protection under the Fourth Amendment, *see, e.g.*, ██████████ Mem. Op. at 37, this Court has recognized that conducting acquisitions under Section 702 creates a "real and non-trivial likelihood of intrusion on Fourth Amendment-protected interests" of United States persons or persons located in the United States who, for example, communicate directly with a Section 702 target, *id.* at 38.¹⁴ In particular, as described herein, 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. ~~(TS//SI//NF)~~

2. The Government's Interest in the Foreign Intelligence Information Contained in All Transactions, Including Those Containing Multiple Discrete Communications, is Paramount. ~~(TS//SI//NF)~~

On the other side of the ledger, it is axiomatic that the Government's interest in obtaining foreign intelligence information to protect the Nation's security and conduct its foreign affairs is paramount. *See, e.g., Haig v. Agee*, 453 U.S. 280, 307 (1981) ("[I]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." (citations omitted)). Equally indisputable is the Government's interest in conducting acquisitions of foreign intelligence information¹⁵ under Section 702 of the Act. *See* ██████████ Mem. Op. at 37

¹⁴ Although the scope of Fourth Amendment protection for e-mail is not settled, the Government has argued before this Court that United States persons have a reasonable expectation of privacy in the content of such electronic communications. *See, e.g.,* United States of America's Supplemental Brief on the Fourth Amendment, Docket No. 105B(g) 07-01, filed Feb. 15, 2008, at 1. The Government likewise assumes for purposes of this filing that the collection of ██████████ implicates privacy interests protected by the Fourth Amendment. ~~(TS//SI//NF)~~

¹⁵ "Foreign intelligence information" is defined as:

- (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against --
 - (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
 - (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
 - (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
- (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to --
 - (A) the national defense or the security of the United States; or
 - (B) the conduct of the foreign affairs of the United States.

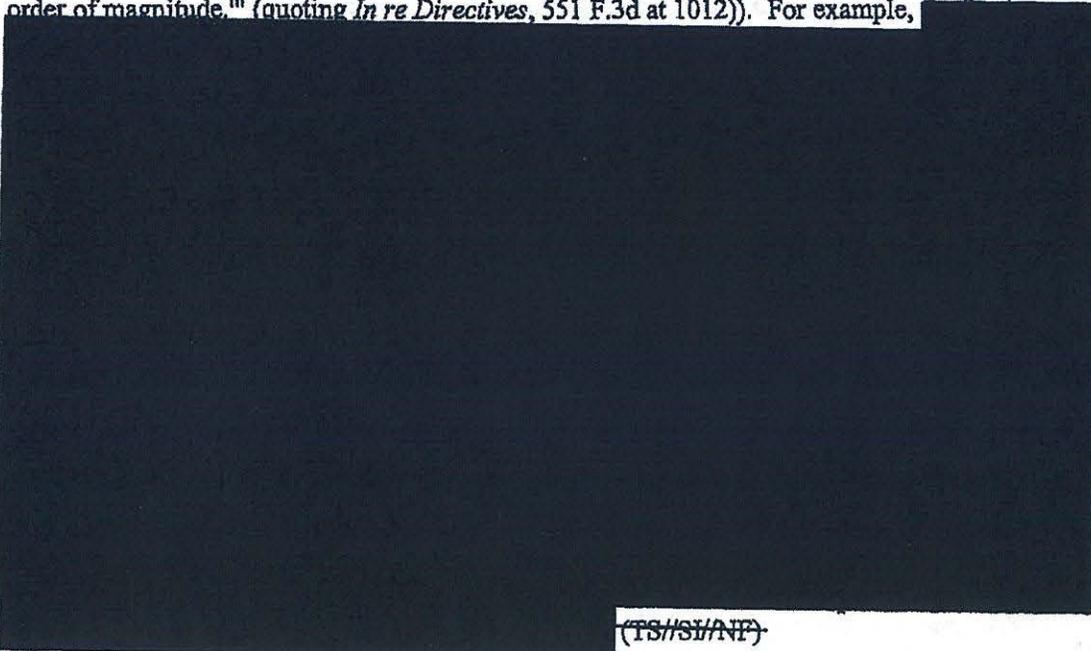
~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

("The government's national security interest in conducting these acquisitions 'is of the highest order of magnitude.'" (quoting *In re Directives*, 551 F.3d at 1012)). For example,



The Supreme Court has indicated that in addition to examining the governmental interest at stake, some consideration of the efficacy of the search being implemented -- that is, some measure of fit between the search and the desired objective -- is also relevant to the reasonableness analysis. See, e.g., *Knights*, 534 U.S. at 119 (noting that the reasonableness of a search "is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which [the search] is needed for the promotion of legitimate governmental interests." (internal quotation marks omitted)); see also *Board of Educ. v. Earls*, 536 U.S. 822, 834 (2002) ("Finally, this Court must consider the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them.")). Here, NSA's acquisition of transactions through upstream collection is an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount governmental interest of protecting the Nation and conducting its foreign affairs.

~~(TS//SI//NF)~~

The AG and DNI have attested that a significant purpose of all acquisitions under Section 702, which includes those conducted by NSA's upstream collection, is to obtain foreign intelligence information. These acquisitions are 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

50 U.S.C. § 1801(e). (U)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

afford a degree of particularity that is reasonable under the Fourth Amendment." [REDACTED] Mem. Op. at 39-40 (footnote omitted). Indeed, certain of the valuable foreign intelligence information NSA seeks to acquire through upstream collection of transactions simply cannot be acquired by any other means. (TS//SI//NF)

Specifically, as this Court has recognized, NSA's upstream collection "is particularly important because it is *uniquely capable* of acquiring certain types of targeted communications containing valuable foreign intelligence information," such as [REDACTED]

[REDACTED]
Such foreign intelligence information is particularly useful, for example, [REDACTED]

¹⁶ In

¹⁶ More specifically, during the course of the Court's consideration of DNI/AG-702(g) Certification [REDACTED] the Government explained the unique value of NSA's [REDACTED]

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

addition, NSA's upstream collection enables NSA to acquire foreign intelligence information from [REDACTED]

[REDACTED] All of these types of communications are intercepted in transactions acquired through NSA's upstream collection. Valuable foreign intelligence information such as this simply cannot be obtained by means other than the acquisition of transactions through NSA's upstream collection. ~~(TS//SI//NF)~~

3. The Acquisition of Foreign Intelligence Information Contained in Transactions is Conducted Using the Least Intrusive Means Available.
~~(TS//SI//NF)~~

The fact that NSA's upstream collection acquires transactions that may contain several discrete communications, only one of which is to, from, or about a tasked selector, does not render NSA's upstream collection unreasonable. *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); *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful [Title III] surveillance is not violative of the Fourth Amendment."); *cf. 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"). Indeed, the Supreme Court has repeatedly rejected suggestions that reasonableness requires "the least intrusive search practicable." *City of Ontario v. Quon*, 130 S. Ct. 2619, 2632 (2010) (quotation marks omitted); *see, e.g., Earls*, 536 U.S. at 837 ("[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 quotation marks omitted)); *Vernonia*, 515 U.S. at 663 ("We have repeatedly refused to declare

[REDACTED]

~~(TS//SI//OC,NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." (TS//SI//NF)

Although not demanded by the Fourth Amendment, NSA is nevertheless conducting "the least intrusive search practicable" when it acquires a single transaction which may contain several discrete communications, only one of which may contain foreign intelligence information because it is to, from, or about a tasked selector.

Accordingly, at the time of acquisition, NSA generally cannot know whether a transaction contains only a single communication to, from, or about a tasked selector, or whether that transaction contains that single communication along with several other communications.¹⁷

also render the information 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 contained within that discrete communication, therefore, is to acquire the entire transaction in which it is contained. 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. 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"). (TS//SI//NF)

At the same time, NSA is making every reasonable effort to ensure that its upstream collection acquires this singularly valuable foreign intelligence information in a manner that minimizes the intrusion into the personal privacy of United States persons to the greatest extent possible. As discussed above, these acquisitions are conducted in accordance with FISC-approved targeting procedures reasonably designed to ensure that the acquisitions are directed only "toward communications that are likely to yield the foreign intelligence information sought." Mem. Op. at 39-40 (footnote omitted). The application of the targeting procedures further ensures that "[t]he targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that United States person information will be obtained." Mem. Op. at 23; cf. *In re Directives*, Docket No. 105B(g):07-01, Mem. Op. at 87 (USFISC April 25, 2008) (recognizing 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") (footnote omitted), *aff'd*, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008). Lastly, to the extent that United States person information is incidentally acquired in the acquisition of a whole transaction by NSA's upstream collection,

¹⁷ See Government's response to questions 2(c) and (d) *infra*. (U)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

such information will be handled in accordance with strict minimization procedures, as discussed in more detail below. ~~(TS//SI//NF)~~

4. United States Person Information Acquired Incidentally Through NSA's Acquisition of Transactions Containing Multiple Discrete Communications is Protected by NSA's Section 702 Minimization Procedures. ~~(TS//SI//NF)~~

As discussed above, the fact that NSA's upstream collection may result in the incidental acquisition of communications of United States persons cannot, by itself, render the overall collection unreasonable. Instead, courts have repeatedly found support for the constitutionality of foreign intelligence activities resulting in the incidental acquisition of United States person information in the existence and application of robust minimization procedures. *See, e.g., In re Directives*, 551 F.3d at 1015 (recognizing that minimization procedures are a "means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons");

~~Mem. Op. at 40 (concluding that minimization procedures meeting the definition in 50 U.S.C. § 1801(h)(1) "constitute a safeguard against improper use of information about United States persons that is inadvertently or incidentally acquired, and therefore contribute to the Court's overall assessment that the targeting and minimization procedures are consistent with the Fourth Amendment").~~ As explained below, NSA's current Section 702 minimization procedures, which this Court previously has found to satisfy the definition of minimization procedures in 50 U.S.C. § 1801(h)(1),¹⁸ adequately protect the privacy interests of United States persons whose communications may be incidentally acquired through NSA's upstream collection and thus contribute significantly to the overall reasonableness of that collection. ~~(TS//SI//NF)~~

At the outset, it is worth noting that NSA's acquisition of Internet transactions containing multiple discrete communications does not necessarily increase the risk that NSA will incidentally acquire United States person information. For example, as discussed above, the ~~means by which NSA ensures it does not intentionally acquire wholly domestic communications limits the acquisition of certain transactions such as~~ to persons located outside the United States, who reasonably can be presumed to be non-United States persons. Thus, to the extent that the ~~of those non-United States persons contain communications that are not to, from, or about a targeted selector, those communications are unlikely to be United States person communications.~~ *See In re Directives*, Docket No. 105B(g):07-01, Mem. Op. at 87 (recognizing 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") (footnote omitted). For this same reason, the risk that United States person information would be obtained through the acquisition of a ~~is no greater than in the acquisition of a~~

¹⁸ 50 U.S.C. § 1801(h)(1) defines "minimization procedures" as "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, 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." (U)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

~~(TS//SI//NF)~~

a. Acquisition (U)

As discussed above, with limited exceptions,¹⁹ it is technologically infeasible for NSA's upstream collection to acquire only the discrete communication to, from, or about a tasked selector that may be contained in a transaction containing multiple discrete communications. That does not mean, however, that the minimization procedures governing NSA's upstream collection do not adequately minimize the acquisition of any United States person information that may be contained in those transactions. Specifically, minimization procedures must be 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." 50 U.S.C. § 1801(h)(1). As discussed above, the *only* way to obtain the foreign intelligence information contained within a discrete communication is to acquire the entire transaction in which it is contained. Thus, to the extent that United States person information may be contained within other discrete communications not to, from, or about the target in that transaction, the acquisition of such United States person information would be "consistent with the need of the United States to obtain . . . foreign intelligence information." ~~(TS//SI//NF)~~

Congress has recognized that "in many cases it may not be possible for technical reasons to avoid acquiring all information" when conducting foreign intelligence surveillance. H.R. Rep. No. 95-1283, pt. 1, at 55 (1978); *see also id.* at 56 ("It may not be possible or reasonable to avoid acquiring all conversations."); *cf. Scott*, 436 U.S. at 140 (recognizing that Title III "does not forbid the interception of all nonrelevant conversations, but rather instructs the agents to conduct the surveillance in such a manner as to 'minimize' the interception of such conversations"). Rather, in situations where, as here, it is technologically infeasible to avoid incidentally acquiring communications that are not to, from, or about the target, "the reasonable design of the [minimization] procedures must emphasize the minimization of retention and dissemination." H.R. Rep. No. 95-1283, pt. 1, at 55. ~~(TS//SI//NF)~~

b. Retention (U)

In addition, for reasons discussed more fully below, nothing in the statutory definition of minimization procedures obligates NSA to immediately destroy any United States person information in a communication that is not to, from, or about a tasked selector within a transaction acquired by NSA's upstream collection. ~~(TS//SI//NF)~~

¹⁹ *See supra* footnote 6. (U)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~**i. Destruction Is Not Technologically Feasible ~~(TS//SI//NF)~~**

First, Congress intended that the obligation to destroy non-pertinent information would attach only if the destruction of such information is 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)). That is because Congress recognized that in some cases, the 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 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."). ~~(TS//SI//NF)~~

A transaction containing several communications, only one of which contains the tasked selector, is to NSA's systems ~~technologically indistinguishable from a transaction containing a single message to, from, or about a tasked selector.~~ That is true both for NSA's collection systems and for the NSA systems that process and then route Section 702-acquired information to NSA's corporate stores. Thus, unlike other instances where it is technologically possible for certain kinds of communications to be recognized, segregated, and prevented from being routed to NSA's corporate stores, the transaction as a whole, including all of the discrete communications that may be included within it, is forwarded to NSA corporate stores, where it is available to NSA analysts. ~~(TS//SI//NF)~~

The transaction is likewise not divisible into the discrete communications within it even once it resides in an NSA corporate store. That is because NSA assesses that it is not technologically feasible to extract, post-acquisition, only the discrete communication that is to, from, or about a tasked selector within a transaction without destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including the single, discrete communication which is to, from or about the tasked selector. Thus, an NSA analyst cannot, for example, simply cut out any pertinent part of the transaction (i.e., the discrete communication that contains the tasked selector), paste it into a new record, and then discard the remainder. In this way, the transactions at issue here are a present-day version of the very same problem that Congress recognized over thirty years earlier -- i.e., that in some cases, "it might not be feasible to cut and paste files . . . where some information is relevant and some is not." H.R. Rep No. 95-1283, pt.1, at 56. Given that Congress recognized it might be necessary to retain all acquired information regardless of its pertinence because destruction of the non-pertinent information may not be feasible, minimization procedures that permit the retention of transactions in their entireties because their further divisibility is infeasible (if not technologically impossible) are consistent with the statutory requirement that such procedures minimize the retention of United States person information. ~~(TS//SI//NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

ii. **Retention of United States Person Information Can Be Effectively Minimized Through Restrictions on its Retrieval** ~~(TS//SI//NF)~~

Second, although it is not required that all non-pertinent United States person information be destroyed, NSA's retention of non-pertinent information concerning innocent United States persons is not without bounds. FISA's legislative history suggests that the retention of such information could still be effectively minimized through means other than destruction. *See* H.R. Rep. No. 95-1283, pt. 1, at 56 ("There are a number of means and techniques which the minimization procedures may require to achieve the purposes set out in the definition."). Of particular relevance here, Congress recognized that minimizing the retention of such information can be accomplished by making the information "not retrievable by the name of the innocent person" through the application of "rigorous and strict controls." *Id.* at 58-59. Those "rigorous and strict controls," however, need only be applied to the retention of United States person information "for purposes other than counterintelligence or counterterrorism." *Id.* That is because Congress intended that "a significant degree of latitude be given in counterintelligence and counterterrorism cases with respect to the retention of information." *Id.* at 59. ~~(TS//SI//NF)~~

NSA's current Section 702 minimization procedures flatly prohibit the use of United States person names or identifiers to retrieve any Section 702-acquired communications in NSA systems. *See, e.g.*, Amendment 1 to DNI/AG 702(g) Certification [REDACTED] Ex. B, filed [REDACTED] 2010, § 3(b)(5) (hereinafter "NSA Section 702 minimization procedures"). This "rigorous and strict control[]" applies even to United States person information that relates to counterintelligence or counterterrorism, despite Congress's stated intent that agencies should have "a significant degree of latitude . . . with respect to the retention of [such] information." H.R. Rep. No. 95-1283, pt. 1, at 59; *see id.* at 58-59 (recognizing that "for an extended period it may be necessary to have information concerning [the] acquaintances [of a hypothetical FISA target] retrievable" for analytic purposes, even though "[a]mong his contacts and acquaintances . . . there are likely to be a large number of innocent persons"). NSA's current Section 702 minimization procedures thus require the retention of information concerning United States persons (innocent or otherwise) to be minimized to a significantly greater degree than is necessary for those procedures to be reasonable. ~~(TS//SI//NF)~~

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. *E.g.*, DNI/AG 702(g) Certification [REDACTED] Ex. B, filed Apr. 20, 2011, § 3(b)(5). Under these revised NSA Section 702 minimization procedures, the use of such selection terms must be approved in accordance with NSA procedures. *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. The Government will ensure that these NSA procedures contain "rigorous and strict controls" on the retrieval of United States person information consistent with statutory requirements and Congressional intent. H.R. Rep. No. 95-1283, pt. 1, at 59. ~~(TS//SI//NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

c. Dissemination (U)

As discussed above, the NSA current Section 702 minimization procedures prohibit the use of United States person identifiers to retrieve any Section 702-acquired communications in NSA systems. Accordingly, the only way incidentally acquired United States person information currently will be reviewed by an NSA analyst is if that information appears in a communication that the analyst has retrieved using a permissible query term -- i.e., one that is reasonably likely to return information about non-United States person foreign intelligence targets. See NSA Section 702 minimization procedures, § 3(b)(5). Any identifiable United States person information contained in a communication retrieved in this manner would be subject to the dissemination restrictions in the NSA Section 702 minimization procedures, which operate to ensure that any dissemination of United States person information is consistent with the Act. These restrictions apply regardless of whether the United States person information is contained in a discrete communication that is to, from, or about a tasked selector. Moreover, the same dissemination restrictions will continue to apply to any United States person information retrieved through the use of a United States person identifier as a selection term in accordance with NSA's revised 702 minimization procedures. Indeed, given the small probability that an incidentally acquired communication of a United States person that is not to, from, or about a tasked selector would contain foreign intelligence information or evidence of a crime, it is highly unlikely that NSA would disseminate any information from that incidentally acquired communication, let alone information concerning the United States person. (TS//SI//NF)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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



20



21



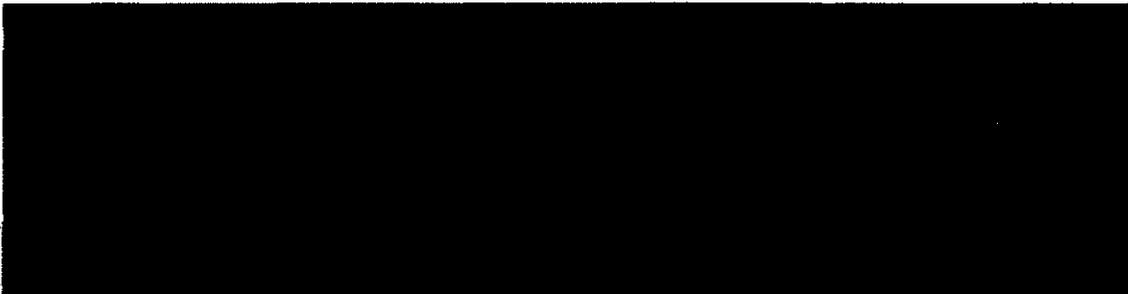
²² See footnote 22 below. (S)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

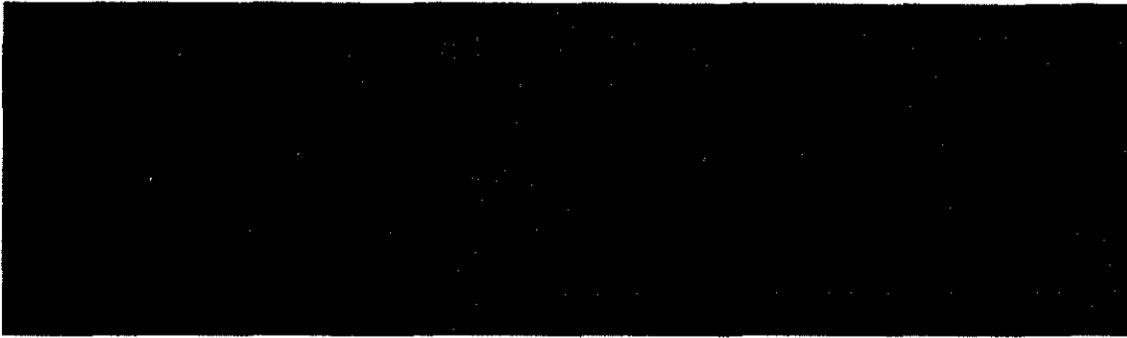


~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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



c. The May 2 Letter states that NSA is not presently capable of "separating out individual pieces of information" contained within [REDACTED] May 2 Letter at 3. Please explain why and state whether it would be feasible for NSA to implement such capability, either at the time of acquisition or thereafter. ~~(TS//SI//NF)~~

d. Can [REDACTED] be identified as distinct from other, discrete communications between users, either at the time of acquisition or thereafter? If so, can NSA filter its Section 702 collection on this basis? ~~(TS//SI//NF)~~



Except as described above, at the time of acquisition, NSA is not presently capable of separating out transactions that contain multiple electronic communications into logical constituent parts without destabilizing -- and potentially rendering unusable -- some or all of the entire collected transaction, including any particular communication therein which is in-fact to, from, or about the tasked selector. Each electronic communication service provider develops protocols that perform the services being provided in a manner designed to be economical in speed, size, and other factors that the provider considers important. [REDACTED]

²⁵ An NSA analyst would, however, 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, such as an analytic store. Even so, the original transaction from which that copy was made would be retained in the corporate store in its original state, which cannot be altered for the reasons discussed below. ~~(TS//SI//NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

Each of the major providers change protocols often to suit their own business purposes, and it is therefore generally not possible for NSA to isolate or separate out individual pieces of information contained within single transactions at the time of NSA acquisition. Any protocol in use today could easily be changed by the provider tomorrow [REDACTED]

[REDACTED]

In short, except in cases involving [REDACTED] described above, at the time of acquisition it is not technologically feasible for NSA to extract any particular communication that is to, from, or about a tasked selector within a transaction containing multiple discrete communications. (TS//SI//NF)

For the same reasons that protocol volatility and myriad user settings prevent the extraction of only discrete communications at the point of acquisition, it is not technologically feasible to extract, post-acquisition, only the specific communication(s) to, from, or about a tasked selector within a transaction without destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including any particular communication therein which is to, from, or about the tasked selector. Thus, an NSA analyst cannot, for example, simply cut out the discrete communication that contains the tasked selector, paste it into a new record, and then discard the remainder. (TS//SI//NF)

3. The May 2 Letter notes that NSA uses Internet Protocol (IP) filtering and [REDACTED] to prevent the intentional acquisition of communications as to which the sender and all known recipients are inside the United States. May 2 Letter at 3. (TS//SI//NF)

a. Please describe how NSA applies IP filtering in the context of [REDACTED] (TS//SI//NF)

i. [REDACTED] (TS//SI//NF)

ii. [REDACTED] (TS//SI//NF)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

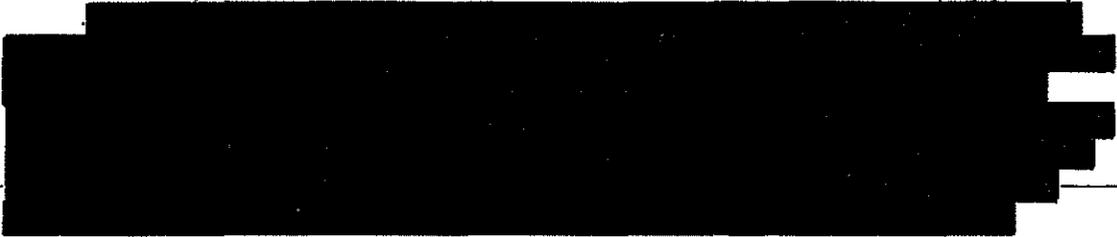
NSA acquires Internet communications by collecting the individual packets of data that make up those communications. As required by NSA's targeting procedures, all Internet communications data packets that may contain abouts information that NSA intercepts through its Section 702 upstream collection must either pass through an "Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas." or



~~(TS//SI//OC,NF)~~



~~(TS//SI//OC,NF)~~



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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

[REDACTED] Accordingly, NSA cannot prevent the acquisition of, or even mark for separate treatment, those types of transactions that may feature multiple discrete communications [REDACTED] (TS//SI//OC,NF)

- b. In the collection of "to/from" communications, are the communicants always the individual users of particular facilities [REDACTED], or does NSA sometimes consider [REDACTED] Please explain. (TS//SI//NF)

In the collection of "to/from" communications, NSA considers the communicants as being the individual users of particular selectors. More particularly, NSA considers those individual users to be the senders and intended recipients of "to/from" communications. Conversely, NSA does not consider [REDACTED] (TS//SI//NF)

- 4. How, in terms of numbers and volume, does NSA's collection of [REDACTED] under Section 702 compare with the collection of discrete Internet communications (such as e-mail messages) between or among individual users? (TS//SI//NF)

As a result of the present technological limitations [REDACTED] NSA cannot precisely measure the number of transactions that might contain information or data representing several discrete communications [REDACTED] for purposes of comparing that figure with transactions containing a single, discrete communication [REDACTED] without manually examining each transaction that NSA has acquired. However, in an attempt to provide an estimate of the volume of such collection at the Court's request, NSA performed a series of queries into the SIGINT Collection Source System of Record that holds the relevant transactions in question. [REDACTED]

Results were sampled manually to confirm collection of [REDACTED] Results were reviewed for three randomly selected days in April, averaged to produce an estimated figure of collection of [REDACTED] for the month of April. This figure was then compared to the total take of Section 702 upstream collection of web activity for the month. From this sample, NSA estimates that approximately 9% of the monthly Section 702 upstream collection of [REDACTED] It is important

²⁶ NSA notes that it is likely that this 9% figure includes [REDACTED] of the user of the targeted selector him/herself. (TS//SI//NF)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

to note that this was a manually intensive and imprecise means to quantify the volume of [REDACTED] collection and should not be interpreted to suggest that any technological method of pre-filtering can be applied to the collection before it is available to the analyst. ~~(TS//SI//NF)~~

5. Given that some of the information acquired through upstream collection is likely to constitute "electronic surveillance" as defined in 50 U.S.C. § 1801(f)(2) that has not been approved by this Court, how does the continued acquisition of, or the further use or dissemination of, such information comport with the restrictions of 50 U.S.C. § 1809(a)(1) and (a)(2)? ~~(TS//SI//NF)~~
- I. THE CONTINUED ACQUISITION, USE, AND DISSEMINATION OF INFORMATION ACQUIRED THROUGH UPSTREAM COLLECTION DOES NOT VIOLATE 50 U.S.C. § 1809. ~~(TS//SI//NF)~~

A. Introduction (U)

Section 702 of FISA, as codified at 50 U.S.C. § 1881a, provides that "[n]otwithstanding any other provision of law," upon the issuance of an appropriate Order from the Court, the Attorney General (AG) and the Director of National Intelligence (DNI) may jointly authorize the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information as long as certain conditions set out in subsection 702(b) are met. The joint authorizations of the AG and the DNI authorized NSA's upstream acquisition of communications that are to, from, or about a tasked selector. The Court, in turn, approved the implementing certifications as well as the use of proffered targeting and minimization procedures. Accordingly, because the acquisition of communications to, from, or about a tasked selector was authorized by the AG and DNI, and the Court approved the certifications and procedures used to implement those authorizations, NSA's acquisition of such communications upstream does not constitute unauthorized electronic surveillance and, therefore, does not violate the terms of 50 U.S.C. § 1809. ~~(TS//SI//NF)~~

As noted above, the Government readily acknowledges that it did not fully describe to the Court that the upstream collection technique would result in NSA acquiring [REDACTED] types of Internet transactions that could include multiple individual, discrete communications [REDACTED]. As discussed below, however, this omission does not invalidate the AG and DNI's prior authorizations. Nor does it mean that the incidental acquisition of communications that are not to, from, or about a tasked selector as a consequence of obtaining communications that are to or from a tasked selector or contain reference to a tasked selector, exceeds the scope of those authorizations. For the same reasons, the Government respectfully suggests that the Orders of

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

this Court upon which those authorizations rely likewise remain valid. Thus, Section 1809 is not implicated by NSA's upstream collection activities under Section 702. ~~(TS//SI//NF)~~

B. Statutory Framework (U)

i. Section 1809 (U)

Under Subsection 1809(a), a person is guilty of a criminal offense if he or she "intentionally (1) engages in electronic surveillance under color of law, except as authorized by this Act . . . ; or (2) disclose[s] or uses 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 this Act."²⁷ (U)

For purposes of Section 1809 the issue is whether the Government's prior failure to fully explain to the Court the steps NSA must take in order acquire communications to, from, or about a tasked selector, and certain technical limitations regarding the IP address filtering it applies, means that the acquisition of such communications was not authorized by the DNI and AG, and inconsistent with Court approval of the targeting and minimization procedures. ~~(TS//SI//NF)~~

ii. Section 702 Collection Authorizations ~~(S)~~

Pursuant to 50 U.S.C. § 1881a(a), "notwithstanding any other provision of law," the AG and the DNI may jointly authorize for a period of up to one year the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, subject to targeting and minimization procedures approved by this Court, and certain limitations set out in § 1881a(b). Authorizations are premised on certifications to the Court, in which the AG and DNI attest to the fact that, among other things, the targeting and minimization procedures comply with certain statutory requirements and the Fourth

²⁷ This Court has previously noted that the legislative history of this provision focuses on a predecessor bill that was substantially different from the provision subsequently enacted and codified. See [REDACTED] Mem. Op. at 6-7 (Dec. 10, 2010). Yet, both the predecessor bill and the codified provision use the word intentionally, which has been described as "carefully chosen" and intended to limit criminal culpability to those who act with a "conscious objective or desire" to commit a violation. See H.R. Rep. No. 95-1283, pt.1, at 97 (1978) ("The word 'intentionally' was carefully chosen. It is intended to reflect the most strict standard for criminal culpability. . . . The Government would have to prove beyond a reasonable doubt both that the conduct engaged in was in fact a violation, and that it was engaged in with a conscious objective or desire to commit a violation."). Based upon discussions between responsible NSA officials and the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) and DOJ and ODNI's review of documents related to this matter, DOJ and ONDNI have not found any indication that there was a conscious objective or desire to violate the authorizations here. ~~(TS//SI//NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

Amendment. 50 U.S.C. § 1881a(g)(2). Authorizations become effective “upon the issuance of an order [of this Court]” approving the certification and the use of the targeting and minimization procedures as consistent with the statute and the Fourth Amendment. *Id.* §§ 1881a(a) (AG and DNI authorizations go into effect upon “issuance of an order”); 1881a(i)(2)-(3) (laying out scope of FISC review).²⁸ ~~(TS//SI//NF)~~

Thus, if an acquisition is authorized by the AG and DNI, and the certification and targeting and minimization procedures which implement that authorization are approved by the Court, and the authorization remains valid, then the acquisition does not constitute unauthorized electronic surveillance under 50 U.S.C. § 1801(f)(2) and is not a violation of 50 U.S.C. § 1809. ~~(TS//SI//NF)~~

C. At a Minimum, the Upstream Acquisition of Single, Discrete Communications To, From, or About a Tasked Selector Was Authorized by the AG and the DNI

~~(TS//SI//NF)~~

The relevant AG and DNI authorizations and the targeting procedures the AG approved explicitly permit the acquisition of Internet communications that are to, from, or about a tasked selector. *See, e.g.*, NSA Targeting Procedures at 1 (describing the safeguards used in the acquisition of “about” as compared with “to/from” communications). In addition, the accompanying Affidavits of the Director of NSA described upstream collection in a paragraph detailing the various methods of obtaining such acquisitions. *See, e.g.*, DNI/AG 702(g) Certification [REDACTED] Affidavit of General Keith B. Alexander, Director, NSA, filed July 16, 2010, ¶ 4. Thus, it is clear that the authorizations permit – at a minimum – the upstream acquisition of single, discrete communications to, from, or about a tasked selector. ~~(TS//SI//NF)~~

As described in detail in response to questions 2 and 3 above, due to certain technological limitations, in general the only way NSA can currently acquire as part of its upstream collection single, discrete communications to, from, or about a tasked selector [REDACTED] is by obtaining the Internet transactions of which those communications are a part. An Internet transaction can include either a single, discrete communication to, from, or about a tasked

²⁸ For reauthorizations, the AG and the DNI submit, to the extent possible, a certification to the FISC laying out, among other things, the targeting and minimization procedures adopted at least 30 days prior to the expiration of the prior authorization. The prior authorization remains in effect, notwithstanding the otherwise applicable expiration date, pending the FISC's issuance of an order with respect to the certification for reauthorization. 50 U.S.C. § 1881a(i)(5). The scope of the court's review is the same for reauthorizations as it is for initial authorizations. *Id.* § 1881a(i)(5)(B). (U)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

selector [REDACTED], or several discrete communications, only one of which may be to, from, or about a tasked selector [REDACTED] ~~(TS//SI//NF)~~

Where an Internet transaction includes multiple communications, not all of which are to, from, or about a tasked selector, it currently may not be technologically feasible for NSA to separate out, at the time of acquisition or thereafter, the discrete electronic communications within that transaction that are to, from, or about a tasked selector. Indeed, at the time of acquisition, NSA's upstream Internet collection devices are, with limited exception, not capable of distinguishing or further separating discrete electronic communications [REDACTED] within a single Internet transaction. Thus, in some cases, NSA can collect communications to, from, or about a tasked selector, as authorized by the certification, only by obtaining the Internet transaction of which those communications may be just a part.

~~(TS//SI//NF)~~

In this respect, the upstream acquisition of Internet transactions which contain multiple, discrete communications not all of which are (and, in some instances, only one of which is) to, from or about a tasked selector is akin to the Government's seizure of a book or intact file that contains a single page or document that a search warrant authorizes the government to seize. In *United States v. Wuagneux*, 683 F.2d 1343, for example, the Eleventh Circuit rejected appellants' argument that a search was unreasonable because the agents seized an entire file, book, or binder if they identified a single document within the file, book, or binder as being within the authorization of the warrant. As the court explained, "a search may be as extensive as reasonably required to locate items described in the warrant." *Id.* at 1352. It was therefore "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." *Id.* at 1353. *See also 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); *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"). ~~(TS//SI//NF)~~

That the certifications by the AG and DNI did not specifically describe this aspect of NSA's upstream collection does not mean that collection was unauthorized by the AG and DNI. Again, case law involving the reasonableness of searches conducted pursuant to criminal search warrants is instructive on this point. For example, in *Dalia v. United States*, 441 U.S. 238, 259 (1979), the Supreme Court recognized that "[o]ften in executing a warrant the police may find it

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant." *Id.* at 257. 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.") (quoting *Dalia*, 441 U.S. 238, 257 (1979)). This is especially true where, as in *Dalia*, "[t]here is no indication that [the] intrusion went beyond what was necessary" to effectuate the search authorized. *Dalia*, 441 U.S. at 258 n. 20. ~~(TS//SI//NF)~~

Like the seizure of an entire book or file simply because it contained a single page or document within the scope of the warrant, NSA only acquires an Internet transaction containing several discrete communications if at least one of those communications within the transaction is to, from, or about a tasked selector. Moreover, unlike the agents in *Wuagneux*, who presumably could have opted to seize only the responsive pages out of the books and files searched, except in limited circumstances, NSA has no choice but to acquire the whole Internet transaction in order to acquire the to, from, or about communication the DNI and AG authorized NSA to collect. NSA only acquires an Internet transaction if *in fact* it contains at least one communication to, from, or about a tasked selector. NSA's acquisition of Internet transactions containing several discrete communications, only one of which is to, from, or about a tasked selector, is therefore "as extensive as reasonably required to locate the items described" in the DNI and AG's authorization, and thus cannot be said to exceed the scope of that authorization. ~~(TS//SI//NF)~~

Moreover, as described in response to questions 1(b)(ii) and (iii), the Government has concluded that such collection fully complies with the statutory requirements and the Fourth Amendment. Having now considered the additional information that is being presented to this Court, the AG and DNI have confirmed that their prior authorizations remain valid. Accordingly, Government personnel who rely on those authorizations to engage in ongoing acquisition are not engaging in unauthorized electronic surveillance, much less doing so "intentionally." ~~(TS//SI//NF)~~

D. The Court Approved the Certifications and Targeting and Minimization Procedures Used to Implement the Authorizations of the AG and DNI ~~(TS//SI//NF)~~

A second issue concerns whether this Court's orders cover the full scope of the authorizations, and, if not, whether that affects the validity of the AG and DNI authorizations. Like the AG and DNI authorizations, in approving the applicable certifications and the use of the proffered targeting and minimization procedures this Court's Opinions and Orders clearly contemplated and approved some upstream collection of communications to, from, or about a target. See, e.g., [REDACTED] Mem. Op. at 15-17 (describing acquisition of communications to, from,

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

and about a target).²⁹ Thus, for the reasons described above, the acquisition of Internet transactions that include at least one communication to, from, or about a target falls within the scope of the Court's Orders – even if additional communications are also incidentally acquired due to limits in technology. ~~(TS//SI//NF)~~

The fact that the Government did not fully explain to the Court all of the means by which such communications are acquired through NSA's upstream collection techniques does not mean that such acquisitions are beyond the scope of the Court's approval, just as in the criminal context a search does not exceed the scope of a warrant because the Government did not explain to the issuing court all of the possible means of execution, even when they are known beforehand and could possibly implicate privacy rights. See *Dalia*, 441 U.S. at 257 n.19 (noting that "[n]othing in the decisions of this Court . . . indicates that officers requesting a warrant should be constitutionally required to set forth the anticipated means for execution even in those cases where they know beforehand that [an additional intrusion such as] unannounced or forced entry likely will be necessary."). In addition, as discussed herein, the incidental acquisitions do not go beyond what is reasonably necessary to acquire the foreign intelligence information contained in a communication to, from, or about a targeted selector within a transaction. See *id.* at 258 n. 20. ~~(TS//SI//NF)~~

In any event, the Government believes that the additional information should not alter the Court's ultimate conclusion that the targeting and minimization procedures previously approved are consistent with the statutory requirements, including all the requirements of § 1881a(b), and the Fourth Amendment, and the Court's orders therefore remain valid. Cf. *Franks v. Delaware*, 438 U.S. 154 (1978) (establishing that a search warrant is valid unless it was obtained as the result of a knowing and intentional false statement or reckless disregard for the truth and the remaining content is insufficient to establish the requisite probable cause needed to obtain the warrant). ~~(TS//SI//NF)~~

Pursuant to § 1881a, the Court reviews the following issues: (i) whether the AG and DNI certifications contain all the required elements; (ii) whether the targeting procedures are consistent with the requirements of § 1881a(d)(1); (iii) whether the minimization procedures are consistent with § 1881a(i)(e)(1); and (iv) whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(2), (3). See also *id.* § 1881a(i)(5)(B) (specifying that reauthorizations are to be reviewed under the same

²⁹ Each of the relevant 2010 FISC Orders is based on the "reasons stated in the Memorandum Opinion issued contemporaneously herewith." These Opinions, in turn, rely on the analysis conducted by the Court in Dockets [REDACTED], which incorporate and rely on the analysis of earlier FISC Opinions, including Docket 702(i)-08-01. ~~(TS//SI//NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

standards). The Government believes that the Court's ultimate conclusions with respect to each of these issues should not change based on the additional information provided. ~~(TS//SI//NF)~~

First, there is no suggestion that the prior certifications failed to contain all the required elements. ~~(TS//SI//NF)~~

Second, while the Government acknowledges that it did not fully explain to the Court the steps NSA must take in order to implement its Section 702 upstream Internet collection techniques, and certain technical limitations regarding its IP address filtering, the Court did approve the DNI/AG certifications and the use of targeting and minimization procedures which authorized the acquisition of communications to, from, or about tasked selectors. As discussed above and in response to questions 1(b)(ii) (iii) and 3, Internet transactions are collected because they contain at least one discrete communication to, from, or about a tasked selector. Each tasked selector has undergone review, prior to tasking, designed to ensure that the user is a non-United States person reasonably believe to be located outside the United States. Moreover, with respect to "abouts" communications, for the reasons discussed in the response to question 1(b)(ii), NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of any communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.³⁰ Thus, NSA is targeting persons reasonably believed to be outside the United States and is not intentionally acquiring communications in which both the sender and all intended recipients are known at the time of acquisition to be in the United States. ~~(TS//SI//NF)~~

Third, as described throughout, in many cases, it is not technologically feasible for NSA to acquire only Internet transactions that contain a single, discrete communication to, from, or about a tasked selector that may be contained in an Internet communication containing multiple discrete [REDACTED] communications. As discussed in detail in response to questions 1(b)(ii) and (iii), this does not mean that NSA's procedures do not adequately minimize the acquisition of any U.S. person information that may be contained within those transmissions. Rather, the minimization procedures fully comport with all statutory requirements. ~~(TS//SI//NF)~~

³⁰ As the Court is aware, § 1881a(b)(4) provides that an acquisition authorized under section 702, "may not intentionally acquire 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 . . ." Although this prohibition could be read at first glance to be absolute, another provision of Section 702 indicates otherwise. Specifically, § 1881a(d)(1)(B) provides that the targeting procedures that the AG, in consultation with the DNI, must adopt in connection with an acquisition authorized under section 702 need only 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." (U)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

Finally, as described in response to question 1(b)(iii), the targeting and minimization procedures fully comply with the Fourth Amendment. ~~(TS//SI//NF)~~

Thus, the additional information the Government has provided concerning details of its upstream collection does not – in the Government’s view – undercut the validity of the targeting or minimization procedures. ~~(TS//SI//NF)~~

E. Compliance with the Authorizations: Use and Disclosure ~~(TS//SI//NF)~~

As described above, § 1809(a)(2) criminalizes the intentional use and disclosure of electronic surveillance, “knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act.” Having concluded that the upstream collection conducted by NSA falls within the scope of the relevant authorizations, the Government respectfully submits that the continued use and disclosure of such information is likewise valid, so long as the minimization procedures approved by the Court (and discussed in detail in response to questions 1(b)(ii) and (iii)) are followed.³¹ ~~(TS//SI//NF)~~

6. Please provide an update regarding the [REDACTED] over collection incidents described in the government’s letter to the Court dated April 19, 2011.

The April 19, 2011, notice to the Court described two overcollection incidents involving entirely unrelated communications that had been [REDACTED]. The notice also advised that as part of its continued investigation into these incidents, NSA would examine other systems to determine whether similar [REDACTED] issues occurred in those systems. ~~(TS//SI//NF)~~

The first incident described in the April 19 notice involved [REDACTED]. Each [REDACTED] contained at least one communication to, from, or about a Section 702-tasked selector, but also [REDACTED] unrelated communications. This overcollection started [REDACTED].

³¹ Although this analysis has focused on acquisitions conducted pursuant to the 2010 Section 1881a Authorizations, the Government believes that, for all of the reasons discussed herein, the upstream collection conducted pursuant to previous certifications authorized under Section 1881a of the Foreign Intelligence Surveillance Act of 1978, as amended, the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 5, 2007), [REDACTED]

[REDACTED] falls within the scope of the relevant authorizations and Orders of this Court.

~~(TS//SI//NF)~~

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

[REDACTED] (TS//SI//NF)

[REDACTED]

All such communications will be processed in accordance with NSA's minimization procedures.³² The Government will advise the Court of the final disposition of these communications.

[REDACTED] (TS//SI//NF)

The second-described [REDACTED] incident involved overcollection [REDACTED]. As described in the April 19 notice, on March 28, 2011, NSA discovered a [REDACTED] of Section 702-acquired communications that had not been properly [REDACTED]

In contrast to the communications overcollected between [REDACTED] discussed above, the [REDACTED] acquired as a result of the [REDACTED] overcollection incident involved fewer communications [REDACTED]

³² In particular, section 3(b)(1) of NSA's Section 702 Minimization Procedures state:

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 in the processing cycle 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. Such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications.

(Emphasis added). (S//SI)

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

As in the [REDACTED] incident, each [REDACTED] contains at least one communication that is to, from, or about a Section 702-task selector. ~~(TS//SI//NF)~~

As of April 11, 2011, NSA began to sequester in its Collection Stores all communications involving the affected [REDACTED]

[REDACTED]. NSA was deliberately overinclusive in adding objects to the [REDACTED]; while some of these objects include [REDACTED] other objects consist of only one communication to, from, or about a Section 702-task selector.

~~(TS//SI//NF)~~

Since the filing of the April 19 notice, NSA has continued to evaluate collection from [REDACTED] and has observed no evidence of [REDACTED] issues other than the above-described issues [REDACTED]

~~(TS//SI//NF)~~

NSA has identified no reporting based upon overcollected communications and is currently exploring options to automate ways to accelerate identification of [REDACTED]

[REDACTED] NSA anticipates that it will be able to reach a decision by June 30, 2011, on whether this approach is effective. ~~(TS//SI//NF)~~

~~(TS//SI//NF)~~

The April 19 notice also advised the Court that NSA would "examine [REDACTED] and other upstream collection systems to ensure that similar [REDACTED] problems are not occurring in those systems." NSA now reports that unlike the most recent [REDACTED]

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

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

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

these other systems were designed

33

[REDACTED]
[REDACTED]
(S//SI//NF)

7. Are there any other issues of additional information that should be brought to the Court's attention while it is considering the certifications and amendments filed in the above-captioned dockets?

At this time, the Department of Justice (DOJ) and Office of the Director of National Intelligence (ODNI) are currently investigating certain possible incidents of non-compliance about which the Department of Justice intends to file preliminary notices in accordance with the rule of this Court. These incidents do not relate to any of the matters discussed in this filing and, based on the information currently available to DOJ and ODNI, the Government does not believe that the nature of these incidents is sufficiently serious such that they would bear on the Court's consideration of the certifications and amendments filed in the above-captioned dockets.

(S//OC,NF)

³³ As discussed in response to question 2(c) and (d), NSA has the ability to separate out individual pieces of information in certain cases [REDACTED]. In the course of the investigation into the most recent [REDACTED] incident, NSA additionally identified [REDACTED]

[REDACTED] Though testing demonstrated the possibility that incompletely processed communications could have been forwarded through the SIGINT system, NSA has identified no actual overcollection that occurred as a result. NSA is currently in the process of developing a software fix designed to properly process such communications under the limited circumstances in which overcollections could occur. Until such a fix can be tested and deployed, NSA will continue to monitor [REDACTED] and other upstream Section 702 collection systems [REDACTED]

(S//SI//NF)

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

Exhibit 26

~~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]

[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).

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

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

- 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] [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.

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

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

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?

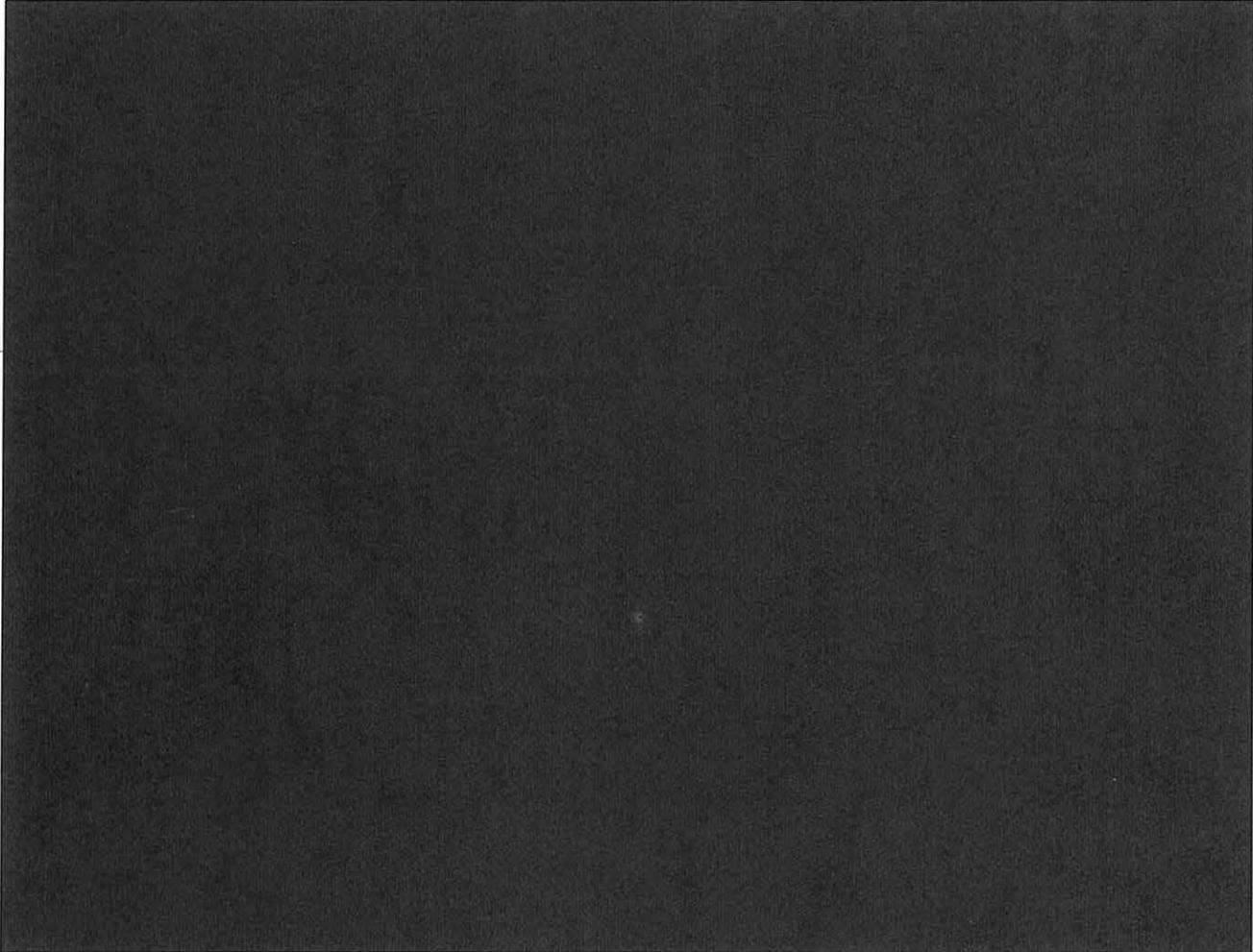
16. The government acknowledges that it previously “did not fully explain all of the means by which . . . communications are acquired through NSA’s upstream collection techniques” (June 1 Submission at 2), yet states that the “[Attorney General] and [Director of National Intelligence] have confirmed 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?

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

~~SECRET//ORCON,NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

JUN 28 PM 4:51
LEAST FIVE HALL
COURT



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

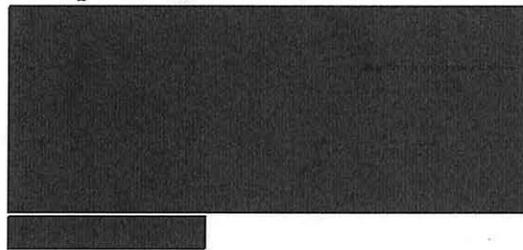
~~SECRET//ORCON,NOFORN~~

Classified by: ~~Tashina Gauhar, Deputy Assistant
Attorney General, NSD, DOJ~~
Reason: ~~1.4(c)~~
Declassify on: ~~28 June 2036~~

~~SECRET//ORCON,NOFORN~~

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,



National Security Division
United States Department of Justice

~~SECRET//ORCON,NOFORN~~

~~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)



Signals Intelligence Directorate Compliance Architect
National Security Agency

~~SECRET//ORCON,NOFORN~~

~~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]

[REDACTED] June 1 Submission at 25.

a. Please provide some examples of the [REDACTED] instance, could such acquisitions include [REDACTED]

FOI

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]

[REDACTED] s. 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, [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

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

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)~~

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

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

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] 1
~~(TS//SI//NF)~~

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

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

DNI/AG 702(g) Certification [REDACTED] Ex. B, filed Aug. 12, 2010, § 3(b)(5) (hereinafter "Current NSA Minimization Procedures"). ~~(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)~~

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

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

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* ██████████ 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)~~

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

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

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 ██████████ 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)~~

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

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

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)~~

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

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

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)~~

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

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

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] [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] [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]

[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

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

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

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]

[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)~~

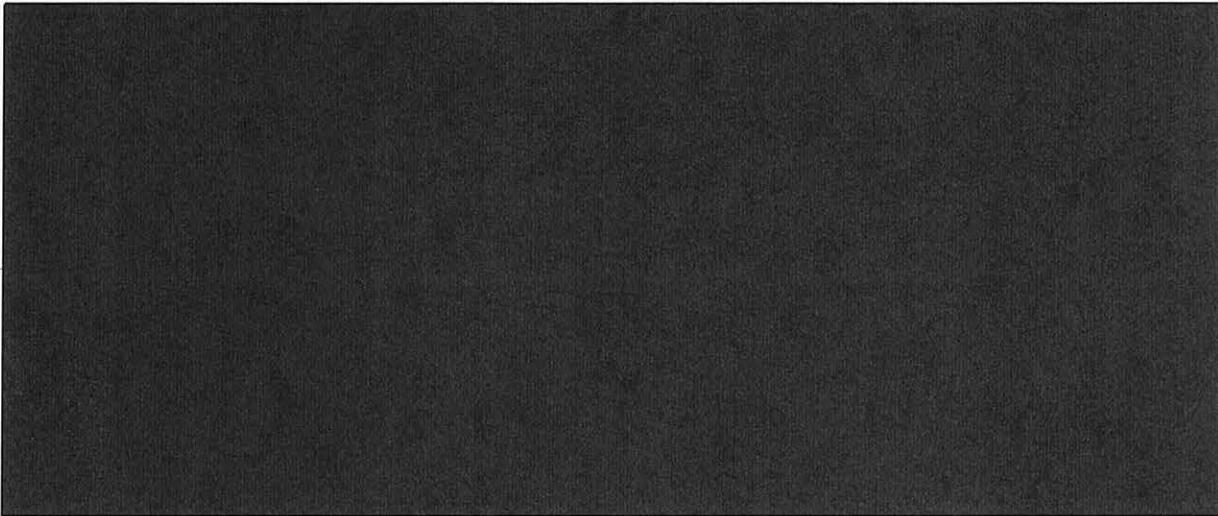
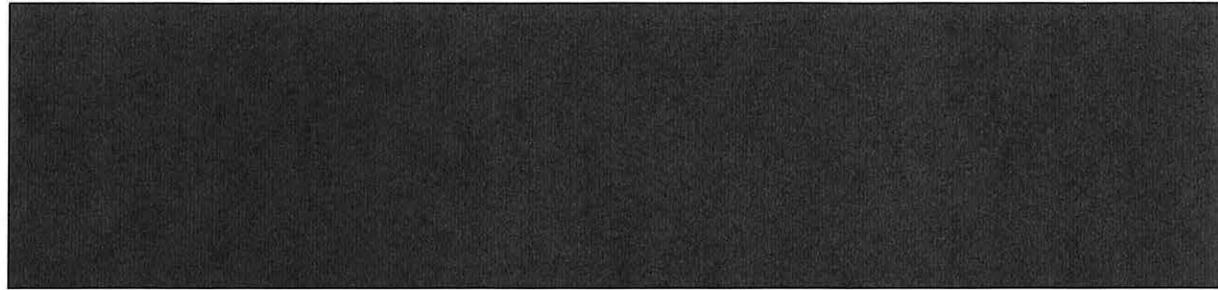
9. What is the factual basis for NSA's suggestion that [REDACTED] [REDACTED] ? See June 1 Submission at 8 n.9.

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)~~

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

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



10. The government repeatedly characterizes as “unintentional” NSA’s collection of discrete non-target communications as part of transactional acquisitions, [REDACTED] [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)

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

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

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)~~

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

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

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. ██████████ 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-Urquidez*, 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 ██████████
██████████
██████████
~~(TS//SI//OC/NF)~~

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

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

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." ██████████ 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,

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

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

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; see 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)~~

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

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

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] [redacted] Mem. Op. at 20 & n.17. As discussed in the June 1 Submission, apart from one exception involving [redacted] [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] [redacted] in particular?

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

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

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]

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

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

[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)

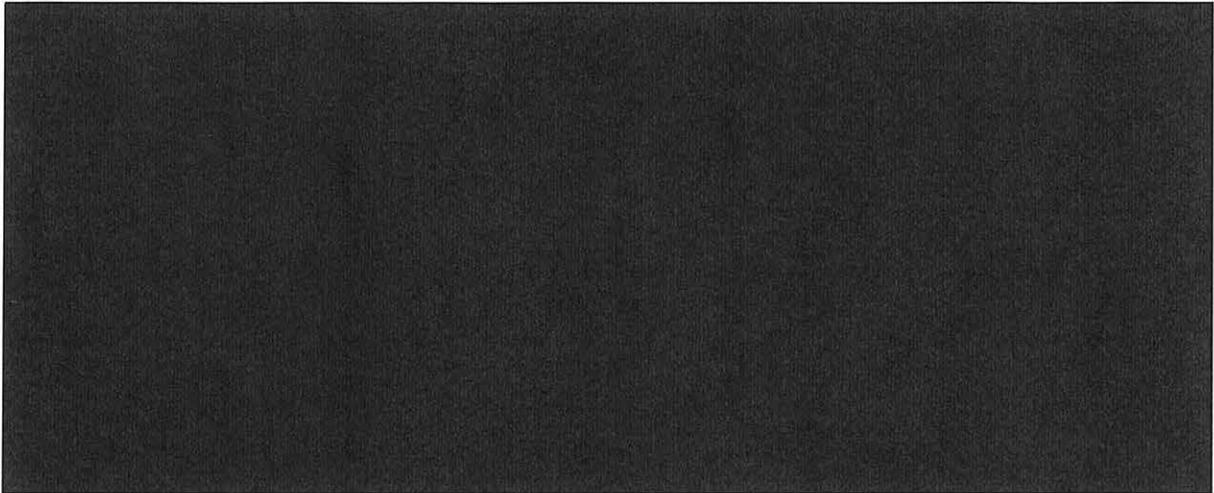
Additionally, NSA's Section 702 upstream collection would not acquire many of the above categories of communications, and thus the foreign intelligence contained within these communications, if NSA's upstream collection were limited to acquisition solely of discrete communications to, from, or about tasked selectors that are [REDACTED] referenced in footnote 2 on page 2 of the June 1 Submission. Currently,

[REDACTED] (TS//SI//NF)

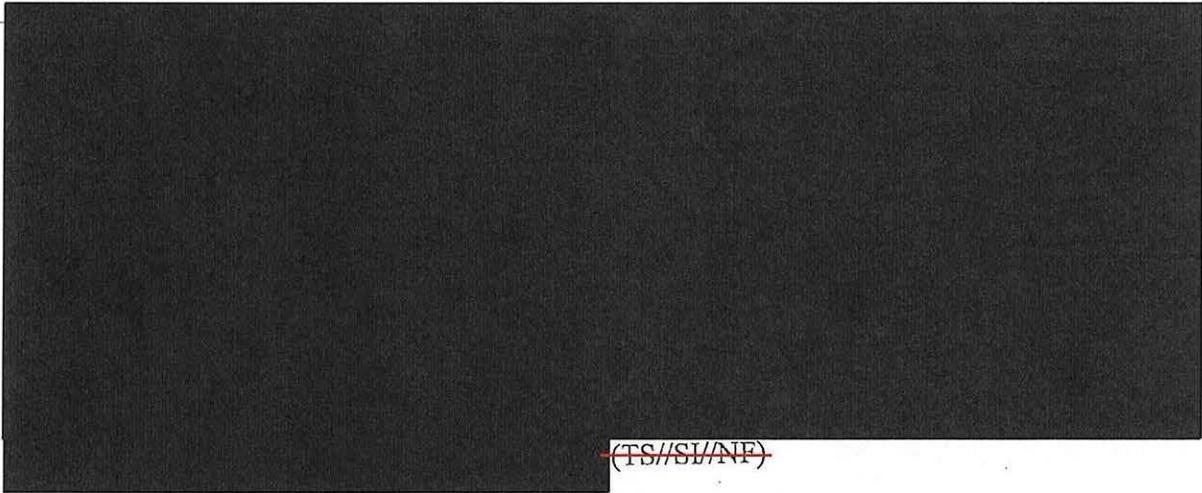
15 [REDACTED] (TS//SI//NF)

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

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

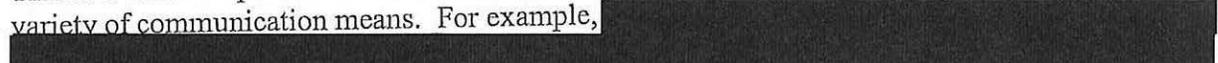
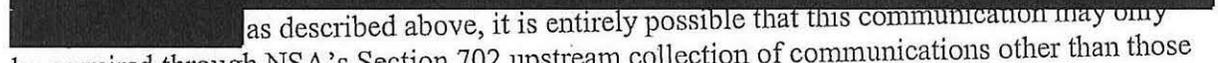
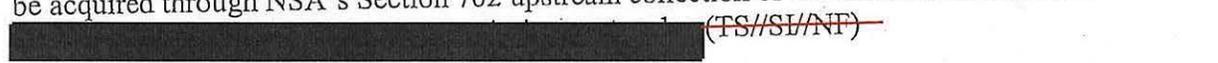


~~(TS//SI//NF)~~



~~(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,


 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


~~(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



~~(TS//SI//NF)~~

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

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

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]

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

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

[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)~~

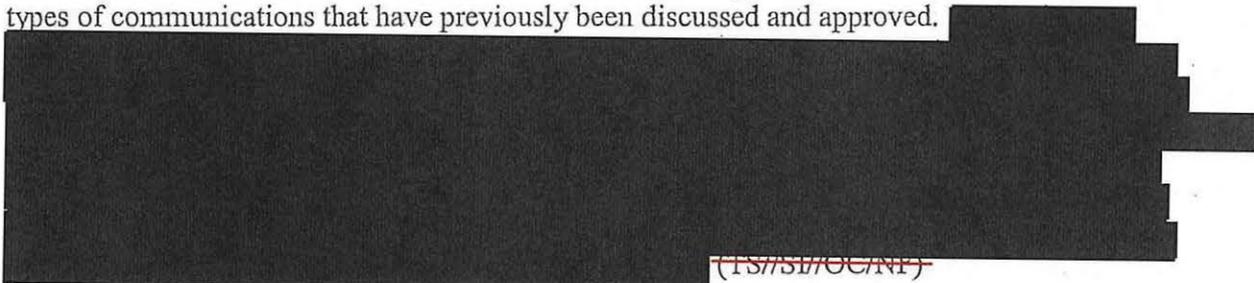
~~TOP SECRET//COMINT//ORCON//NOFORN~~

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

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.



~~(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,

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

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

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 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). 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)~~

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

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

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

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

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

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

~~(TS//SI//OC/NF)~~

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

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

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)~~

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

Exhibit 27

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

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.



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

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

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

[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.”

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

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

I. BACKGROUND

A. The Certifications and Amendments

The April 2011 Submissions include DNI/AG 702(g) Certification [REDACTED]

[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]

[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].

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

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

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

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

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

revised NSA and CIA minimization procedures that have been submitted for use in connection with Certifications [REDACTED]

[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]

[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]. [REDACTED]

⁴ The concept of “Internet transactions” is discussed more fully below. See infra, pages 27-41 and note 23.

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

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

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).

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

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

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

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

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

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(j)(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.

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

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

government's acquisition of foreign intelligence information under Certifications [REDACTED]

[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

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

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

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]

[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]

[REDACTED] Accordingly, the Court extended the deadline to October 10, 2011. [REDACTED]

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

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

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 procedures⁷ 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]

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

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

with 50 U.S.C. § 1881a(g)(2)(D), see Certification [REDACTED]

The Court therefore finds that Certification [REDACTED]

[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]

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

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

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]

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

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

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).

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

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

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"

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

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

communications falling within [REDACTED] specific categories that had been first described to the Court in prior proceedings. [REDACTED]

[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...)

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

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

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...)

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

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

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].

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

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

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]

[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.

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

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

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]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

The new language proposed by the government would allow the FBI to [REDACTED]

[REDACTED]

[REDACTED] The government has advised the Court that this change was prompted by the fact that [REDACTED]

[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]

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

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

[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]

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

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

[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]. [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

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

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

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.

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

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

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

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

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

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]

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

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

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)

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

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

(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

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

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

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.

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

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

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] [REDACTED] [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.

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

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

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.

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

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

[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]

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

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

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



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

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

First, the Court previously understood that NSA's technical measures²⁹ 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]

[REDACTED]

[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 collection³⁰ 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.

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

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

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...)

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

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

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.

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

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

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).”

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

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

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.

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

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

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.

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

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

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...)

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

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

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]

[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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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).

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

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

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]

[REDACTED]

[REDACTED]

[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]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

⁴⁴ See *supra*, note 33.

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

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

[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

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

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

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

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

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

“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.

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

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

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.

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

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

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...)

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

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

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.”

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

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

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.

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

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

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.").

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

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

- 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...)

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

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

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)

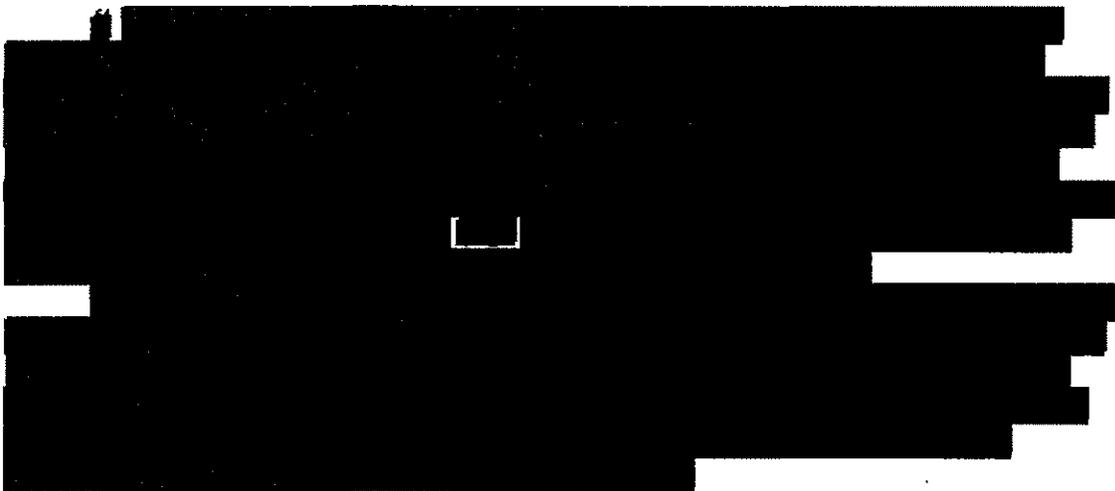
of thousands of wholly domestic SCTs that contain references to targeted selectors. See supra, pages 33-34 & note 33 (discussing the limits [REDACTED])

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.

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

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

accepts the government's assertion that the collection of MCT's 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 MCT's 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.

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

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

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

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

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

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.

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

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

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

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

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

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.

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

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

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]

[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.

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

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

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...)"

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

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

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).

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

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

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.

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

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

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.

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

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

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] [REDACTED] conducted for the purpose of national security – a

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

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

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.

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

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

tolerated.” In re Directives at 19-20 (citations omitted), quoted in Docket No. [REDACTED]

[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.

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

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

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

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

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

“are not protected by the Fourth Amendment.” Docket No. [REDACTED]

[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.

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

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

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,

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

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

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.

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

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

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

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

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

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).

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

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

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

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

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

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

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

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

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.

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

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

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.

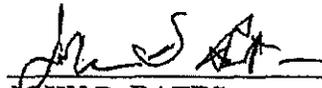
⁶⁹ See Docket No. [REDACTED].

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

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

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

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

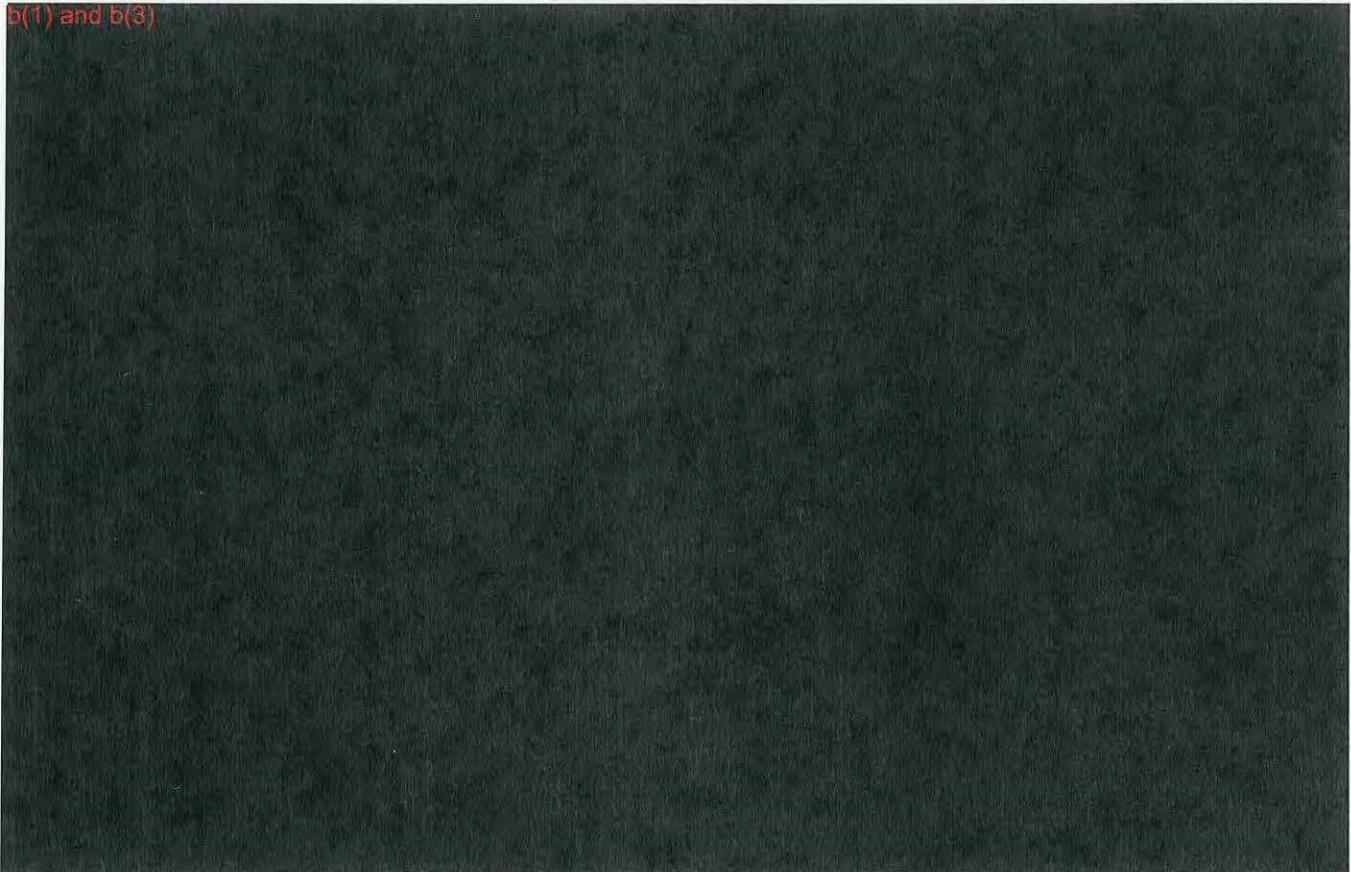
██████████, Deputy Clerk,
FISC, certify that this document
is a true and correct copy of
the original. ██████████

Exhibit 28

~~TOP SECRET//SI//ORCON,NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

b(1) and b(3)



MEMORANDUM OPINION

This matter is before the Foreign Intelligence Surveillance Court (“FISC” or “Court”) on 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,” which was filed on August 24, 2012

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

(“August 24 Submission”). Through the August 24 Submission, 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 request for approval is granted.

I. BACKGROUND

The August 24 Submission includes (b)(1) and (b)(3)

(b)(1) and (b)(3)

(b)(1) and (b)(3) all of which were executed by the Attorney General and the Acting Director of National Intelligence (“DNI”) pursuant to Section 702. Each of the (b)(1) and (b)(3) certifications is accompanied by the supporting affidavits of the 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 four sets of minimization procedures, for use by NSA, FBI, CIA, and the National Counterterrorism Center (“NCTC”), respectively.

Like the acquisitions approved by the Court in all prior Section 702 dockets, collection under Certifications (b)(1) and (b)(3) is limited to “the targeting of non-United States persons reasonably believed to be located outside the United States.”

(b)(1) and (b)(3)

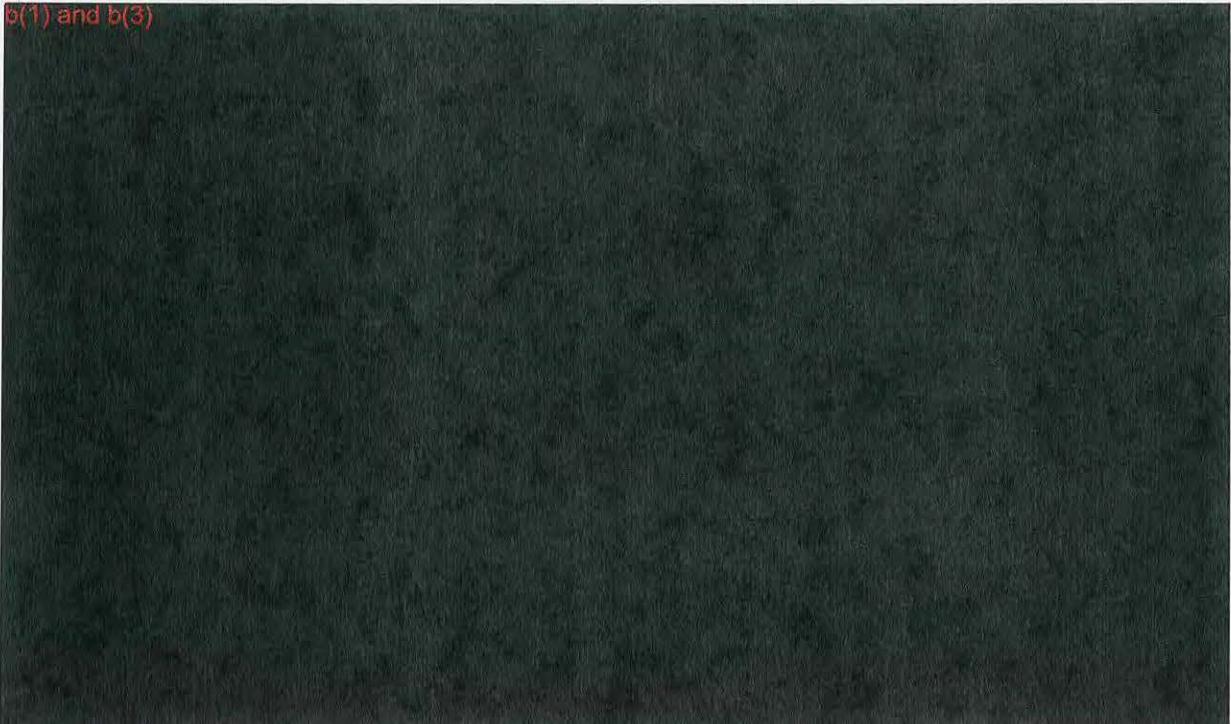
(b)(1) and (b)(3)

(b)(1) and (b)(3)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

b(1) and b(3)



The August 24 Submission also includes amendments to certifications that have been submitted by the government and approved by the Court in all prior Section 702 dockets. See

Docket Nos.

b(1) and b(3)

b(1) and b(3)

(collectively, 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 b(1) and b(3) be handled

subject to the same minimization procedures that have been submitted for use in connection with

Certifications

b(1) and b(3)

b(1) and b(3)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

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,¹ as required by 50 U.S.C. § 1881a(g)(1)(A), see [REDACTED]
- (2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see [REDACTED]
- (3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures² and minimization procedures,³
- (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);⁴ and
- (5) each of the certifications includes an effective date for the authorization in compliance

¹ The Principal Deputy Director of National Intelligence, in her capacity as Acting DNI, executed the Certifications in accordance with 50 U.S.C. § 403-3A(a)(6), which provides in pertinent part that “the Principal Deputy Director of National Intelligence shall act for, and exercise the powers of, the Director of National Intelligence during the absence or disability of the Director of National Intelligence.”

[REDACTED] ² The NSA targeting procedures and FBI targeting procedures are attached to each of the certifications as Exhibits A and C, respectively.

³ The NSA minimization procedures, FBI minimization procedures, CIA minimization procedures, and NCTC minimization procedures are attached to each of the [REDACTED] certifications as Exhibits B, D, E, and G, respectively.

⁴ See Affidavits of John C. Inglis, Acting Director, NSA (Tab 1 to [REDACTED]); Affidavits of Robert S. Mueller, III, Director, FBI (Tab 2 to [REDACTED]); Affidavits of David H. Petraeus, Director, CIA (Tab 3 to [REDACTED])

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

with 50 U.S.C. § 1881a(g)(2)(D), see [REDACTED] b(1) and b(3)
[REDACTED] b(1) and b(3)

The Court therefore finds that [REDACTED] b(1) and b(3)

[REDACTED] b(1) and b(3) 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 each of the certifications filed in the Prior 702 dockets, as originally submitted to the Court and previously amended, contained all the required elements. 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

[REDACTED] b(1) and b(3) 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. [REDACTED] b(1) and b(3)

[REDACTED] b(1) and b(3) The latest amendments also

⁵ 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).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

include effective dates that comply with 50 U.S.C. § 1881a(g)(2)(D) and § 1881a(i)(1).

b(1) and b(3)

[REDACTED] All other aspects of the certifications in the Prior 702 dockets – including the further attestations made therein in accordance with Section 1881a(g)(2)(A), the FBI and NSA targeting procedures submitted therewith in accordance with Section 1881a(g)(2)(B),⁶ and the affidavits executed in support thereof in accordance with Section 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).

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),” which is set out

⁶ Of course, targeting under the certifications filed in the Prior 702 Dockets will no longer be permitted once [REDACTED] take effect.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

in full in Subpart B below. 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 NSA and FBI Targeting Procedures Meet the Statutory Requirements.

The NSA and FBI targeting procedures included as Exhibits A and C, respectively, to the August 24 Submission differ in several respects from the corresponding procedures that have previously been approved by the Court. The government has edited Sections II and IV of the NSA targeting procedures, which address “Post-Targeting Analysis by NSA” and “Oversight and Compliance,” respectively. Section II.b of the targeting procedures describes the process used by NSA to determine when collection on a tasked electronic communications facility (e.g., an e-mail account) must stop because a user of the facility has entered the United States. See Amended NSA Targeting Procedures at 6 (§ II.b). The changes, which are clarifying rather than substantive in nature, serve the purpose of describing this process more precisely. The revised provision is consistent with the government’s prior representations to the Court regarding NSA’s post-targeting analysis and presents no difficulty under Section 1881a(d). See Docket Nos.

~~(b)(1) and (b)(3)~~ June 2, 2010 Mem. Op. at 19-23.

The government has made three changes to Section IV of the NSA targeting procedures. First, the provision has been amended to require NSA to “implement a compliance program” and “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.” Amended NSA Targeting Procedures at 7 (§ IV). The addition of this undertaking

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

obviously raises no issue under Section 1881a(d). Second, the government has replaced several references to particular components of NSA in Section IV with references to NSA generally. Id. at 7-8 (§ IV). This change has the effect of making the entire agency, rather than any particular component, responsible for ensuring adherence to particular oversight and compliance requirements set forth in the procedures. Because this change does not alter what must be done, it also presents no concern for the Court under Section 1881a(d). Third, no issue is presented by changing the required frequency for oversight reviews by the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) “at least once every sixty days,” see Docket No. b(1) and b(3) NSA Targeting Procedures at 8 (§ IV), to “approximately once every two months,” see Amended NSA Targeting Procedures at 8 (§ IV).

The government has made only one change to the FBI targeting procedures that have previously been approved by the Court. b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED]

[REDACTED] See Amended FBI Targeting Procedures at 2 (§ I.4). b(1), b(3), and b(7)(E)

[REDACTED] his alteration does not result in any substantive change and, therefore, presents no issue under Section 1881a(d)(1).

For the reasons stated above and in the Court’s opinions in the Prior 702 Dockets, the Court concludes that the revised NSA and FBI targeting procedures are reasonably designed: (1) to ensure that any acquisition authorized under Certifications b(1) and b(3) is

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

limited to targeting persons reasonably believed to be located outside the United States, and (2) 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, as required by Section 1881a(d).

B. All Four Sets of Minimization Procedures Satisfy the Statutory Requirements.

The NSA, FBI, and CIA minimization procedures attached as Exhibits B, D, and E of the August 24 Submission differ in some respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications b(1) and b(3)

b(1) and b(3) The NCTC minimization procedures included as Exhibit G to the August Submission are entirely new.

As noted above, the Court must determine whether these procedures meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) and 1821(4). See 50 U.S.C. § 1881a(e)(1). The definitions at Sections 1801(h) and 1821(4) are substantively identical for present purposes and define “minimization procedures” in pertinent part as:

(1) 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;[⁷]

⁷ Section 1801(e) defines “foreign intelligence information” as

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –

(continued...)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

50 U.S.C. § 1801(h); see also *id.* § 1821(4).⁸ For the reasons set forth below, the Court concludes that the minimization procedures filed as part of the August 24 Submission satisfy this definition, as required by 50 U.S.C. § 1881a(e).

⁷(...continued)

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or a foreign territory that relates to, and if concerning a United States person is necessary to –

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

⁸ The definitions of “minimization procedures” set forth in these provisions are substantively identical (although Section 1821(4)(A) refers to “the purposes . . . of the particular physical search”) (emphasis added). For ease of reference, subsequent citations refer only to the definition set forth at Section 1801(h)).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

I. *The CIA Minimization Procedures.*

The government has made several changes to the CIA minimization procedures.

Queries of Section 702 Information. The government has modified Section 4, which addresses the querying by CIA of information collected pursuant to Section 702. Like the previously-approved provision, the revised provision still generally requires that CIA queries of Section 702 information be “reasonably designed to find and extract foreign intelligence information”; that CIA keep records of such queries; and that DOJ and ODNI review the query records. See Amended CIA Minimization Procedures at 3 (§ 4). However, new qualifying language in the amended provision states that notwithstanding these general requirements, CIA personnel may: (1) “query CIA electronic and data storage systems that contain metadata to find, extract, and analyze metadata⁹ pertaining to communications”; (2) “use such metadata to analyze communications”; (3) “upload or transfer some or all such metadata to other CIA electronic and data storage systems for authorized foreign intelligence purposes”; and (4) “disseminat[e] . . . metadata from communications acquired under Section 702 of the Act . . . in accordance with the applicable provisions of these procedures.” Id. (§ 4.a).

The FBI Minimization Procedures previously approved by the Court contain a similar provision for metadata queries. See, e.g., Docket No. b(1) and b(3) FBI Minimization Procedures at 16 (§ 3.D (“Retention - Queries of Electronic and Data Storage Systems

⁹ The procedures provide that “‘metadata’ is dialing, routing, addressing, or signaling information associated with a communication, but does not include information concerning the substance, purport, or meaning of the communication.” Amended CIA Minimization Procedures at 1 (§ 1.c).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

Containing Raw FISA-acquired Information”)). b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED]

[REDACTED] b(1) and b(3)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Section 4 of the CIA minimization procedures has also been modified to clarify that for purposes of the procedures, “the term query does not include a user’s search or query of a CIA electronic and data storage system that contains raw FISA-acquired information, where the user does not receive the underlying raw FISA-acquired information in response to the search or otherwise have access to the raw FISA-acquired information that is searched.” Amended CIA Minimization Procedures at 3 (§ 4.b). This addition to Section 4 clarifies that a search that merely notifies the querying analyst of the existence of responsive Section 702 information – without actually providing access to the information itself – is not subject to the general querying restrictions of Section 4. Because this addition does not affect the circumstances under which CIA may acquire, retain, or disseminate U.S.-person information, it presents no concern under Section 1801(h).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

Oversight Functions and Vulnerability Assessments. The government has also added two new provisions to Section 6 of the CIA minimization procedures. The first provides that nothing in the procedures prohibits the performance of “lawful oversight functions” by CIA itself, or by DOJ, ODNI, or the “applicable Offices of the Inspectors General.” Amended CIA Minimization Procedures at 4 (§6.f). The new language merely makes explicit that the procedures should not be read to obstruct or hinder lawful and appropriate oversight functions. The Court has previously approved a similar provision in the Section 702 context. The previously-approved FBI minimization procedures, for instance, include a provision stating b(1), b(3), and b(7)(E)

Docket No. b(1) and b(3), FBI Minimization Procedures at 3 (§ I.F). The new CIA provision is broader, insofar as it expressly contemplates that certain agencies outside of CIA may perform oversight functions and in so doing could conceivably receive U.S. person information. The Court is satisfied, however, that limited disclosure of information to these recipients in order for them to discharge their oversight responsibility does not run afoul of Section 1801(h).

The second new component of Section 6 states that nothing in the procedures prevents CIA from conducting “vulnerability assessments using information acquired pursuant to Section 702 of the Act in order to ensure that CIA systems have not been compromised.” Amended CIA Minimization Procedures at 4 (§ 6.g). This language allows CIA to use information collected under Section 702 in efforts to prevent its information systems from being compromised by malware or other similar threats and to detect and remedy intrusions after they have occurred. The new language states that Section 702 information used for vulnerability assessments may be

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

“retained for one year solely for that limited purpose,” and “may be disseminated only in accordance with the applicable provisions of these procedures.” *Id.* at 4-5 (§ 6.g). This provision changes nothing about the circumstances in which CIA may acquire or disseminate Section 702 information. Though the new provision broadens CIA’s authority to retain certain Section 702 information, including U.S. person information, the resulting change is modest in scope. Furthermore, the new provision is narrowly tailored to serve an important national security purpose; maintaining the integrity of CIA’s systems is essential to the agency’s fulfillment of its mission to produce, obtain, and disseminate foreign intelligence information. This amendment is consistent with Section 1801(h).

Waiver of Destruction Requirement. Finally, the government has made a minor change to Section 8 of the CIA minimization procedures. Section 8 generally requires the CIA to destroy any communication that is acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-U.S. person located outside the United States, but who was in fact, at the time of acquisition, a U.S. person or a person located in the United States. Amended CIA Minimization Procedures at 7 (§ 8). The Director of the CIA may waive the destruction requirement for such a communication by making a specific determination in writing that the communication contains significant foreign intelligence information or evidence of a crime. *Id.* New language further clarifies that such waiver determinations must be made “on a communication-by-communication” basis. *Id.* This further specification of the waiver process presents no issue under Section 1801(h).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

2. *The FBI and NCTC Minimization Procedures.*¹⁰

Presumptions Regarding U.S. Person Status. The government has altered the language of the FBI minimization procedures regarding when it is appropriate [REDACTED] b(1), b(3), b(7)(E)

[REDACTED] Under the previously-approved procedures, [REDACTED] b(1), b(3), and b(7)(E)

[REDACTED] the procedures require the FBI to [REDACTED] b(1), b(3), and b(7)(E)

[REDACTED] See

Docket No. [REDACTED] b(1) and b(3) FBI Minimization Procedures at 2 (§ I.C). However, the previously-approved procedures permitted the FBI to [REDACTED] b(1), b(3), and b(7)(E) See

id. at 3 (§ I.C). The amended procedures adopt a uniform rule that allows the FBI [REDACTED] b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED] Amended FBI Minimization Procedures at 2-3 (§ I.D).

This change brings the FBI minimization procedures into line with [REDACTED] b(1), b(3), and b(7)(E)

¹⁰ The FBI minimization procedures previously submitted by the government and approved by the Court consist of a copy of the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search, modified in a number of respects by a three-page cover document. *See, e.g.*, Docket No. [REDACTED] b(1) and b(3) 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 Amendment Certifications, Exh. D (filed Apr. 22, 2011). Although the amended FBI minimization procedures are substantively similar in many respects to the previously-approved procedures, the amended procedures consist of a single, self-contained document that does not resort to cross-referencing. This formatting change reduces the risk of confusion and mistake and serves to bring the procedures into conformity with the FISC rules, which now restrict cross-referencing in procedures submitted to the Court for review. *See* FISC Rule 12 (adopted Nov. 1, 2010).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

b(1), b(3), and b(7)(E)

See, e.g., Docket No. b(1) and b(3) Oct. 31, 2011 b(1), b(3), and b(7)(E)

. In the context of acquisitions that are directed at non-U.S. persons located outside the United States, the Court concludes that this change to the FBI minimization procedures, b(1), b(3), and b(7)(E) comports with the definition of minimization procedures set forth at Section 1801(h).

b(1), b(3), and b(7)(E) The government has added language providing that notwithstanding the remainder of the procedures, (1), b(3), and b(7)(E)

Amended FBI Minimization Procedures at 3 (§ I.G). Like the similar provision of the amended CIA minimization procedures that is discussed above, this new provision of the FBI procedures is narrowly tailored to serve its purpose. See *id.* at 3-4 (§I.G) b(1), b(3), and b(7)(E)

The Court similarly finds that this change to the FBI procedures is consistent with the requirements of Section 1801(h).¹¹

b(7)(E) The government has modified the previously-

¹¹ The government has also broadened Section I.G to include “lawful oversight” of the FBI by DOJ, ODNI, and “applicable Offices of the Inspectors General,” in addition to oversight by the FBI itself. See Amended FBI Minimization Procedures at 3 (§ I.G). Like the similar amendment to the CIA minimization procedures discussed above, this change presents no issue under Section 1801(h).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

approved provision regarding FBI queries of information acquired under Section 702. [REDACTED]

[REDACTED]

[REDACTED] Amended FBI Minimization Procedures at 11

(§ III.D). [REDACTED]

[REDACTED]

[REDACTED] See *id.* Like the similar change to the CIA minimization procedures discussed above, this change presents no issue under Section 1801(h).

[REDACTED] The government has deleted the provisions of the FBI minimization procedures limiting the acquisition and use of [REDACTED] See Docket No. [REDACTED] FBI Minimization Procedures at 8-9 (§ 2.C); *id.* at 13-14 (§ III.C.2). In the context of telephone and Internet communications, the term [REDACTED]

[REDACTED] See *id.* at 8-9 (§ 2.C). The Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search limit the circumstances in which such communications can be retained and used for investigative or analytical purposes. See Docket No. [REDACTED] Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search at 13-14 (§ III.C.2) (as approved by the FISC on May 18, 2012). Although the same restrictions appear in prior versions of the FBI's Section 702 minimization procedures, they have no practical effect because

[REDACTED] See Docket No. [REDACTED]

FBI Minimization Procedures, Cover Document at 1. In light of that definition (which is retained

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

in the amended procedures¹²), there are no [REDACTED] for the FBI to minimize. Because the deletion of the provisions regarding [REDACTED] does not alter the manner in which the FBI acquires, retains, or disseminates Section 702 information, this change is not problematic under Section 1801(h).¹³

[REDACTED] The government has added a new provision to the FBI minimization procedures requiring the FBI to [REDACTED]. [REDACTED] See Amended FBI Minimization Procedures at 9-10 (§ III.C.2). This change obviously presents no issue under Section 1801(h).

[REDACTED] The government has made a minor change to the [REDACTED] provision set forth in the final paragraph of Section III.A of the amended FBI minimization procedures. This provision, [REDACTED] generally requires the FBI to remove from its systems any communication that is acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-U.S. person located outside the United States but who is located inside the United States at the time of acquisition or is subsequently determined to be a U.S. person. See Amended FBI Minimization Procedures at 6 (§ III.A). The Director or Deputy Director of the FBI may

¹² See Amended FBI Minimization Procedures at 2 (§ I.B.3) [REDACTED] [REDACTED]

¹³ The Court reaches this conclusion with the understanding the FBI does not acquire, either directly or through NSA, so-called “about” communications – *i.e.*, communications that are not to or from a tasked facility but merely contain a reference to a tasked facility. Certain “about” communications are acquired by NSA through its upstream collection of Internet communications, the fruits of which are not shared with FBI or CIA in unminimized form. See Nov. 30 Op., *supra*, at 7 n.3.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

b(1), b(3), and b(7)(E) by making a specific determination in writing that b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED]

[REDACTED] Id. The amended

provision contains new language further clarifying that b(1), b(3), and b(7)(E) must be made

b(1), b(3), and b(7)(E) basis. b(1), b(3), and b(7)(E)

[REDACTED] this amendment to the FBI procedures does not alter

the requirements of the b(1), b(3), and [REDACTED] and therefore presents no issue under Section 1801(h).

b(1), b(3), b(7)(E) The amended FBI minimization procedures retain a previously-approved provision requiring that FBI b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED]

Amended FBI Minimization Procedures at 19 (§ III.G.1.a). However, new language provides

that an AD (or his superior) can b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED] Id. The amended provision further

states that b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED] Id. This change limits the FBI's discretion to b(1), b(3), and b(7)(E) Section

702 information and, therefore, presents no concern under Section 1801(h).

b(1), b(3), b(7)(E) The amended FBI minimization procedures retain the

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

previously-approved requirements for [REDACTED], with one minor change. See Amended FBI Minimization Procedures at 12-16 (§ III.E). The previously-approved minimization procedures require that, when the FBI determines that [REDACTED] has been identified, the FBI shall [REDACTED]

[REDACTED]
[REDACTED]
Docket No. [REDACTED], FBI Minimization Procedures at 18 (§ III.E.1.c) & 20 (§ III.E.2.c). The amended FBI Minimization Procedures require the FBI to [REDACTED]

[REDACTED] See Amended FBI Minimization Procedures at 12-13 (§ III.E.1.c) & 14 (§ III.E.2.c). The Court recently approved identical changes to the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search. See Docket Numbers [REDACTED] May 18, 2012 Mem. Op. and Order (“May 18 Opinion”) at 18-19. The Court sees no reason to reach a different result here, in the context of collection that is directed at non-U.S. persons located outside the United States and, therefore, less likely to [REDACTED]

Dissemination. The dissemination provisions of the FBI minimization procedures reflect a number of changes from the previously-approved procedures. Three of these changes conform the Section 702 minimization procedures to the dissemination provisions of the recently-revised Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search:

- The amended FBI minimization procedures [REDACTED]

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

b(1), b(3), and b(7)(E)
[REDACTED] Amended FBI Minimization Procedures at 21 (§ IV.A) (emphasis added).

• With regard to foreign governments, the amended FBI minimization procedures explicitly b(1), b(3), and b(7)(E) [REDACTED]. See Amended FBI Minimization Procedures at 22-24 (§ IV.C).

• The amended FBI minimization procedures b(1), b(3), and b(7)(E) [REDACTED] that the FBI b(1), b(3), and b(7)(E) [REDACTED]. The previously-approved procedures state " See Docket No. b(1) and b(3) [REDACTED] FBI Minimization Procedures at 27 (§ IV.A) (emphasis added).¹⁴ In contrast, the amended procedures b(1), b(3), and b(7)(E) [REDACTED] Amended FBI Minimization Procedures at 21 (§ IV.A) (emphasis added). As discussed in the May 18 Opinion, b(1), b(3), and b(7)(E) [REDACTED]. See May 18 Op. at 14-15.¹⁵

¹⁴ Section IV.A of the previously-approved FBI minimization procedures further provides that b(1), b(3), and b(7)(E) [REDACTED] (Emphasis added.) This language is stricken by the amendments to the FBI procedures and rendered superfluous by b(1), b(3), and b(7)(E) [REDACTED]

¹⁵ The amendments to the FBI procedures also replace certain references to b(1), b(3), and b(7)(E) [REDACTED] Compare, e. g., Docket No. [REDACTED] FBI Minimization Procedures at 30-31 (§ IV.D), with Amended FBI Minimization Procedures at 24 (§ IV.D). The government advises that this change in terminology is not (continued...)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

For the reasons set forth in the May 18 Opinion approving the same modifications to the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search, the Court concludes that these changes to the amended FBI minimization procedures for Section 702 acquisitions also are consistent with the requirements of Section 1801(h). In reaching this conclusion, the Court relies upon the same Executive Branch representations on which it relied in the May 18 Opinion.

The amended FBI minimization procedures contain a new provision permitting the FBI, in the event Section 702 information ~~b(1), b(3), and b(7)(E)~~

~~_____~~

~~_____~~

~~_____~~

Amended FBI Minimization

Procedures at 26 (§ IV.H). This provision closely tracks language that the Court has approved as a supplemental minimization procedure in numerous orders granting authority to conduct

electronic surveillance and physical search in cases ~~b(1), b(3), and b(7)(E)~~

~~_____~~

See, e.g., Docket No. ~~b(1) and b(3)~~ Primary Order and Warrant at 10.

The Court sees no issue under Section 1801(h) with the inclusion of such a provision in the Section 702 minimization procedures.

Finally, the amended FBI minimization procedures ~~b(7)(E)~~

~~_____ b(1), b(3), and b(7)(E)~~

¹⁵(...continued)

intended to have any substantive effect. See May 18 Op. at 13 n.23.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

b(1), b(3), and b(7)(E)

Amended FBI Minimization Procedures at 26 (§ IV.G) b(7)(E)

NCTC is “the primary organization in the United States Government for analyzing and integrating all intelligence . . . pertaining to terrorism and counterterrorism,” excepting exclusively domestic matters. 50 U.S.C. § 404o(d)(1). Its responsibilities include “ensur[ing] that agencies, as appropriate, have access to and receive all-source intelligence support needed to execute their counterterrorism plans” and “disseminat[ing] terrorism information, including current terrorism threat analysis, to the President” and other executive branch officials, as well as “the appropriate committees of Congress.” § 404o(d)(4), (f)(1)(D). It also has “primary responsibility within the United States Government for conducting net assessments of terrorist threats.” § 404o(f)(1)(G).

Pursuant to an order issued in 2008, NCTC was authorized to receive certain FISA-

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

derived information from terrorism cases that FBI had uploaded to its [redacted] does not contain raw FISA information. Rather, it contains FBI investigative reports and other work product, some of which contain FISA information. As a result, FISA-derived information regarding U.S. persons that NCTC personnel can access [redacted] has already been subject to minimization by the FBI. The Court approved procedures in 2008 that permit the FBI to [redacted]

[redacted] b(1), b(3), and b(7)(E)

[redacted]

[redacted]

[redacted] Docket No. [redacted] Oct. 8, 2008 Mem. Op. at 3-6. The Court

found that [redacted] FBI b(1), b(3), and b(7)(E)

[redacted]. *Id.* at 3.

[redacted] b(1), b(3), and b(7)(E)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

See Docket No. [redacted] b(1) and b(3) [redacted] b(1), b(3), and b(7)(E)

[redacted]

¹⁶ [redacted] b(1), b(3), and b(7)(E)

[redacted]

(continued...)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

The new Section IV.G of the amended Section 702 FBI minimization procedures and the new NCTC minimization procedures are consistent with the requirements of Section 1801(h). In light of NCTC's important role in analyzing and processing intelligence regarding terrorism and counterterrorism, providing it with access to terrorism- and counterterrorism-related information in FBI general indices is consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information, as required by Section 1801(h)(1). Given the non-U.S. person, overseas focus of Section 702 collection, the information at issue b(1), b(3) and b(7)(E) to contain U.S. person information that is not foreign intelligence information as defined in Section 1801(e)(1), which is the principal concern of Section 1801(h)(2). Finally, the FBI will have applied its own minimization procedures to the information at issue here before it is shared with NCTC, and those procedures allow the dissemination of evidence of a crime for law enforcement purposes. See Amended FBI Minimization Procedures at 22-24 (§ IV.B & C). Accordingly, the Court is satisfied that the FBI and NCTC minimization procedures, taken together, permit the dissemination of evidence of a crime for law enforcement purposes, as required by Section 1801(h)(3).

3. *The NSA Minimization Procedures.*

The NSA minimization procedures have been altered in a number of respects. Before addressing the changes, some background discussion is warranted.

¹⁶(...continued)

b(1), b(3), and b(7)(E)

The amended FBI procedures at issue here do not permit the sharing of unminimized Section 702 information with NCTC.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

a. *The Scope of NSA's Upstream Collection.*

Last year, following the submission of Certifications ~~b(1) and b(3)~~ for renewal, the government made a series of submissions to the Court disclosing that it had materially misrepresented the scope of NSA's "upstream collection" under Section 702 (and prior authorities including the Protect America Act). The term "upstream collection" refers to the acquisition of Internet communications as they transit the "internet backbone" facilities ~~b(1) and b(3)~~ as opposed to the collection of communications directly from Internet service providers like ~~b(1) and b(3)~~. See Docket Nos. ~~b(1) and b(3)~~ ~~b(1) and b(3)~~ Oct. 3, 2011 Memorandum Opinion ("Oct. 3 Op.") at 5 n.3. Since 2006, the government had represented that NSA's upstream collection only acquired discrete communications to or from a facility tasked for acquisition and communications that referenced the tasked facility (so-called "about" communications). See *id.* at 15-16. With regard to the latter category, the government had repeatedly assured the Court that NSA only acquired ~~b(1)~~ specific categories of "about" communications. *Id.*

The government's 2011 submissions made clear, however, that NSA's upstream collection was much broader than the government had previously represented. For the first time, the government explained that NSA's upstream collection results in the acquisition of "Internet transactions" instead of discrete communications to, from or about a tasked selector. See *id.* at 15. Internet transactions, the government would ultimately acknowledge, could and often do contain multiple discrete communications, including wholly domestic non-target communications and other non-target communications to, from, or concerning U.S. persons. *Id.*

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

While the government was able to show that the percentage of wholly domestic non-target communications and other non-target communications to, from, or concerning U.S. persons being acquired was small relative to the total volume of Internet communications acquired by the NSA pursuant to section 702, the acquisition of such communications nonetheless presented a significant issue for the Court in reviewing the procedures. In fact, it appeared that NSA was annually acquiring tens of thousands of Internet transactions containing at least one wholly domestic communication; that many of these wholly domestic communications were not to, from, or about a targeted facility; and that NSA was also likely annually acquiring tens of thousands of additional Internet transactions containing one or more non-target communications to or from U.S. persons or persons in the United States. *Id.* at 33, 37.

In the October 3 Opinion, the Court approved in large part Certifications b(1) and b(3) and the accompanying targeting and minimization procedures. The Court concluded, however, that one aspect of the proposed collection – NSA’s upstream collection of Internet transactions containing multiple communications, or “MCTs” – was, in some respects, deficient on statutory and constitutional grounds. The Court concluded that although NSA’s targeting procedures met the statutory requirements, the NSA minimization procedures, as the government proposed to apply them to MCTs, did not satisfy the statutory definition of “minimization procedures” with respect to retention. Oct. 3 Op. at 59-63. As applied to the upstream collection of Internet transactions, the Court found that the procedures were not reasonably designed to minimize the retention of U.S. person information consistent with the government’s national security needs. *Id.* at 62-63. The Court explained that the net effect of the

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

procedures would have been that thousands of wholly domestic communications, and thousands of other discrete communications that are not to or from a targeted selector but that are to, from, or concerning United States persons, would be retained by NSA for at least five years, despite the fact that they have no direct connection to a targeted selector and, therefore, were unlikely to contain foreign intelligence information. Id. at 60-61. For the same reason, the Court concluded that NSA's procedures, as the government proposed to apply then to MCTs, failed to satisfy the requirements of the Fourth Amendment. Id. at 78-79. The Court noted that the government might be able to remedy the deficiencies that it had identified, either by tailoring its upstream acquisition or by adopting more stringent post-acquisition safeguards. Id. at 61-62, 79.

By operation of the statute, the government was permitted to continue the problematic portion of its collection for 30 days while taking steps to remedy the deficiencies identified in the October 3 order and opinion. See 50 U.S.C. § 1881a(i)(3)(B). In late October of 2011, the government timely submitted amended NSA minimization procedures that included additional provisions regarding NSA's upstream collection. The amended procedures, which took effect on October 31, 2011 ("Oct. 31, 2011 NSA Minimization Procedures"), require NSA to restrict access to the portions of its ongoing upstream collection that are most likely to contain wholly domestic communications and non-target information that is subject to statutory or Fourth Amendment protection. See Nov. 30 Op. at 7-9. Segregated Internet transactions can be moved to NSA's general repositories only after having been determined by a specially trained analyst not to contain a wholly domestic communication. Id. at 8. Any transaction containing a wholly domestic communication (whether segregated or not) would be purged upon recognition. Id. at

~~TOP SECRET//SI//ORCON,NOFORN~~

Page 28

THIS PAGE WAS RELEASED IN FULL

~~TOP SECRET//SI//ORCON,NOFORN~~

8, 9. Any transaction moved from segregation to NSA's general repositories would be permanently marked as having previously been segregated. Id. at 8. On the non-segregated side, any discrete communication within an Internet transaction that an analyst wishes to use is subject to additional checks. Id. at 8-10. NSA is not permitted to use any discrete, non-target communication that is determined to be to or from a U.S. person or a person who appears to be in the United States, other than to protect against an immediate threat to human life. Id. at 9. Finally, all upstream acquisitions are retained for a default maximum period of two, rather than five, years. Id. at 10-11.

The Court concluded in the November 30 Opinion that the October 31, 2011 NSA Minimization Procedures adequately remedied the deficiencies that had been identified in the October 3 opinion. Id. at 14-15. Accordingly, NSA was able to continue its upstream collection of Internet transactions (including MCTs) without interruption, but pursuant to amended procedures that are consistent with statutory and constitutional requirements.

However, issues remained with respect to the past upstream collection residing in NSA's databases. Because NSA's upstream collection almost certainly included at least some acquisitions constituting "electronic surveillance" within the meaning of 50 U.S.C. § 1801(f), any overcollection resulting from the government's misrepresentation of the scope of that collection implicates 50 U.S.C. § 1809(a)(2). Section 1809(a)(2) makes it a crime 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. The Court therefore directed the government to make a written submission addressing

~~TOP SECRET//SI//ORCON,NOFORN~~

THIS PAGE WAS RELEASED IN FULL

~~TOP SECRET//SI//ORCON,NOFORN~~

the applicability of Section 1809(a), which the government did on November 22, 2011. See Docket No. b(1) and b(3) Oct. 13, 2011 Briefing Order, and Government's Response to the Court's Briefing Order of Oct. 13, 2011 (arguing that Section 1809(a)(2) does not apply).

Beginning late in 2011, the government began taking steps that had the effect of mitigating any Section 1809(a)(2) problem, including the risk that information subject to the statutory criminal prohibition might be used or disclosed in an application filed before this Court. The government informed the Court in October 2011 that although the amended NSA procedures do not by their terms apply to information acquired before October 31, NSA would apply portions of the procedures to the past upstream collection, including certain limitations on the use or disclosure of such information. See Nov. 30 Opinion at 20-21. Although it was not technically feasible for NSA to segregate the past upstream collection in the same way it is now segregating the incoming upstream acquisitions, the government explained that it would apply the remaining components of the amended procedures approved by the Court to the previously-collected data, including (1) the prohibition on using discrete, non-target communications determined to be to or from a U.S. person or a person in the United States, and (2) the two-year age-off requirement. See id. at 21.

Thereafter, in April 2012, the government orally informed the Court that NSA had made a "corporate decision" to purge all data in its repositories that can be identified as having been acquired through upstream collection before the October 31, 2011 effective date of the amended NSA minimization procedures approved by the Court in the November 30 Opinion. NSA's

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

effort to purge that information, to the extent it is reasonably feasible to do so, is now complete.

See Aug. 24 Submission at 9-10.¹⁷

Finally, NSA has adopted measures to deal with the possibility that it has issued reports based on upstream collection that was unauthorized. NSA has identified (b)(1) and (b)(7) reports that were issued from the inception of its collection under Section 702 to October 31, 2011, that rely at least in part on information derived from NSA's upstream acquisitions from that period. See Sept. 12, 2012 Supplement to the Government's Ex Parte Submission of Reauthorization Certifications at 2 ("Sept. 12 Submission"). The government advises that, of the (b)(1) and (b)(7) reports, (b)(1) have been confirmed to be based entirely upon communications that are to, from or about persons properly targeted under Section 702 and therefore present no issue under Section 1809(a)(2). See id. The government is unable to make similar assurances, however, regarding the remaining (b)(1) reports. Accordingly, NSA will direct the recipients of those (b)(1) reports (both within NSA and outside the agency) not to further use or disseminate information contained therein without first obtaining NSA's express approval. Id. at 3-4. Upon receipt of such a request, NSA will review the relevant report to determine whether continued use thereof is

¹⁷ The government has informed the Court that NSA stores some of the past upstream collection in repositories in which it may no longer be identifiable as such. (b)(1) and (b)(3)

See Aug. 24 Submission at 14-16. Assuming that NSA cannot with reasonable effort identify information in its repositories as the fruit of an unauthorized electronic surveillance, such information falls outside the scope of Section 1809(a)(2), which by its terms applies only when there is knowledge or "reason to know that the information was obtained through electronic surveillance not authorized" by statute.

~~TOP SECRET//SI//ORCON,NOFORN~~

THIS PAGE WAS RELEASED IN FULL

~~TOP SECRET//SI//ORCON,NOFORN~~

appropriate. *Id.* at 4.¹⁸ Finally, the government has informed the Court that it will not use any report that cites to upstream collection acquired prior to October 31, 2011 in an application to this Court absent express notice to, and approval of, the Court. Aug. 24 Submission at 24.

Taken together, the remedial steps taken by the government since October 2011 greatly reduce the risk that NSA will run afoul of Section 1809(a)(2) in its handling of the past upstream acquisitions made under color of Section 702. NSA's self-imposed prohibition on using non-target communications to or from a U.S. person or a person in the United States helped to ensure that the fruits of unauthorized electronic surveillance were not used or disclosed while it was working to purge the pre-October 31, 2011 upstream collection. And NSA's subsequent purge of that collection from its repositories and the above-described measures it has taken with respect to derivative reports further reduce the risk of a problem under Section 1809(a)(2). Finally, the amended NSA minimization procedures provide that in the event, despite NSA's effort to purge the prior upstream collection, the agency discovers an Internet transaction acquired before October 31, 2011, such transaction must be purged upon recognition. See Amended NSA Minimization Procedures at 8 § 3(c)(3). In light of the foregoing, it appears to the Court that the outstanding issues raised by NSA's upstream collection of Internet transactions have been resolved, subject to the discussion of changes to the minimization procedures that appears

¹⁸ For instance, NSA may determine that the report is fully supported by cited communications other than the ones obtained through upstream communication. Sept. 12 Submission at 4. In other instances, NSA may revise the report so that it no longer relies upon upstream communications and reissue it. *Id.* If such steps are not feasible because the report cannot be supported without the upstream communication, NSA will cancel the report. *Id.*

~~TOP SECRET//SI//ORCON,NOFORN~~

THIS PAGE WAS RELEASED IN FULL

~~TOP SECRET//SI//ORCON,NOFORN~~

below.¹⁹

b. Changes to the NSA Minimization Procedures.

“Processing” versus “handling” information. In a number of places in the amended NSA minimization procedures, the government has replaced the term “processed” with the word “handled.” See Amended NSA Minimization Procedures at 9 (§ 5(1)) & 12 (§§ 6(c)(1) & 6(c)(2)). Both the previously-approved NSA minimization procedures and the amended procedures define the terms “processed” or “processing” to mean “any step necessary to convert a communication into an intelligible form intended for human inspection.” *Id.* at 2 (§ 2(h)). The previously-approved procedures did not uniformly use the terms in a manner consistent with that narrow definition. This clarifying change remedies that inconsistency by using the distinct term “handled” or “handling” to refer to the treatment of communications after they have been rendered intelligible for human inspection. This non-substantive change reduces the potential for confusion and mistake and raises no issue under Section 1801(h).

Oversight Functions. Like the amended CIA and FBI minimization procedures discussed above, the amended NSA minimization procedures contain language stating that the procedures do not restrict the exercise of “lawful oversight” of NSA by NSA itself, DOJ, ODNI, or “the applicable Offices of Inspectors General.” Amended NSA Minimization Procedures at 1 (§ 1). For the same reasons, the Court finds that this provision is consistent with Section 1801(h).

¹⁹ Under the circumstances, the Court finds it unnecessary to further address the arguments advanced by the government in its November 22, 2011 response to the Court’s October 13, 2011 briefing order regarding Section 1809(a), particularly those regarding the scope of prior Section 702 authorizations.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

Vulnerability or Network Assessments. The amended NSA minimization procedures also state that the procedures do not restrict NSA's performance of "vulnerability or network assessments using information acquired pursuant to Section 702 . . . in order to ensure that NSA systems are not or have not been compromised." Amended NSA Minimization Procedures at 1 (§ 1). (b)(1), (b)(3), and (b)(7)(E)

[REDACTED], this "vulnerability or network assessments" language also raises no concern under Section 1801(h). The language allows NSA to use information collected under Section 702 in efforts to prevent its information systems from being compromised by malware or other similar threats and to detect and remedy intrusions after they have occurred. Maintaining the integrity of NSA's systems is essential to the agency's fulfillment of its national security mission, including the acquisition, production, and dissemination of foreign intelligence information. The new language is narrowly crafted to serve that purpose, stating that Section 702 information used for vulnerability or network assessments may be "retained for one year solely for that limited purpose," and "may be disseminated only in accordance with the applicable provisions of these procedures." *Id.* at 1 (§ 1).

Upstream Collection. The government has made several changes to Section 3(b) of the NSA minimization procedures, which, among other things, addresses NSA's handling of Internet transactions acquired through its upstream collection. Section (3)(b)(4)(a)²⁰ generally requires NSA to use technical means to segregate and restrict access to the two categories of MCTs that

²⁰ The government has renumbered portions of Section 3 so that the substance of Section 3(b)(5) of the previously-approved procedures now appears in Section 3(b)(4).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

are most likely to contain non-target information concerning U.S. persons or persons in the United States. See Nov. 30, 2012 Mem. Op. at 11-12. The amended procedures include new language stating that notwithstanding this general segregation requirement, “NSA may process Internet transactions . . . in order to render such transactions intelligible to analysts.” See Amended NSA Minimization Procedures at 4 (§ 3(b)(4)(a)(1)). The Court’s understanding is that this new language permits NSA to render Internet transactions intelligible to humans before segregating them in accordance with Section 3(b)(4)(a). With the understanding that the procedures continue to preclude access to Internet transactions by intelligence analysts until after segregation (and even then, only in accordance with the remainder of the procedures), the Court is satisfied that this amendment is consistent with Section 1801(h).

The previously approved procedures required NSA to “destroy[] upon recognition” any Internet transaction containing a discrete wholly domestic communications (i.e., a communication as to which the sender and all intended recipients are reasonably believed to be in the United States). See Oct. 31, 2011 NSA Minimization Procedures at 4 § 3(b)(5)(a)(1)(a); see also Nov. 30, 2011 Mem. Op. at 9. The amended procedures state that Internet transactions recognized as containing a discrete wholly domestic communication must “be handled in accordance with Section 5 below.” Amended NSA Minimization Procedures at 4-5 (§§ 3(b)(4)(a)(2)(a), 3(b)(4)(b)(1)). Section 5 requires as a general rule that “a communication identified as a domestic communication (and if applicable the Internet transaction in which it is contained) will be promptly destroyed upon recognition.” Id. at 8 (§ 5). As explained below, however, Section 5 allows the Director of NSA to waive the destruction of a particular

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

communication under certain circumstances. Id. at 8-9 (§ 5). Accordingly, the effect of this amendment to Section 3(b) is to convert what was an absolute destruction requirement into a qualified destruction requirement. Nevertheless, as discussed below, the circumstances in which a Director's waiver may be granted are narrowly defined, so that the Court is satisfied that this amendment to the NSA minimization procedures is consistent with Section 1801(h).

Another change to Section 3(b) of the NSA minimization procedures involves metadata. The procedures approved by the Court in the November 30, 2011 Memorandum Opinion contain a provision allowing NSA to copy metadata from Internet transactions that are not subject to segregation pursuant to Section 3(b) without first complying with the other rules for handling non-segregated transactions – i.e., without ruling out that the metadata pertained to a discrete wholly domestic communication or to a discrete non-target communication to or from a U.S. person or a person inside the United States. See Nov. 30, 2011 Mem. Op. at 15-20. Metadata copied pursuant to this provision must be handled in accordance with the other provisions of the procedures. Id. at 16. Furthermore, in the event that NSA later identifies an Internet transaction as containing a wholly domestic communication, any metadata that has been extracted from that transaction must be destroyed. Id.

The amended procedures retain this provision, but now expressly limit it to Internet transactions acquired on or after October 31, 2011. Amended NSA Minimization Procedures at 6 (§ 3(b)(4)(b)(4)). This date change accounts for the fact that, as discussed above, NSA's upstream acquisitions before that date have been subject to an earlier set of minimization procedures that did not provide for the extraction and use of metadata by NSA. See Nov. 30,

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

2011 Mem. Op. at 20-21. The addition of the date makes clear that although the amended NSA minimization procedures now generally apply to Section 702 information acquired by NSA under all certifications, this metadata provision continues to apply only to information acquired under the 2011 and 2012 certifications. Because this amendment serves only to preserve the status quo with respect to metadata, it presents no issue under Section 1801(h).

Destruction of Raw Data. The government has amended Section 3(c) of the NSA minimization procedures, which limits the retention of raw Section 702 information acquired by NSA. Like the previously-approved procedures, the amended procedures provide a default retention period of two years for upstream Internet communications and a default retention period of five years for all other communications. See Amended NSA Minimization Procedures at 7 (§ 3(c)). The government has added language to Section 3(c) to make clearer that these retention limits are subject to separate provisions of the procedures, which may allow a particular communication to be retained longer – e.g., because it contains U.S. person-identifying information that is necessary to understand foreign intelligence information or assess its importance. See id. at 7 (§ 3(c)); id. at 10-11 (§ 6). New language also makes clear that the determination that a communication qualifies for retention beyond the default “age off” period must be made by NSA on a communication-by-communication basis and, in the case of Internet transactions, is subject to the special rules set forth in Section 3(b) of the procedures. Id. at 7 (§ 3(c)). These clarifying changes raise no issue under Section 1801(h).

The final change to Section 3(c) is new language requiring NSA to destroy upon recognition “[a]ny Internet transaction acquired through NSA’s upstream collection techniques

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

prior to October 31, 2011.” Amended NSA Minimization Procedures at 8 (§ 3(c)(3)). As discussed above, NSA has deleted “all data objects identified as acquired through NSA’s upstream Internet collection techniques on or before October 31, 2011.” See Aug. 24 Submission at 9. This new language formalizes NSA’s undertaking to destroy any additional information that is hererafter identified as having been acquired through its prior upstream Internet collection and presents no issue under Section 1801(h).

Waiver of Destruction Requirement. The previously-approved NSA minimization procedures generally require that NSA destroy upon recognition any communication that is defined as a domestic communication. Oct. 31, 2011 NSA Minimization Procedures at 8 (§ 5). Domestic communications include: (1) any communication that does not have at least one communicant outside the United States, see id. at 2 (§ 2(e)); (2) any communication 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 communication was acquired, id. at 7 (§ 3(d)(2)); and (3) any communication acquired by targeting a person who at the time of targeting was believed to be a non-U.S. person but was in fact a U.S. person, id. The destruction requirement can be waived, however, if the Director or Acting Director of the NSA “specifically determines in writing” that:

- (1) the communication is “reasonably believed to contain significant foreign intelligence information,” in which case it can be “provided to the FBI (including United States person identities) for possible dissemination in accordance with its minimization procedures”;
- (2) the communication is “reasonably believed to contain evidence of a crime,” in which case it can be disseminated to appropriate federal law enforcement authorities and retained for a reasonable period of time to permit appropriate

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

access by law enforcement agencies;

(3) the communication is reasonably believed to contain information necessary to be retained for cryptanalytic, traffic analytic, or signal exploitation purposes, or information necessary to understand or assess a security vulnerability, in which case it can be obtained for a period sufficient to permit exploitation; or

(4) the communication contains information pertaining to a threat of serious harm to life or property.

See id. The previously-approved procedures further provide that notwithstanding these requirements: (1) “if a domestic communication indicates that a target has entered the United States, NSA may advise FBI of that fact”; and (2) NSA may retain and provide to FBI and CIA certain information deemed necessary “for collection avoidance purposes.” Id. at 9 (§ 5).

~~b(1), b(3), and b(7)(E)~~

~~_____~~, the government has amended Section 5 to further clarify that waivers may only be made on a “communication-by-communication basis.” See Amended NSA Minimization Procedures at 8 (§ 5). This change does not alter the requirements of the waiver provision and raises no concern under Section 1801(h).²¹

²¹ In October 2011, the government reported a compliance incident involving NSA’s application of Section 5. The incident was the subject of a more detailed follow-up submission made on August 28, 2012 (“Aug. 28 Submission”). As previously approved by the Court, Section 5 states that a waiver may occur only when “the Director (or Acting Director) specifically determines, in writing,” that one of the four enumerated criteria is met with respect to “[a] communication.” See, e.g., Oct. 31, 2011 NSA Minimization Procedures at 8 (§ 5). In accordance with this language, the government represented to the Court in 2008 that the waiver provision would be applied on a “case-by-case basis” rather than categorically. Docket No. ~~b(1) and b(3)~~ Aug. 27, 2008 Hrg. Tr. at 36-37. The Court relied on this representation in approving Section 5. Docket No. ~~b(1) and b(3)~~ Sept. 4, 2008 Mem. Op. at 25 n.24.

In March 2011, however, the Acting Director of NSA made an “advance waiver

(continued...)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

Another change to Section 5 is the addition of new language that limits the types of domestic communications that may be the subject of a destruction waiver. As amended, the provision requires the Director (or Acting Director) to specifically determine in writing not only that one of the four enumerated conditions is satisfied, but also that “the sender or intended recipient of the domestic communication had been properly targeted under Section 702 of the Act.” See Amended NSA Minimization Procedures at 8 (§ 5). The change has the practical effect of limiting the reach of the waiver provision to domestic communications acquired with the reasonable but mistaken belief that the target is a non-U.S. person located outside the United States. This narrowing amendment is consistent with the requirements of Section 1801(h).

A third change to Section 5 of the NSA minimization procedures broadens the effect of a waiver made on the ground that the communication at issue contains significant foreign intelligence information. While the previously-approved language of Section 5(1) states that a

²¹(...continued)

determination” pursuant to which NSA personnel could thereafter deem “certain terrorism-related communications that met specific criteria . . . to contain ‘significant foreign intelligence’ and hence . . . subject to a destruction waiver.” Aug. 28 Submission at 2. This advance waiver determination was relied upon seven times by NSA personnel until September 2011, when it was rescinded as inconsistent with the requirements of Section 5. Id. It was later determined, however, that in six of those instances no waiver was required. Id. After reporting the incident to the Court, DOJ and NSA undertook a review of NSA’s practice under Section 5 of the procedures. That review revealed that NSA has used the waiver provision on 16 other occasions and that each of those other waivers was consistent with the requirements of Section 5. Id. at 3. Furthermore, NSA, working together with DOJ, has undertaken a number of steps to improve coordination of guidance involving NSA’s FISA authorities (including Section 702) and is continuing to strengthen its internal compliance infrastructure. Id. at 3-6. In light of the corrective measures taken by the government following the “advance waiver determination” incident, the Court is satisfied that the incident does not preclude a finding that NSA’s minimization procedures satisfy the requirements of Section 1801(h).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

communication retained on that basis can be “provided to the FBI . . . for possible dissemination in accordance with its minimization procedures,” Oct. 31, 2011 NSA Minimization Procedures at 8 (§ 5(1)), the amended provision states that such a communication “may be retained, handled, and disseminated in accordance with these procedures,” Amended NSA Minimization Procedures at 9 (§ 5(1)). The result of this change is that NSA may retain, use, and disseminate such a communication as if it constitutes a “foreign communication.” See Amended NSA Minimization Procedures at 10-12 (§§ 6-7) (setting forth rules for retention and dissemination of foreign communications). Read in isolation, this amendment appears to give NSA substantially more leeway to retain, use, and disseminate a domestic communication that is the subject of the waiver on “significant foreign intelligence” grounds. As discussed in the preceding paragraph, however, the waiver provision, as amended, now may be applied only to those domestic communications acquired with a reasonable, but mistaken, belief that the target is a non-U.S. person located outside the United States. The Court has previously recognized that Section 702 authorizes the government to acquire such communications. See Docket No. [REDACTED] Sept. 4, 2008 Mem. Op. at 25-26. Moreover, if a communication retained on this basis contains U.S.-person identifying information, that information must be deleted before the communication can be disseminated outside NSA unless one of eight specific exceptions applies. See Amended NSA Minimization Procedures at 11-12 (§ 6(b)). Under the circumstances, the Court is satisfied that this amendment to Section 5(1) of the NSA minimization procedures is consistent with Section 1801(h).

Another change to the NSA minimization procedures provides that in the event a

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

domestic communication subject to a waiver by the Director or Acting Director is contained within an Internet transaction, NSA may retain the entire transaction. See Amended Minimization Procedures at 9 (§ 5). This change addresses NSA's inability to disaggregate Internet transactions that it has acquired under Section 702 without destabilizing its systems. See Docket Nos. b(1) and b(3) Government's Response to the Court's Briefing Order of May 9, 2011 (filed June 1, 2012) at 22. The change permits NSA to retain not just the particular portion of an Internet transaction that is deemed to qualify for a waiver, but also other unrelated portions of the transaction within which it was acquired, which may include non-target U.S. person information with no foreign intelligence value. For several reasons, the Court is satisfied that this change is consistent with the requirements of Section 1801(h). First, NSA has only applied the waiver provision 16 times since Section 702 collection commenced in 2008. See Aug. 28 Submission at 2. Furthermore, as discussed above and in the November 30 Opinion, NSA's minimization procedures include special handling requirements for Internet transactions, including protections for non-target U.S. person information, that will apply to any transaction that is retained by NSA following a Section 5 waiver. Finally, the procedures require NSA to delete U.S.-person identifying information from a communication before disseminating it outside the agency, unless one of eight specific exceptions applies. See Amended NSA Minimization Procedures at 11-12 (§ 6(b)).

The final change to Section 5 involves what NSA may do, absent a Director's waiver, in the event that a domestic communication indicates that a target has entered the United States. The previously-approved procedures allow NSA to advise the FBI of the fact of the target's entry

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

into the United States and to retain and provide to FBI and CIA technical information about the communication for “collection avoidance purposes.” Oct. 31, 2011 NSA Minimization Procedures at 9 (§ 5). The amended procedures permit NSA not only to inform the FBI of the fact of the target’s entry into the United States and share with the FBI and CIA the same technical “collection avoidance” information, but also to provide to the FBI “any information concerning the target’s location that is contained in the communication.” Amended NSA Minimization Procedures at 10 (§ 5). In addition, the amended provision states that 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).” *Id.* This change to Section 5 allows NSA to share limited information with the FBI and serves to better facilitate the transition from Section 702 coverage of the target to other forms of surveillance or investigation that are permitted within the United States. The Court is satisfied that this amendment to the procedures is consistent with Section 1801(h).

C. The Targeting and Minimization Procedures Are Consistent with the Fourth Amendment.

The final question before the Court is whether the targeting and minimization procedures included as part of the August 24 Submission are consistent with the Fourth Amendment. *See* 50 U.S.C. § 1881a(i)(3)(A). Largely for the same reasons that the Court has concluded that the amended procedures meet the requirements of Section 1881a(d)-(e), the Court is also satisfied that the amended procedures are reasonable under the Fourth Amendment. The basic framework of protections formed by the previously-approved procedures remains intact. Many of the amendments made by the government add to those protections or merely serve to clarify what is

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

required of the government. The remaining changes do not individually or collectively alter the Court's prior conclusion that the targeting and minimization procedures are consistent with the Fourth Amendment.

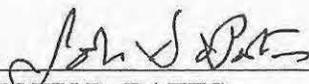
IV. CONCLUSION

For the foregoing reasons, the Court finds that the certifications and amendments submitted in the above-captioned dockets pursuant to Section 1881a(g) contain all the required elements and that the targeting and minimization procedures adopted in accordance with Section 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment.

Orders approving the certifications, the amendments, and the use of the accompanying procedures are being entered contemporaneously herewith.

ENTERED this 20th day of September 2012, in Docket Nos. b(1) and b(3)

[REDACTED]



JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

b(6), b(7)(C)

~~TOP SECRET//SI//ORCON,NOFORN~~

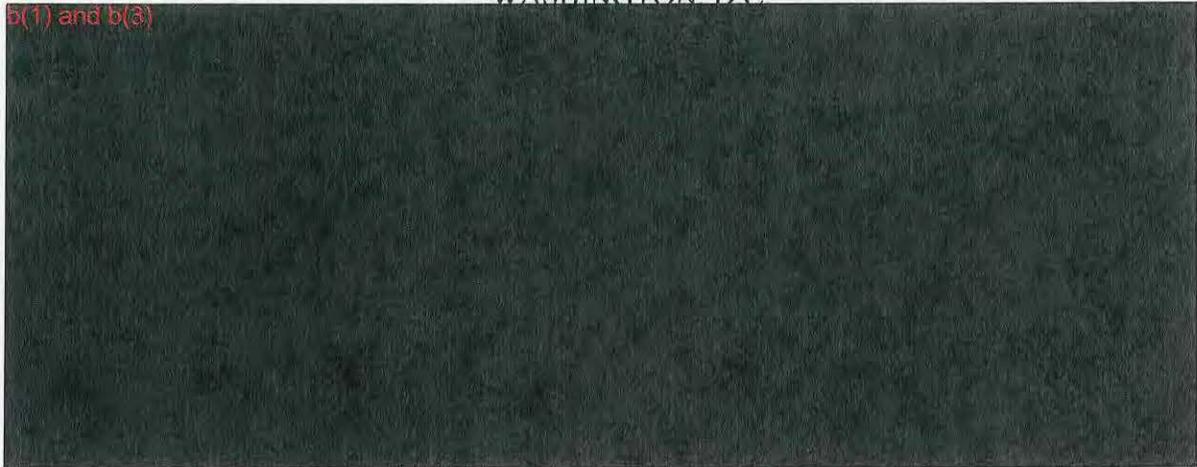
~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

b(1) and b(3)



ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications referenced above contain all the required elements and that the targeting procedures and minimization procedures approved for use in connection with those certifications are consistent with 50 U.S.C. §1881a(d)-(e) and with the Fourth Amendment.

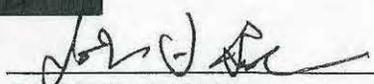
Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications and the use of such procedures are approved.

ENTERED this 20th day of September 2012, at 09-20-2012 P05:56 Eastern Time, in

Docket Nos.

b(1) and b(3)





JOHN D. BATES

Judge, United States Foreign
Intelligence Surveillance Court

b(6), b(7)(C)

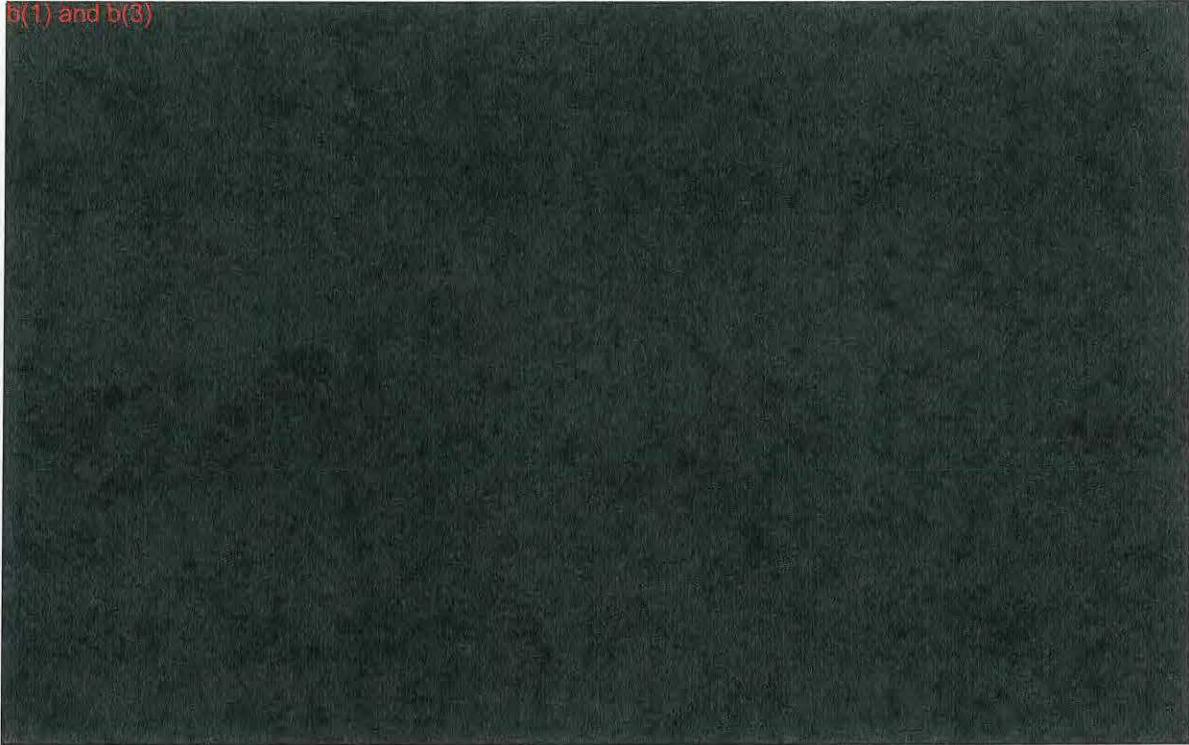


~~SECRET~~

~~SECRET~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

b(1) and b(3)



ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications referenced above, as amended on August 23, 2012, contain all the required elements and that the targeting procedures and minimization procedures approved for use in connection with those amended certifications are consistent with the requirements of 50 U.S.C. §1881a(d)-(e) and with the Fourth Amendment.

~~SECRET~~

~~SECRET~~

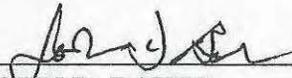
Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the amended certifications and the use of such procedures are approved.

09-20-2012 P05:56

ENTERED this 25th day of September 2012, at _____ Eastern Time, in

Docket Nos.

b(1) and b(3)
[Redacted]



JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

b(6), b(7)(C)
[Redacted]

~~SECRET~~

Exhibit 29

~~TOP SECRET//SI//ORCON/NOFORN~~
United States Foreign
Intelligence Surveillance Court

APR 26 2017

LeeAnn Flynn Hall, Clerk of Court

~~TOP SECRET//SI//ORCON/NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.



MEMORANDUM OPINION AND ORDER

These matters are before the Foreign Intelligence Surveillance Court (“FISC” or “Court”) on the “Government’s Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications,” which was filed on September 26, 2016 (“September 26, 2016 Submission”), and the “Government’s Ex Parte Submission of Amendments to DNI/AG 702(g) Certifications and Ex Parte Submission of Amended Targeting and Minimization Procedures,” which was filed on March 30, 2017 (“March 30, 2017 Submission”). (Collectively, the September 26, 2016 and March 30, 2017 Submissions will be

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

referred to herein as the “2016 Certification Submissions.”) For the reasons explained below, the government’s request for approval of the certifications and procedures accompanying the September 26, 2016 Submission, as amended by the March 30, 2017 Submission, is granted, subject to certain reporting requirements. The Court’s approval of the amended certifications and accompanying targeting and minimization procedures is set out in separate orders, which are being entered contemporaneously herewith.

I. BACKGROUND

A. The Initial 2016 Certifications

The September 26, 2016 Submission included [REDACTED] certifications that were executed by the Attorney General (“AG”) and the Director of National Intelligence (“DNI”) pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA” or “the Act”), which is codified at 50 U.S.C. § 1881a [REDACTED]

[REDACTED] Each of the [REDACTED] certifications submitted in September (collectively referred to as “the Initial 2016 Certifications”) was accompanied by the supporting affidavits of the Director of the National Security Agency (“NSA”), the Director of the Federal Bureau of Investigation (“FBI”), the Director of the Central Intelligence Agency (“CIA”), and the Director of the National Counterterrorism Center (“NCTC”); two sets of targeting procedures, for use by the NSA and FBI respectively;¹ and four sets of minimization procedures, for use by the

¹ The targeting procedures for each of the Initial 2016 Certifications are identical. The
(continued...)

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

NSA, FBI, CIA, and NCTC respectively.² The September 26, 2016 Submission also included an explanatory memorandum prepared by the Department of Justice (“DOJ”) (“September 26, 2016 Memorandum”).

The Court was required to complete its review of the Initial 2016 Certifications within 30 days of their submission, i.e., by October 26, 2016. See 50 U.S.C. § 1881a(i)(1)(B). The Court may extend this period, however, “as necessary for good cause in a manner consistent with national security.” See 50 U.S.C. § 1881a(j)(2). The Court has issued two such extensions in these matters.

¹(...continued)

targeting procedures for the NSA (“NSA Targeting Procedures”) appear as Exhibit A to each of the 2016 Certifications and the March 30, 2017 Submission includes identical amendments to those procedures for each of the certifications. (Unless otherwise specified, references to those targeting procedures shall refer to the procedures as amended, as discussed below, in the March 30, 2017 Submission.) The targeting procedures for the FBI (“FBI Targeting Procedures”) appear as Exhibit C to each of the 2016 Certifications and are not amended by the March 30, 2017 Submission.

² The minimization procedures for each of the Initial 2016 Certifications are identical. The minimization procedures for the NSA (“NSA Minimization Procedures”) appear as Exhibit B to each of the 2016 Certifications and the March 30, 2017 Submission includes identical amendments to those procedures for each of the certifications. (Unless otherwise specified, references to those minimization procedures shall refer to the procedures as amended, as discussed below, in the March 30, 2017 Submission.) The minimization procedures for the FBI (“FBI Minimization Procedures”) appear as Exhibit D to each of the 2016 Certifications. The minimization procedures for the CIA (“CIA Minimization Procedures”) appear as Exhibit E to each of the 2016 Certifications. The minimization procedures for the NCTC (“NCTC Minimization Procedures”) appear as Exhibit G to each of the 2016 Certifications. The minimization procedures for the FBI, CIA, and NCTC are not amended by the March 30, 2017 Submission.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

On October 24, 2016, the government orally apprised the Court of significant non-compliance with the NSA's minimization procedures involving queries of data acquired under Section 702 using U.S. person identifiers. The full scope of non-compliant querying practices had not been previously disclosed to the Court. Two days later, on the day the Court otherwise would have had to complete its review of the certifications and procedures, the government made a written submission regarding those compliance problems, see October 26, 2016, Preliminary and Supplemental Notice of Compliance Incidents Regarding the Querying of Section 702-Acquired Data ("October 26, 2016 Notice"), and the Court held a hearing to address them. The government reported that it was working to ascertain the cause(s) of those compliance problems and develop a remedial plan to address them. Without further information about the compliance problems and the government's remedial efforts, the Court was not in a position to assess whether the minimization procedures accompanying the Initial 2016 Certifications, as they would be implemented, would comply with statutory standards and were consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A)-(B). Accordingly, the Court found good cause to extend the time limit for its review of the Initial 2016 Certifications through January 31, 2017, and, based on the government's representations, found that such extension was consistent with national security.³ See Docket Nos [REDACTED]

[REDACTED] Order entered on Oct. 26, 2016 ("October 26, 2016 Order").

³ By operation of the statute, the predecessors to each of the Initial 2016 Certifications and the procedures accompanying them remained in effect during the extended periods for the Court's consideration of the 2016 Certifications. See 50 U.S.C. § 1881a(i)(3)(A)-(B).

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

On January 3, 2017, the government made a further submission describing its efforts to ascertain the scope and causes of those compliance problems and discussing potential solutions to them. See January 3, 2017, Supplemental Notice of Compliance Incidents Regarding the Querying of Section 702-Acquired Data (“January 3, 2017 Notice”). The Court was not satisfied that the government had sufficiently ascertained the scope of the compliance problems or developed and implemented adequate solutions for them and communicated a number of questions and concerns to the government. The government submitted another update on January 27, 2017, in which it informed the Court that, due to the complexity of the issues involved, NSA would not be in a position to provide thorough responses to the Court’s questions and concerns by January 31, 2017. See January 27, 2017, Letter In re: DNI/AG 702(g) Certifications [REDACTED] and their Predecessor Certifications (“January 27, 2017 Letter”). The government submitted that a further extension, through May 26, 2017, was necessary for it to address those issues and that such extension would be consistent with national security. The Court granted a shorter extension, through April 28, 2017, for reasons stated in its order approving the extension. See Docket Nos. [REDACTED] Order entered on Jan. 27, 2017 (“January 27, 2017 Order”).

B. The 2017 Amendments

On March 30, 2017, the Attorney General and Director of National Intelligence, acting pursuant to 50 U.S.C. § 1881a(i)(1)(C), executed Amendments to each of the [REDACTED] Initial 2016 Certifications. See Amendment to [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]

(collectively, the “2017 Amendments”).⁴ As discussed below, those amendments substantially change how NSA will conduct certain aspects of Section 702 collection, and largely resolve the compliance problems mentioned above. The March 30, 2017 Submission included the 2017 Amendments, a revised supporting affidavit by the Director of NSA, and revised targeting and minimization procedures for NSA, which replace Exhibits A and B, respectively, to each of the Initial 2016 Certifications. That submission also included an explanatory memorandum prepared by DOJ (“March 30, 2017 Memorandum”).

C. Subject Matter of the Certifications

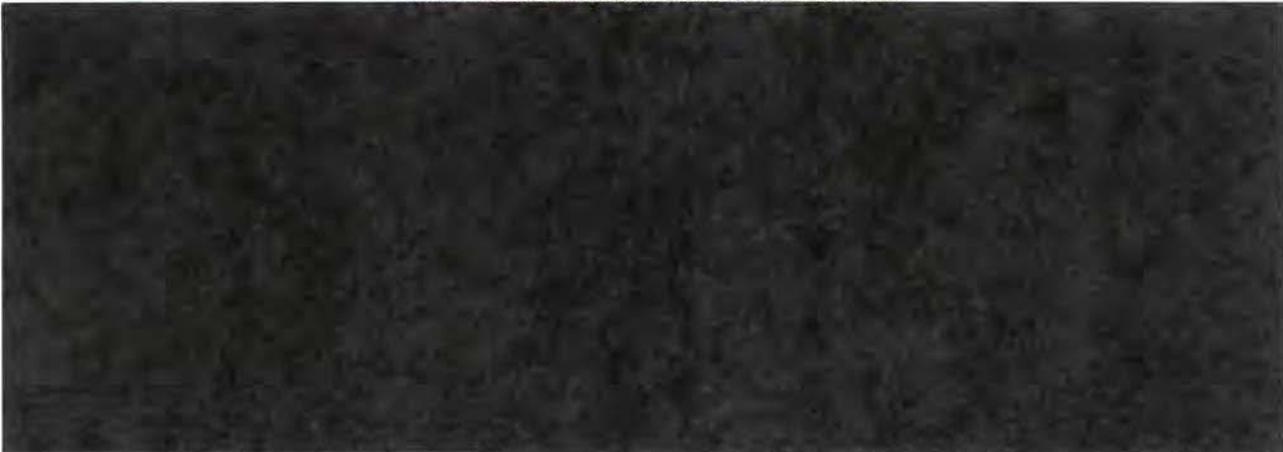
Each of the 2016 Certifications involves “the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information.”

[REDACTED]

⁴ Unless otherwise stated, subsequent references to the “2016 Certifications” are to the Initial 2016 Certifications and accompanying procedures, as later amended by the 2017 Amendments and the accompanying revised procedures.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~



Each of the 2016 Certifications generally proposes to continue acquisitions of foreign intelligence information that are now being conducted under the corresponding certification made in 2015 (“the 2015 Certifications”). See September 26, 2016 Memorandum at 2. The 2015 Certifications, which are similarly differentiated by subject matter and [REDACTED] [REDACTED] were approved by the FISC on November 6, 2015.⁵ The 2015 Certifications, in turn, generally renewed authorizations to acquire foreign intelligence information under a series of certifications made by the AG and DNI pursuant to Section 702 that dates back to 2008.⁶ The government also seeks approval of amendments to the certifications in the Prior 702 Dockets, such that the NSA, CIA, FBI and NCTC henceforward will apply the same minimization

⁵ See Docket Nos. [REDACTED] Memorandum Opinion and Order entered on Nov. 6, 2015 (“November 6, 2015 Opinion”). The Court issued an order on November 9, 2015, approving amendments to prior Section 702 certifications and authorizing the use of revised minimization procedures in connection with those certifications.

⁶ See Docket Nos. [REDACTED]

[REDACTED] These dockets, together with Docket Numbers [REDACTED] are collectively referred to as “the Prior 702 Dockets.”

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

procedures to information obtained under prior certifications as they will to information to be obtained under the 2016 Certifications. See September 26, 2016 Memorandum at 2-3;

[REDACTED]

This practice, long approved by the FISC, has the advantage of applying a single set of updated procedures to Section 702-acquired information rather than requiring personnel to follow different rules for information acquired on different dates.

D. Review of Compliance Issues

The Court's review of targeting and minimization procedures under Section 702 is not confined to the procedures as written; rather, the Court also examines how the procedures have been and will be implemented. See, e.g., Docket No. [REDACTED], Memorandum Opinion entered on Apr. 7, 2009, at 22-24 ("April 7, 2009 Opinion"); Docket Nos. [REDACTED] [REDACTED] Memorandum Opinion entered on Aug. 30, 2013, at 6-11 ("August 30, 2013 Opinion"). Accordingly, for purposes of its review of the 2016 Certifications, the Court has examined quarterly compliance reports submitted by the government since the most recent FISC review of Section 702 certifications and procedures was completed on November 6, 2015,⁷ as well as individual notices of non-compliance relating to implementation of Section 702. The Court held a hearing on October 4, 2016, to address certain issues raised by the September 26,

⁷ See Quarterly Reports to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on December 18, 2015, March 18, 2016, June 17, 2016, September 16, 2016, December 16, 2016 and March 17, 2017. These reports are cited herein in the form "[Date] Compliance Report."

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

2016 Submission, as well as certain compliance issues regarding the government's collection and handling of information under prior certifications ("October 4, 2016 Hearing").⁸ The Court held a further hearing on October 26, 2016, to address matters raised in the October 26, 2016 Notice ("October 26, 2016 Hearing").⁹

II. REVIEW OF CERTIFICATIONS [REDACTED] AND OF THEIR PREDECESSOR CERTIFICATIONS AS AMENDED BY THE SEPTEMBER 26, 2016 AND MARCH 30, 2017 SUBMISSIONS

The Court must review a certification submitted pursuant to Section 702 "to determine whether [it] contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). The Court's examination of Certifications [REDACTED] as amended by the 2017 Amendments, confirms that:

(1) the certifications have been made under oath by the AG and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see [REDACTED]

(2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see [REDACTED]

(3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures and minimization procedures;

⁸ See generally Transcript of Proceedings Held Before the Honorable Rosemary M. Collyer on October 4, 2016 ("October 4, 2016 Transcript").

⁹ See generally Transcript of Proceedings Held Before the Honorable Rosemary M. Collyer on October 26, 2016 ("October 26, 2016 Transcript").

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

(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);¹⁰ and

(5) each of the certifications includes an effective date for the authorization in compliance with 50 U.S.C. § 1881a(g)(2)(D) – specifically, the certifications become effective on April 28, 2017, or on the date upon which this Court issues an order concerning the certifications under Section 1881a(i)(3), whichever is sooner, see [REDACTED]

¹¹

The Court therefore finds that [REDACTED]

[REDACTED] contain all the required statutory elements. See 50 U.S.C. § 1881a(i)(2)(A).

Similarly, the Court has reviewed the certifications in the Prior 702 Dockets, as amended by the 2016 Certifications, and finds that they also contain all the elements required by the statute. Id.¹²

¹⁰ See Affidavits of Admiral Michael S. Rogers, United States Navy, Director, NSA; Affidavits of James B. Comey, Director, FBI; Affidavits of John O. Brennan, Director, CIA; and Affidavits of Nicholas Rasmussen, Director, NCTC, which are appended to each of Certifications [REDACTED]. Admiral Rogers filed amended affidavits in connection with the March 30, 2017 Submission.

¹¹ 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).

¹² The effective dates for the amendments to the certifications in the Prior 702 Dockets are the same as the effective dates for the 2016 Certifications. See [REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

III. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is also required, pursuant to 50 U.S.C. § 1881a(i)(2)(B) and (C), 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). Pursuant to 50 U.S.C. § 1881a(i)(3)(A), the Court further assesses whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

A. Statutory Standards for Targeting Procedures

Section 1881a(d)(1) requires targeting procedures that are “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.” In addition to these statutory requirements, the government uses the targeting procedures as a means of complying with Section 1881a(b)(3), which provides that acquisitions “may not intentionally target a United States person reasonably believed to be located outside the United States.” The FISC considers steps taken pursuant to these procedures to avoid targeting United States persons as relevant to its assessment of whether the procedures are consistent with the requirements of the Fourth Amendment. See Docket No. 702(i)-08-01, Memorandum Opinion entered on Sept. 4, 2008, at 14 (“September 4, 2008 Opinion”).

Under the procedures adopted by the government, NSA is the lead agency in making targeting decisions under Section 702. Pursuant to its targeting procedures, NSA may target for

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

acquisition a particular “selector,” which is typically a facility such as a telephone number or e-mail address. The FBI Targeting Procedures come into play in cases where [REDACTED] [REDACTED] that has been tasked under the NSA Targeting Procedures. See FBI Targeting Procedures § I.1. “Thus, the FBI Targeting Procedures apply in addition to the NSA Targeting Procedures, whenever [REDACTED] acquired.” September 4, 2008 Opinion at 20 (emphasis in original). Proposed changes to the existing NSA and FBI targeting procedures are discussed below.

B. Statutory Standards for Minimization Procedures

Section 1881a(e)(1), in turn, requires minimization procedures that “meet the definition of minimization procedures under [50 U.S.C. §] 1801(h) or 1821(4).” Sections 1801(h) and 1821(4) define “minimization procedures” in pertinent part as:

(1) 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;[¹³]

¹³ Section 1801(e) defines “foreign intelligence information” as

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of

(continued...)

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]

50 U.S.C. § 1801(h); see also id. § 1821(4).¹⁴ Each agency having access to “raw,” or unminimized,¹⁵ information obtained under Section 702 is governed by its own set of

¹³(...continued)

weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or a foreign territory that relates to, and if concerning a United States person is necessary to –

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

¹⁴ The definitions of “minimization procedures” set forth in these provisions are substantively identical (although Section 1821(4)(A) refers to “the purposes . . . of the particular physical search”). For ease of reference, subsequent citations refer only to the definition set forth at Section 1801(h).

¹⁵ This opinion uses the terms “raw” and “unminimized” interchangeably. The proposed NCTC Minimization Procedures define “raw” information as “section 702-acquired information that (i) is in the same or substantially the same format as when NSA or FBI acquired it, or (ii) has been processed only as necessary to render it into a form in which it can be evaluated to

(continued...)

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

minimization procedures in its handling of Section 702 information. Under Section 1881a(i)(2)(C), the Court must determine whether the agencies' respective minimization procedures meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) or 1821(4), as appropriate.

The most significant changes to the procedures proposed by the government in connection with the 2016 Certifications relate to: (i) the changes in the scope of NSA collection under Section 702, as reflected in the March 30, 2017 Amendments; and (ii) the government's proposal in the September 26, 2016 Submission to allow NCTC access to unminimized information acquired by NSA and FBI [REDACTED] [REDACTED] relating to international terrorism [REDACTED].

Because those changes cut across several sets of procedures, each is discussed individually in a separate section. This opinion then examines several other changes to various sets of procedures proposed by the government in the September 26, 2016 Submission. The opinion then will assess whether, taken as a whole and including the proposed changes, the proposed targeting and minimization procedures satisfy applicable statutory and Fourth Amendment requirements.

C. Significant Changes to NSA Targeting and Minimization Procedures in the March 30, 2017 Submission

The October 26, 2016 Notice disclosed that an NSA Inspector General (IG) review and report and NSA Office of Compliance for Operations (OCO) verification activities indicated that,

¹⁵(...continued)
determine whether it reasonably appears to be foreign intelligence information or to be necessary to understand foreign intelligence information or assess its importance." NCTC Minimization Procedures § A.3.d.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

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. To understand why such queries were prohibited, and why this disclosure gave the Court substantial concern, some historical background is necessary.

1. Upstream Collection and the Acquisition of MCTs

“Upstream” collection of Internet communications refers to NSA’s interception of such communications as they transit the facilities of an Internet backbone carrier [REDACTED] [REDACTED] as distinguished from acquiring communications from systems operated by Internet service providers [REDACTED].¹⁶ Upstream Internet collection constitutes a small percentage of NSA’s overall collection of Internet communications under Section 702, *see, e.g.*, October 3, 2011 Memorandum Opinion at 23 n.21 (noting that, at that time, upstream Internet collection constituted only 9% of NSA’s Internet collection), but it has represented more than its share of the challenges in implementing Section 702.

In 2011, the government disclosed that, as part of its upstream collection of Internet transactions, NSA acquired certain “Multiple Communication Transactions” or “MCTs.”¹⁷

¹⁶ *See In re DNI/AG 702(g) Certifications* [REDACTED] [REDACTED] Memorandum Opinion, October 3, 2011 (“October 3, 2011 Memorandum Opinion”), at 5 n.3. For purposes of the discussion that follows, familiarity with that opinion is presumed. As discussed below, NSA does not share raw upstream collection (Internet or telephony) with any other agency.

¹⁷ NSA’s procedures define an Internet transaction as consisting of either a discrete communication (e.g., an individual e-mail) or multiple discrete communications obtained within (continued...)

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

MCTs might take the form of [REDACTED] containing

multiple e-mail messages [REDACTED]

[REDACTED]. See March 30, 2017 Memorandum at 8 n.8. The term “active user” refers to the user of a communication service to or from whom the MCT is in transit when it is acquired (e.g., the user of an e-mail account [REDACTED])

Eventually, as discussed below, a complicated set of minimization rules was adopted for handling different types of MCTs, based on whether the active user was the target¹⁸ and, if not, the nationality and location (to the extent known) of the active user.

Moreover, NSA upstream collection acquired Internet communications that were to, from *or about* (i.e., containing a reference to) a selector tasked for acquisition under Section 702. As a result, upstream collection could acquire an entire MCT for which the active user was a non-target and that mostly pertained to non-targets, merely because a *single* discrete communication within the MCT was to, from *or contained a reference to* a tasked selector. Such acquisitions could take place even if the non-target active user was a U.S. person in the United States and the MCT contained a large number of domestic communications¹⁹ that did not pertain to the foreign

¹⁷(...continued)
an MCT. See NSA Targeting Procedures § I, at 2 n.1; NSA Minimization Procedures § 2(g).

¹⁸ With a narrow exception for [REDACTED] all users of a selector tasked for acquisition under Section 702 are considered targets. See March 30, 2017 Memorandum at 6 n.7.

¹⁹ In this opinion, “domestic communications” are communications in which the sender
(continued...)

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

intelligence target who used the tasked selector. Because of those types of acquisitions particularly, upstream Internet collection was “more likely than other forms of Section 702 collection to contain information of or concerning United States persons with no foreign intelligence value.” November 6, 2015 Opinion at 25 n.21.

It should be noted, however, that not all MCTs in which the active user is a non-target are equally problematic; for example, some MCTs within that description may involve an active user who is a non-U.S. person outside the United States, and for that reason are less likely to contain a large volume of information about U.S. persons or domestic communications.

2. The 2011 Finding of Deficiency and Measures to Remedy the Deficiency

In its October 3, 2011 Memorandum Opinion, the Court found the NSA’s minimization procedures, proffered in connection with Section 702 certifications then under consideration, statutorily and constitutionally deficient with respect to their protection of U.S. person information within certain types of MCTs. See October 3, 2011 Memorandum Opinion at 49-80. In response to the Court’s deficiency finding, the government submitted amended minimization procedures that placed significant new restrictions on NSA’s retention, use, and dissemination of MCTs. Those procedures included a sequestration regime for more problematic categories of MCTs.²⁰ A shorter retention period was also put into place, whereby an MCT of any type could not be retained longer than two years after the expiration of the certification pursuant to which it

¹⁹(...continued)
and all intended recipients are in the United States.

²⁰ This sequestration regime is discussed in Section IV below in connection with an instance of NSA’s not complying with that regime.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

was acquired, unless applicable retention criteria were met. And, of greatest relevance to the present discussion, those procedures categorically prohibited NSA analysts from using known U.S.-person identifiers to query the results of upstream Internet collection. In substantial reliance on these and other changes, the Court approved the modified procedures for acquiring and handling MCTs. See *In re DNI/AG 702(g) Certifications* [REDACTED] [REDACTED] Memorandum Opinion, November 30, 2011 (“November 30, 2011 Memorandum Opinion”).

The Court also observed that one category of MCTs presented far fewer statutory and constitutional difficulties than the others:

[I]f 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 [other] categories [of MCTs] because the communicants were in direct communication with a tasked facility, and the acquisition presumptively serves the foreign intelligence purpose of the collection.

October 3, 2011 Memorandum Opinion at 38. See also *id.* at 58 n.54 (“The government has also suggested that NSA may have limited capability, at the time of acquisition, to identify some MCTs as to which the “active user” is a tasked selector. To the extent that NSA is able to do so, such acquisitions *would be consistent with FISA and the Fourth Amendment* because all discrete communications within this class of MCTs would consist of communications to or from a tasked selector.”) (internal citation omitted, emphasis added); *id.* at 80 (finding that the

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

proposed NSA procedures, although deficient as applied to other forms of MCTs, were consistent with the statute and the Fourth Amendment as applied to “MCTs as to which the ‘active user’ is known to be a tasked selector”). That point is significant to the current matters: as discussed below, the 2016 Certifications only authorize acquisition of MCTs when the active user is the target of acquisition.

3. The October 26, 2016 Notice and Hearing

Since 2011, NSA’s minimization procedures have prohibited use of U.S.-person identifiers to query the results of upstream Internet collection under Section 702. The October 26, 2016 Notice informed the Court that NSA analysts had been conducting such queries in violation of that prohibition, with much greater frequency than had previously been disclosed to the Court. The Notice described the results of an NSA IG Report which analyzed queries using a set of known U.S.-person identifiers (those associated with targets under Sections 704 and 705(b) of the Act, 50 U.S.C. §§ 1881c and 1881d(b)), during the first three months of 2015, in a subset of particular NSA systems that contain the results of Internet upstream collection. That relatively narrow inquiry found that ■ analysts had made ■ separate queries using ■ U.S.-person identifiers that improperly ran against upstream Internet data. The government reported that the NSA IG and OCO were conducting other reviews covering different time periods, with preliminary results suggesting that the problem was widespread during all periods under review.

At the October 26, 2016 hearing, the Court ascribed the government’s failure to disclose those IG and OCO reviews at the October 4, 2016 hearing to an institutional “lack of candor” on NSA’s part and emphasized that “this is a very serious Fourth Amendment issue.” October 26,

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

2016 Transcript at 5-6. The Court found that, in light of the recent revelations, it did not have sufficient information to assess whether the proposed minimization procedures accompanying the Initial 2016 Certifications would comply with statutory and Fourth Amendment requirements, as implemented. Based on the government's representation that an extension of time through January 31, 2017, would provide the government sufficient opportunity to assess and report on the scope of the problem and an appropriate remedial plan, and was consistent with the national security, the Court extended the time period for its consideration of the 2016 Certifications to that date.

4. The January 3, 2017 Supplemental Notice and January 27, 2017 Letter

In anticipation of the January 31 deadline, the government updated the Court on these querying issues in the January 3, 2017 Notice. That Notice indicated that the IG's follow-on study (covering the first quarter of 2016) was still ongoing. A separate OCO review, limited in many of the same ways as the IG studies, and covering the periods of April through December 2015 and April through July of 2016, found that some [REDACTED] improper queries were conducted by [REDACTED] analysts during those periods.²¹ The January 3, 2017 Notice stated that "human error was the primary factor" in these incidents, but also suggested that system design issues contributed. For

²¹ NSA further reported that OCO reviewed queries involving a number of identifiers for known U.S. persons who were not targets under Sections 704 or 705(b) of the Act, and which were associated with "certain terrorism-related events that had occurred in the United States." January 3, 2017 Notice at 6. NSA OCO found [REDACTED] such queries, [REDACTED] of which improperly ran against Section 702 upstream Internet data. [REDACTED] of the improper queries were run in a system called [REDACTED] which NSA analysts use to [REDACTED] [REDACTED] of a current or prospective target of NSA collection, including under Section 702. *Id.* at 6-7.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

example, some systems that are used to query multiple datasets simultaneously required analysts to “opt-out” of querying Section 702 upstream Internet data rather than requiring an affirmative “opt-in,” which, in the Court’s view, would have been more conducive to compliance. See January 3, 2017 Notice at 5-6. It also appeared that NSA had not yet fully assessed the scope of the problem: the IG and OCO reviews “did not include systems through which queries are conducted of upstream data but that do not interface with NSA’s query audit system.” Id. at 3 n.6. Although NSD and ODNI undertook to work with NSA to identify other tools and systems in which NSA analysts were able to query upstream data, id., and the government proposed training and technical measures, it was clear to the Court that the issue was not yet fully scoped out.

On January 27, 2017, the government provided further information on the technical and training measures NSA was taking and proposed to take to address this issue. NSA was implementing its technical measures only on systems with respect to the system thought to be used most frequently to query Section 702 data. The government still had not ascertained the full range of systems that might have been used to conduct improper U.S.-person queries. See, e.g., January 27, 2017 Letter at 5 (“NSA is progressing with its efforts to identify other tools or systems that analysts are using to query upstream data.”). The government also reported that the NSA IG study for the first quarter of 2016 had found ■ improper queries, a substantial

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

improvement over the first quarter of 2015.²² But NSA was still working to determine the scope of its U.S.-person query problem and to identify all relevant storage systems and querying tools.

The January 27, 2017 Letter concluded that, “[b]ased on the complexity of the issues, NSA will not be in a position to provide thorough responses [to the Court’s questions] on or before January 31, 2017.” January 27, 2017 Letter. The government represented that a further extension of the Court’s time to consider the 2016 Certifications through May 26, 2017, would be consistent with the national security and would allow the government time to investigate and remedy the problem.

The Court granted an extension only through April 28, 2017.²³ January 27, 2017 Order at 6. In doing so, the Court noted its concern about the extent of non-compliance with “important safeguards for interests protected by the Fourth Amendment.” *Id.* at 5. The Court also observed that, while recent remedial measures appeared promising, they were being implemented only on certain systems, while other systems remained to be assessed. *Id.* at 5-6.

On March 17, 2017, the government reported that NSA was still attempting to identify all systems that store upstream data and all tools used to query such data, though that effort was nearly complete. March 17, 2017 Compliance Report at 100. NSA had also redoubled training on querying requirements and made technical upgrades to certain commonly-used querying tools

²² In addition to the findings of the IG and OCO reviews, the government identifies improper queries in the course of regular oversight efforts. The government reports those incidents to the Court through individual notices and quarterly reports.

²³ By operation of Section 1881a(i)(1)(B), the government’s submission on March 30, 2017, of amendments to the 2016 Certifications and revised procedures started a new 30-day period for Court review, which ends on April 29, 2017.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

that were designed to reduce the likelihood of non-compliant queries. *Id.* at 100-101.

Meanwhile, the government continued to report further compliance issues regarding the handling and querying of upstream Internet collection²⁴ and to investigate potential root causes of non-compliant querying practices. April 7, 2017 Preliminary Notice (Queries) at 4 n.4.

5. The 2017 Amendments

As embodied in the March 30, 2017 Submission, the government has chosen a new course: [REDACTED]; sequestering and then destroying raw upstream Internet data previously collected; and substantially narrowing the scope of upstream collection [REDACTED]. Most significantly, the government will eliminate “abouts” collection altogether, which will have the effect of eliminating acquisition of the more problematic types of MCTs. These changes should substantially reduce the acquisition of non-pertinent information concerning U.S. persons pursuant to Section 702.

As of March 17, 2017, NSA had [REDACTED]

[REDACTED]. Revisions to the NSA Minimization Procedures now state that all Internet transactions acquired on or before that date and existing in NSA’s institutionally managed

²⁴ See April 7, 2017, Preliminary Notice of Compliance Incidents Regarding the Labeling and Querying of Section 702-Acquired Data (“April 7, 2017 Preliminary Notice (Mislabeling)”) (nearly [REDACTED] communications acquired through upstream Internet collection were “incorrectly labeled” as acquired from Internet service providers and, as a result, likely subject to prohibited queries using U.S.-person identifiers); April 7, 2017, Preliminary Notice of Potential Compliance Incidents Regarding Improper Queries (“April 7, 2017 Preliminary Notice (Queries)”) (identifying another [REDACTED] potential violations of prohibition on using U.S.-person identifiers to query Internet upstream collection).

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

repositories²⁵ will be sequestered pending destruction such that “NSA personnel will not be able to access the[m] for analytical purposes.” March 30, 2017 Memorandum at 4; see NSA Minimization Procedures §3(b)(4)a.

NSA will destroy such sequestered Internet transactions as soon as practicable through an accelerated age-off process. See NSA Minimization Procedures §3(b)(4)a. The government represents that the age-off may take up to one year to complete and verify (with quarterly reports to the Court), and that:

- Pending destruction, sequestered transactions (a) will not be subject to separate age-off or purge processes that otherwise would apply to them, see March 30, 2017 Memorandum at 15-16 & nn. 16-17; and (b) will be available only to NSA technical and compliance personnel for the limited purposes of ensuring the integrity of the systems used to store them and the controls that limit other employees’ access to them, see id. at 14 n.13; NSA Minimization Procedures §3(b)(4)a.
- Copies of sequestered transactions will remain in backup and archive systems, not available for use by intelligence analysts, until they age off of those systems in the ordinary course. See March 30, 2017 Memorandum at 14 n.13;
- Sequestered transactions may be retained for litigation purposes as contemplated by Section 3(c)(3) of the NSA Minimization Procedures, subject to prompt notification to the Court. See id. at 16-17 & n.18.
- Certain records derived from upstream Internet communications (many of which have been evaluated and found to meet retention standards) will be retained by NSA, even though the underlying raw Internet transactions from which they are

²⁵ The March 30, 2017 Submission does not define what an “institutionally managed repository” is. If the government intends not to apply the above-described sequester-and-destroy process to any information acquired on or before March 17, 2017, by Internet upstream collection because the information is not contained in an “institutionally managed repository,” it shall describe the relevant circumstances in a written submission to be made no later than June 2, 2017; however, the government need not submit such a description for circumstances referenced in this Opinion and Order as ones in which NSA may retain such information.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

derived might be subject to destruction. These records include serialized intelligence reports and evaluated and minimized traffic disseminations; completed transcripts and transcriptions of Internet transactions; [REDACTED]; [REDACTED];²⁶ information used to support Section 702 taskings and FISA applications to this Court; and [REDACTED].²⁷ See March 30, 2017 Memorandum at 20-24.

Finally, upstream collection of Internet transactions [REDACTED]

[REDACTED] for communications to or from a targeted person, but “abouts” communications may no longer be acquired. The NSA Targeting Procedures are amended to state that “[a]cquisitions conducted under these procedures will be limited to communications *to or from* persons targeted in accordance with these procedures,” NSA Targeting Procedures § I, at 2 (emphasis added), and NSA’s Minimization Procedures now state that Internet transactions acquired after March 17, 2017, “that are not to or from a person targeted in accordance with NSA’s section 702 targeting procedures are unauthorized acquisitions and therefore will be destroyed upon recognition.” NSA Minimization Procedures § 3(b)(4)b.²⁸ Because they are regarded as unauthorized, the government will report any acquisition of such communications to the Court as an incident of non-compliance. See March 30, 2017 Memorandum at 17-18.

²⁶ [REDACTED] See NSA Targeting Procedures § I at 6.

²⁷ [REDACTED] March 30, 2017 Memorandum at 23.

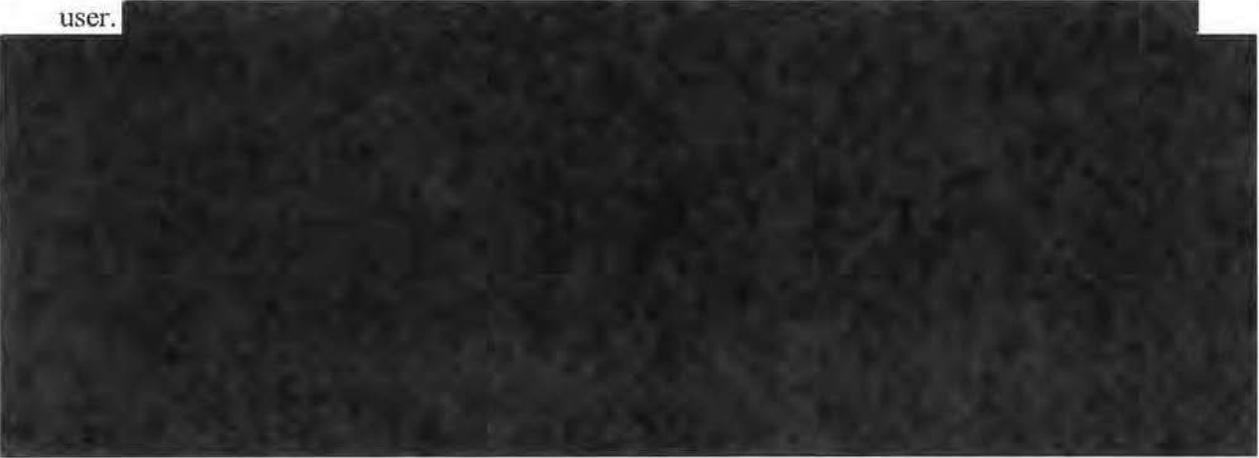
²⁸ The targeting procedures still require NSA either to use Internet Protocol (IP) filtering of upstream Internet collection to “limit such acquisitions to Internet transactions that originate and/or terminate outside the United States” or [REDACTED] Id.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

Conforming changes are made throughout the NSA Minimization Procedures to remove references to “abouts” collection. Section 3(b)(4) of those procedures, in particular, is significantly revised and streamlined to reflect the narrower scope of authorized collection. For example, detailed procedures previously appearing in Section 3(b)(4) requiring sequestration and special handling of MCTs in especially problematic categories (e.g., those in which the “active user” is a non-target who is in the United States or whose location is unknown) are removed. Because NSA is no longer authorized to acquire those forms of MCTs, if it somehow acquires one, NSA must now destroy it upon recognition.²⁹

NSA may continue to acquire MCTs under the amended procedures, but only when it can ensure that the target is a party to the entire MCT or, in other words, when the target is the active user.



²⁹ Internet transactions properly acquired through NSA upstream collection after March 17, 2017, will continue to remain subject to a two-year retention limit, “unless the NSA specifically determines that at least one discrete communication within the Internet transaction meets the retention standards” in the NSA Minimization Procedures. See NSA Minimization Procedures § 3(c)(2). This reflects no change from the current procedures.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]³⁰ See March 30, 2017

Memorandum at 10.

It will still be possible, however, for NSA to acquire an MCT that contains a domestic communication. For example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] If NSA determines that the sender and all intended recipients of a discrete communication within an MCT were located in the United States at the time of that discrete communication, then the entire MCT must be promptly destroyed, see NSA Minimization Procedures § 5, unless the Director makes the required waiver determination for each and every domestic communication contained in the MCT. March 30, 2017 Memorandum at 9 n.9.³¹

U.S.-Person Queries. In light of the elimination of “abouts” communications from Section 702 upstream collection, the government proposes a change to Section 3(b)(5) of the NSA Minimization Procedures that would remove the prohibition on NSA analysts conducting

³⁰ This enumeration is without prejudice to NSA’s ability to acquire other types of communications if it can limit acquisition to communications to or from a target as required by the new procedures.

³¹ The NSA Minimization Procedures generally take an “all-or-nothing” approach to retention or destruction of MCTs. Thus, an MCT in which *any* discrete communication is not to or from a target is also subject to destruction in its entirety. See NSA Minimization Procedures § 3(b)(4)b; March 30, 2017 Memorandum at 13 n.12 (“[I]f for some reason NSA acquires an Internet transaction in which any discrete communication contained therein is not to or from a section 702 target, NSA must destroy such transactions upon recognition.”).

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

queries of Internet upstream data using identifiers of known U.S. persons. Under this proposal, NSA analysts could query upstream data using known U.S. person identifiers, subject to the same requirements that apply to their queries of other Section 702-acquired data. Specifically, any query involving a U.S.-person identifier is subject to NSA internal approval requirements and “require[s] a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information.” NSA is required to maintain records of all such determinations and those records are subject to review by NSD and ODNI. See NSA Minimization Procedures § 3(b)(5).³²

The Court agrees that the removal of “abouts” communications eliminates the types of communications presenting the Court the greatest level of constitutional and statutory concern. As discussed above, the October 3, 2011 Memorandum Opinion (finding the then-proposed NSA Minimization Procedures deficient in their handling of some types of MCTs) noted that MCTs in which the target was the active user, and therefore a party to all of the discrete communications within the MCT, did not present the same statutory and constitutional concerns as other MCTs. The Court is therefore satisfied that queries using U.S.-person identifiers may now be permitted to run against information obtained by the above-described, more limited form of upstream Internet collection, subject to the same restrictions as apply to querying other forms of Section

³² The Court understands that DOJ and ODNI review all U.S.-person identifiers approved for use in querying contents of Section 702-acquired communications as well as the written documentation of the foreign intelligence justifications for each such query during bi-monthly compliance reviews. See November 6, 2015 Opinion at 25 n.22.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

702-acquired data.³³ See generally October 3, 2011 Memorandum Opinion at 22-24 (finding that addition of a provision allowing NSA to query non-upstream Internet transactions using U.S. person identifiers was consistent with the statute and the Fourth Amendment); November 6, 2015 Opinion at 24-26 (after inviting views of amicus curiae on this issue, finding that the CIA and NSA minimization procedures permitting such queries comported with the statute and the Fourth Amendment).

The Court concludes that, taken as a whole, these changes strengthen the basis for finding that the NSA Targeting Procedures meet the requirements of Section 1881a(d)(1) and that the NSA Minimization Procedures meet the definition of such procedures in Section 1801(h). The elimination of “abouts” collection and, consequently, the more problematic forms of MCTs, focuses Section 702 acquisitions more sharply on communications to or from Section 702 targets, who are reasonably believed to be non-U.S. persons outside the United States and expected to receive or communicate foreign intelligence information. That sharper focus should have the effect that U.S. person information acquired under Section 702 will come more

³³ Of course, NSA still needs to take all reasonable and necessary steps to investigate and close out the compliance incidents described in the October 26, 2016 Notice and subsequent submissions relating to the improper use of U.S.-person identifiers to query terms in NSA upstream data. The Court is approving on a going-forward basis, subject to the above-mentioned requirements, use of U.S.-person identifiers to query the results of a narrower form of Internet upstream collection. That approval, and the reasoning that supports it, by no means suggest that the Court approves or excuses violations that occurred under the prior procedures.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

predominantly from non-domestic communications that are relevant to the foreign intelligence needs on which the pertinent targeting decisions were based.³⁴

D. NCTC Raw Take Sharing

1. Sharing of Unminimized Information Acquired Under [REDACTED] with NCTC

The September 26, 2016 Submission proposes for the first time to allow NCTC access to unminimized information acquired by NSA and FBI pursuant to [REDACTED]

[REDACTED] Previously, NCTC only had access to minimized Section 702-acquired information residing in FBI's general indices and relating to certain categories of investigations concerning international terrorism. NCTC has not, and will not under the government's proposal, engage in FISA collection of its own. It does, however, have significant experience with handling FISA-acquired information, including unminimized information obtained pursuant to Titles I and III and Sections 704 and 705(b) of the Act, pursuant to AG- and FISC-approved minimization procedures.

Beginning in 2008, NCTC was authorized to receive certain FISA-derived information from terrorism cases that FBI had uploaded into its Automated Case Support ("ACS") system. FISA information residing in ACS has been minimized by FBI and appears in investigative

³⁴ When the Court approved the prior, broader form of upstream collection in 2011, it did so partly in reliance on the government's assertion that, due to [REDACTED] some communications of foreign intelligence interest could only be acquired by such means. See October 3, 2011 Memorandum Opinion at 31 & n. 27, 43, 57-58. This Opinion and Order does not question the propriety of acquiring "abouts" communications and MCTs as approved by the Court since 2011, subject to the rigorous safeguards imposed on such acquisitions. The concerns raised in the current matters stem from NSA's failure to adhere fully to those safeguards.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

reports and other work product. The FISC in 2008 found that NCTC's access to such information in ACS was "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information" under 50 U.S.C. § 1801(h)(1). Docket No. [REDACTED], Memorandum Opinion and Order entered on Oct. 8, 2008, at 3-6. Later, in 2012, NCTC was granted access to raw information from terrorism cases obtained under Titles I and III and Sections 704 and 705(b) of the Act, subject to expanded minimization procedures. See Docket Nos. [REDACTED], Memorandum Opinion and Order entered on May 18, 2012 ("May 18, 2012 Opinion").

NCTC also has experience handling information obtained under Section 702 of the Act. Since 2012, NCTC has had access to minimized information obtained under Section 702 through its access to certain case categories in FBI's general indices (including ACS and another system known as Sentinel). See Docket Nos. [REDACTED], Memorandum Opinion entered on Sept. 20, 2012, at 22-25 ("September 20, 2012 Opinion").

In each instance in which the FISC has authorized expanded sharing of FISA-acquired information with NCTC, the FISC has recognized NCTC's role as the government's primary organization for analyzing and integrating all intelligence pertaining to international terrorism and counterterrorism. For example, in approving NCTC's access to minimized Section 702-acquired information in FBI general indices in 2012, the FISC observed that NCTC was statutorily charged with ensuring that intelligence agencies receive all-source intelligence support and that executive and legislative branch officials have access to international terrorism-related intelligence information and analysis to meet their constitutional responsibilities. See id. at 23

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

(citing then-applicable statutory provisions); see also Affidavits of Nicholas Rasmussen, Director, NCTC, appended at Tab 5 to each of the 2016 Certifications, at 1. The government further avers in support of the current proposal that: (1) NCTC is statutorily charged with providing “strategic operational plans for the civilian and military counterterrorism intelligence and operations across agency boundaries, both inside and outside the United States;” and (2) the NCTC Director “is assigned ‘primary responsibility within the United States Government for conducting net assessments of terrorist threats.’” September 26, 2016 Memorandum at 12-13 (citing 50 U.S.C. § 3056(f)(1)(B) and (G)).

The Court is satisfied that NCTC’s receipt of information acquired under [REDACTED] [REDACTED] is consistent with its mission. As for the NCTC’s need to have access to this information in raw form, the government asserts that NCTC’s ability to obtain Section 702-acquired information more quickly and in a form closer to its original, and to examine that information in NCTC systems, using its own analytical tools in the context of potentially related information available in NCTC systems, will enhance NCTC’s ability to produce counterterrorism foreign intelligence information. See September 26, 2016 Memorandum at 13-14. The government provides an example in which NCTC was able to use its access to raw FISA-acquired information from collection under other provisions of FISA to provide a timely and unique assessment that was shared with other elements of the Intelligence Community in support of their intelligence collection and analysis functions. See id. at 15. One would hope that this is one of many such examples.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

In any event, as noted above, the government's proffered rationale for sharing raw information with NCTC was accepted by the FISC in the context of information obtained under other provisions of the Act, and the Court is persuaded that it applies with equal force in the context of collection under Section 702. Among other things, the volume of collection under Section 702 militates in favor of bringing all available analytical resources to bear on the careful analysis and exploitation of foreign intelligence information from such collection. The Court also credits the assertion that time can be of the essence in many rapidly-unfolding counterterrorism investigations. The Court is persuaded that timely access to raw Section 702-acquired information will enhance NCTC's ability to perform its distinct mission, to support the activities of other elements of the Intelligence Community, and to provide valuable input to senior decisionmakers in the Executive Branch and Congress.

Moreover, the information acquired under [REDACTED] though voluminous – is the result of targeting persons reasonably believed to be non-United States persons located outside the United States. For that reason, it is unlikely to contain as high a proportion of information concerning United States persons as information acquired by FISA electronic surveillance and physical search, which often involve targets who are United States persons and typically are directed at persons in the United States.

To be sure, information concerning unconsenting United States persons has been and will continue to be acquired under Section 702 and [REDACTED] particularly. The minimization procedures must carefully regulate the government's use and dissemination of such U.S. person information in order to satisfy the definition of "minimization

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

procedures” at Section 1801(h). The procedures NCTC will be required to follow with respect to its handling of such information are examined in detail below.

The Court also finds that the scope of the proposed sharing with NCTC is appropriate. Consistent with NCTC’s mission, the proposed sharing of unminimized Section 702-acquired information is limited to [REDACTED]. The government notes that the sharing will not include telephony data or the results of upstream Internet collection; in other words, it will be limited to Internet communications obtained with the assistance of the direct providers of the communication services involved. See September 26, 2016 Memorandum at 10-11. NCTC will receive raw information [REDACTED] and subject to the same limitations as CIA (no upstream Internet collection and no telephony).

Id.

The government undertakes to notify the Court before altering these arrangements and providing raw telephony or upstream Internet data to NCTC, FBI or CIA. See id. at 11 n.7; accord March 30, 2017 Memorandum at 9-10 n.10. With regard to upstream Internet collection, the Court has determined that mere notification to the FISC would be insufficient, especially as NSA is in the process of transitioning to a narrower form of collection and segregating and destroying the results of the prior, broader collection. Accordingly, the Court is ordering that raw information obtained by NSA’s upstream Internet collection under Section 702 shall not be provided to FBI, CIA or NCTC unless it is done pursuant to revised minimization procedures that are adopted by the AG and DNI and submitted to the FISC for review in conformance with Section 702.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

With that limitation, the Court finds that NCTC's receipt of raw information acquired under [REDACTED] subject to appropriate minimization procedures as described below, will "minimize the . . . 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).³⁵ The NCTC has followed AG- and FISC-approved minimization procedures in connection with its prior receipt of FISA-acquired information, including Section 702-acquired information, with relatively few documented instances of noncompliance. See generally Docket Nos. [REDACTED], Memorandum Opinion and Order entered on Aug. 26, 2014 Opinion ("August 26, 2014 Opinion") at 37 (noting that "no significant compliance issues have arisen under [NCTC's Section 702 minimization] procedures").

a. Changes to FBI and NSA Procedures Relating to Raw Information Sharing with NCTC

As noted above, the extension of raw information sharing to NCTC requires changes to several sets of procedures.³⁶ First, FBI's targeting procedures, and FBI and NSA's minimization procedures, are each amended to reflect the fact that those agencies may now provide to NCTC

³⁵ With regard to § 1801(h)(2)'s limitation on the dissemination of United States person identities, the Court adopts the analysis set out at pages 7-8 of the May 18, 2012 Opinion.

³⁶ Some technical, conforming edits to the certifications and procedures occasioned by the extension of raw information sharing to NCTC are not discussed herein because they raise no issues material to the Court's review. Certain other changes to the proposed certifications and procedures are not discussed for the same reason.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

unminimized communications obtained under [REDACTED] See FBI Targeting Procedures § I.6; NSA Minimization Procedures § 6(c)(3); FBI Minimization Procedures § V.E. NCTC is required to identify to NSA those individual Section 702 selectors for which it wishes to receive unminimized information, and is required to apply its own approved minimization procedures to such information. See NSA Minimization Procedures § 6(c)(3); FBI Minimization Procedures § V.E.

b. Changes to NCTC Minimization Procedures Relating to Raw Information Sharing with NCTC

The NCTC Minimization Procedures have been enhanced significantly to account for its receiving raw information under Section 702. But they are not crafted out of whole cloth. They are modeled on the previously-approved minimization procedures that apply to NCTC's receipt of information under Titles I and III and Sections 704 and 705(b) of the Act.³⁷ Modifications are proposed to address issues that are unique to Section 702 collection and in some instances to harmonize the proposed NCTC procedures with those used by the FBI, NSA, and CIA in their handling of Section 702-acquired information. Several key elements of the NCTC Minimization Procedures are discussed below, focusing on instances in which they depart from the previously approved NCTC Title I Procedures.³⁸

³⁷ For ease of reference, this opinion refers to these procedures (the "National Counterterrorism Center Standard Minimization Procedures for Information Acquired by the Federal Bureau of Investigation Pursuant to Title I, Title III, or Section 704 or 705(b) of the Foreign Intelligence Surveillance Act") as the "NCTC Title I Procedures."

³⁸ The government does not propose targeting procedures for NCTC, so NCTC will not be authorized to engage in any Section 702 collection.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

The NCTC Minimization Procedures do not have a provision restricting NCTC's processing, retention, and dissemination of third-party information. In NCTC's Title I Procedures, third-party information is defined to include "communications of individuals who are not the targets of the collection," and to exclude "any information contained in a communication to which the target is a party." NCTC Title I Procedures § A.3.h. Third-party information thus defined is subject to stricter retention, processing, and dissemination limitations under NCTC's Title I Procedures than information directly involving the target. *See id.* § C.4. In 2012, the FBI removed similar third-party information provisions from its Section 702 minimization procedures. In approving that change, the Court explained that in the context of Section 702 collection such rules

have no practical effect because the term "target" is defined as "the user(s) of a targeted selector." In light of that definition . . . there are no "third party" communications [in Section 702 collection] for the FBI to minimize. Because the deletion of the provisions regarding third party communications does not alter the manner in which the FBI acquires, retains, or disseminates Section 702 information, this change is not problematic under Section 1801(h).

September 20, 2012 Opinion at 17-18 (internal citations omitted). For the same reason, the omission of provisions present in NCTC's Title I Procedures governing the NCTC's retention, processing, and dissemination of third-party information from its Section 702 minimization procedures presents no impediment to their approval.

Exclusion and Departure Provisions. The NCTC Minimization Procedures contain certain exclusions and departure provisions that are consistent with the NCTC Title I Procedures with two notable exceptions:

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

- (1) An exclusion is added for the performance of lawful oversight functions of NSD, ODNI, relevant Inspectors General, and NCTC itself, which is consistent with parallel provisions in other agencies' procedures. See NCTC Minimization Procedures § A.6.e; NSA Minimization Procedures § 1; FBI Minimization Procedures § I.G; CIA Minimization Procedures § 6(f); and
- (2) A separate exclusion addresses compliance with congressional and judicial mandates. NCTC Minimization Procedures § A.6.d.

The latter provision was amended across all the agencies' minimization procedures in the September 26, 2016 Submission and is the subject of separate discussion below.

U.S. Person Presumptions. In general, the procedures provide a rebuttable presumption that persons known to be in the United States are United States persons, and those known or reasonably believed to be outside the United States are non-United States persons. Id. § A.4.a and b. The NCTC Minimization Procedures diverge slightly from their Title I counterpart with respect to individuals whose locations are not known. [REDACTED]

[REDACTED] NCTC Title I Procedures § A.4.a. That approach makes sense in those procedures, which apply to information predominantly obtained by electronic surveillance and physical search – [REDACTED]

[REDACTED] – directed at persons in the United States. [REDACTED]

[REDACTED] Id. §

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

A.4.c. [REDACTED]

[REDACTED]
[REDACTED] NCTC Minimization Procedures
§A.4.e.

The Court assesses that Section 702 collection is more analogous to [REDACTED] than it is to other forms of collection that are regulated by the NCTC Title I Procedures and that the application of the [REDACTED] is appropriate in this context. Section 702 collection focuses exclusively on electronic data and communications collected with the assistance of electronic communication service providers, and its targets are reasonably believed to be non-U.S. persons located overseas. The presumption of non-U.S. person status for a communicant whose location is not known is also consistent with the presumptions allowed under the FBI and NSA's current and proposed Section 702 minimization procedures. See NSA Minimization Procedures § 2(k)(2); FBI Minimization Procedures § I.D. The Court finds the same framework reasonable as applied to NCTC's handling of Section 702 information and consistent with the requirements of Section 1801(h). See September 20, 2012 Opinion at 15-16 (approving parallel change to FBI Section 702 Minimization Procedures).³⁹

Retention. The NCTC Minimization Procedures impose a retention schedule and framework that are consistent with those followed by FBI for Section 702-acquired information

³⁹ The NCTC Minimization Procedures also include provisions regarding unincorporated associations and aliens who have been admitted for lawful permanent residence (NCTC Minimization Procedures § A.4.c and d) that track current provisions in the NSA Minimization Procedures (§ 2(k)(3) and (4)). The Court sees no issue with these provisions.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

and, with a few immaterial exceptions not warranting separate discussion, with corresponding provisions of the NCTC Title I Procedures. In brief, information that the NCTC retains on an electronic and data storage system, but has not reviewed, generally must be destroyed after five years from the expiration date of the certification authorizing the collection. NCTC Minimization Procedures § B.2.a. Information retained on such systems that has been reviewed, but not identified as information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime is generally subject to special access controls after ten years from such expiration date, and shall be destroyed after fifteen years from such date. Id. § B.2.b.⁴⁰

In one respect, the proposed NCTC Minimization Procedures are more restrictive than the NCTC Title I Procedures: Unlike the NCTC Title I Procedures, the NCTC Minimization Procedures expressly provide that the prescribed time limits for retention apply to metadata repositories, NCTC Minimization Procedures § C.3; see October 4, 2016 Transcript at 7. They further require appropriate training and access controls for NCTC employees granted access to Section 702-acquired information. NCTC Minimization Procedures §§ B.1, F.1, F.2 and F.3. They also require that such information be maintained in secure systems that enable NCTC to mark or otherwise identify communications that meet the standards for retention. Id. Consistent with the procedures followed by other agencies, the NCTC Minimization Procedures require

⁴⁰ Generally speaking, information identified as meeting one of those criteria is not subject to the above-described temporal limitations on retention. Id. § B.3. See, however, the discussion on page 46 below regarding limitations on retention and use of evidence of a crime that is not foreign intelligence information.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

destruction of information obtained under a reasonable, but mistaken, belief that the target was appropriate for Section 702 collection, subject to limited waiver provisions. Id. § B.4. Finally, they include provisions for retention of information reasonably believed to be necessary for, or potentially discoverable in, administrative, civil or criminal litigation. Id. § B.5. Analogous provisions already appear in NSA's and CIA's Minimization Procedures. See NSA Minimization Procedures § 3(c)(4); CIA Minimization Procedures § 11.

Processing. The NCTC Minimization Procedures set standards for queries of data obtained under Section 702, including requiring written justifications for queries using U.S. person identifiers that are subject to subsequent review and oversight by NSD and ODNI. NCTC Minimization Procedures § C.1; see also id. § C.3 (metadata queries "must be reasonably likely to return foreign intelligence information"). They apply heightened handling requirements to sensitive information and privileged communications. The provisions for sensitive information are essentially identical to those found in the NCTC Title I Procedures. Compare NCTC Minimization Procedures § C.4 with NCTC Title I Procedures § C.5.

The proposed procedures for NCTC's handling of privileged communications obtained under Section 702 closely track those found in NSA's and CIA's Section 702 minimization procedures. Compare NCTC Minimization Procedures § C.5 with NSA Minimization Procedures § 4; CIA Minimization Procedures § 7. The NCTC Minimization Procedures require, among other things, the destruction of attorney-client communications that are affirmatively determined not to contain foreign intelligence information or evidence of a crime. See NCTC Minimization Procedures § C.5.a. If an attorney-client communication appears to contain foreign

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

intelligence information or evidence of a crime, [REDACTED]

[REDACTED] See *id.* § C.5.b, c, and e. Communications containing privileged information will be segregated when such information pertains to a criminal charge in the United States, [REDACTED]

[REDACTED] See *id.* § C.5.c, d, e, and f. [REDACTED]

[REDACTED] See *id.* § C.5.i. [REDACTED]

[REDACTED] See *id.* § C.5.g and h.

The Court closely examined substantial revisions to the NSA and CIA procedures as they relate to privileged communications in 2015, and found that they “serve to enhance the protection of privileged information” and “present no concern under Section 1801(h).” See November 6, 2015 Opinion at 18. The Court now finds the same to be true with respect to the NCTC Minimization Procedures.

Dissemination. The dissemination provisions of the NCTC Minimization Procedures (§ D) provide for disseminations in a manner consistent with CIA’s and NSA’s handling of Section 702-acquired information. They also track in all material respects the NCTC Title I Procedures, which have been found to satisfy Section 1801(h).

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Handling of Information in FBI General Indices. The NCTC Minimization Procedures, like the NCTC Title I Procedures, include a separate section that addresses NCTC's handling of minimized Section 702 information made available to it through FBI's general indices. This provision of the NCTC Minimization Procedures tracks the corresponding provision of the NCTC Title I Procedures. Compare NCTC Minimization Procedures § E with NCTC Title I Procedures § E. The government points out that the description of individuals who are expected to be allowed access to information in such systems ("NCTC personnel") is meant to be broader than the defined term "NCTC employees" that is used in all other instances throughout the proposed NCTC Minimization Procedures. The government explains that the broader term "NCTC personnel" is meant to encompass (in addition to the NCTC employees, detailees, and contractors who would qualify as "NCTC employees" as defined in the proposed procedures, see NCTC Minimization Procedures § A.3.b) NCTC assignees from other agencies. The government explains that, consistent with the current NCTC Section 702 minimization procedures, such assignees will continue to have access to minimized information in FBI general indices but will not be allowed to access raw Section 702-acquired information. September 26, 2016 Memorandum at 15 n.9. The Court assesses that is a sensible distinction.

Two Additional Issues. Two particular provisions in the agencies' proposed minimization procedures relating to NCTC represent departures from current practice under Section 702 and merit separate discussion. Those provisions pertain to NCTC's retention of evidence of a crime and receipt of information from FBI and NSA for collection avoidance purposes.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

NCTC's Retention of Evidence of Crime. The predecessor procedures that regulated NCTC's retention, use, and dissemination of minimized Section 702 information obtained through FBI's general indices acknowledged that some of the information made available to NCTC might constitute evidence of a crime, but not foreign intelligence information or information necessary to understand such information or assess its importance. As a law enforcement agency, FBI would have a reason to maintain such information in its general indices, where NCTC employees might encounter it. NCTC, as a non-law-enforcement agency, was precluded under its previous Section 702 minimization procedures from retaining (in its own systems), using or disseminating such information. By contrast, under the new NCTC Minimization Procedures (and only with respect to information it receives in raw form),⁴¹ NCTC may retain and disseminate evidence of a crime for law enforcement purposes. *See* NCTC Minimization Procedures §§ A.7, D.2. This proposed approach is consistent with Sections A.7 and D.2 of the NCTC Title I Procedures.

The government asserts that, under the proposed NCTC Minimization Procedures, NCTC might review raw information that has not been, and may never be, reviewed by any other agency. As such, the government posits, NCTC must disseminate evidence of a crime to meet its "crime reporting obligations" under Executive Order 12333 and other applicable law. See

⁴¹ As noted above, the new NCTC Minimization Procedures incorporate (in Section E) the rules currently governing NCTC's retention, use, and dissemination of minimized information that it obtains through FBI's general indices. NCTC continues to be prohibited from retaining, using or disseminating information it obtains from those indices that constitutes evidence of a crime, but not foreign intelligence information, with anyone, including law enforcement, for reasons explained below. See NCTC Minimization Procedures § E.2

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

September 26, 2016 Memorandum at 16-17. Under NCTC's minimization procedures as now in effect, NCTC only has access to information from FBI indices that has already been reviewed and minimized by FBI, so it is presumed that FBI would have taken all necessary steps with respect to actionable law enforcement information. Under that construct, NCTC could, as required by its procedures, simply disregard and delete that information from its holdings (unless there was a foreign intelligence reason for NCTC to retain it). The government asserts that the same would not be true with respect to raw information passed to NCTC. See id.

It is less readily apparent, however, why NCTC would need to retain evidence of a crime after it has been passed to a law enforcement agency. The government asserts that NCTC needs to preserve original copies of the relevant information in order to be able to respond to potential follow-on requests for information or assistance from law enforcement. See October 4, 2016 Transcript at 4-6.⁴² In other words, NCTC would have no reason to retain the information for its own purposes, but it would have a need for retention that derives from the needs of the law enforcement agency to which NCTC passed the information. The government further posits that NCTC may be the only agency that retains a copy of the relevant information and thus may be the only entity able to respond to follow-up requests from law enforcement. See October 4, 2016 Transcript at 5.

⁴² The government correctly points out that in its opinion approving the NCTC's Title I Procedures, which contain identical provisions with respect to crime reporting and evidence of a crime, the Court found that those provisions met the statutory definition of minimization procedures in Section 1801(h)(3), which prescribes procedures that "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." See September 26, 2016 Memorandum at 16 n.10.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

The Court credits the government's explanation of NCTC's derivative need to retain such information for law enforcement purposes. It bears emphasis, however, that NCTC may retain and disseminate evidence of a crime that is not foreign intelligence information or necessary to understand foreign intelligence information or assess its importance and otherwise would be subject to destruction under the generally applicable age-off schedule, see NCTC Minimization Procedures § B.2, only in furtherance of those law enforcement purposes. See id. § D.2. The Court understands and expects that NCTC will only retain such information – including after it has been disseminated in compliance with crime reporting obligations, see id. § A.7 – for so long as is reasonably necessary to respond to law enforcement requests of the kind posited by the government. In the interim, NCTC shall make no independent use of such information. The Court directs the government to take steps to ensure that NCTC abides by these limitations and that any failures to do so are appropriately identified and reported to the FISC.

Collection Avoidance. The FBI and NSA would also be allowed, under proposed amendments to their respective procedures, to share with NCTC for “collection avoidance” purposes information about domestic communications obtained under Section 702 that indicate that a targeted person is in the United States or otherwise should no longer be targeted under Section 702. See NSA Minimization Procedures § 5; FBI Minimization Procedures § III.A. These provisions now allow sharing of such information among FBI, NSA, and CIA. At first it was not clear to the Court why this provision should be extended to include NCTC, given that NCTC engages in no independent collection under Section 702, or, so far as the Court is aware, under any other authorities. [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

████████████████████ and the modifications to the other agencies' procedures relating to NCTC's receipt of such information, are reasonable. The NCTC Minimization Procedures address retention, use, and dissemination of Section 702-acquired information in ways that are consistent with logical analogues. Indeed, the FISC has approved all the major elements of those procedures in the context of other FISA minimization procedures, and the Court finds that, taken as a whole and as applied to raw information acquired under ██████████ ██████████, the NCTC Minimization Procedures conform to 50 U.S.C. § 1801(h).

- E. Other Changes to Targeting and Minimization Procedures in the September 26, 2016 Submission
 - 1. Changes to FBI Minimization Procedures Permitting the Retention of Section 702-Acquired Information Subject to Preservation Obligations Arising from Litigation

In 2014, the FISC approved provisions permitting FBI, NSA, and CIA to retain Section 702-acquired information subject to specific preservation obligations arising in litigation concerning the lawfulness of Section 702. See August 26, 2014 Opinion at 21-25. Under those provisions, information otherwise subject to destruction under the agencies' respective minimization procedures would nonetheless be retained to satisfy litigation preservation obligations. Access to information retained under those provisions is tightly restricted. See id. at 21, 23.

The NSA and CIA minimization procedures accompanying the 2015 Certifications included revisions to these "litigation hold" provisions. Among other things, those procedures included new provisions whereby NSA and CIA may retain for litigation purposes Section 702-

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

acquired information otherwise subject to destruction requirements that are not set forth in the minimization procedures, provided that access to such information is strictly controlled as prescribed in the procedures.⁴⁴ The government must promptly notify the Court and seek its approval whenever this provision is invoked. See NSA Minimization Procedures § 3(c)(4)b; CIA Minimization Procedures § 11.b.

The litigation hold provisions also require NSA and CIA to provide DOJ with a summary of all litigation matters requiring preservation of Section 702-acquired information, a description of the Section 702-acquired information being retained, and, if possible based on the information available to the agencies, the status of each litigation matter. See NSA Minimization Procedures § 3(c)(4)a and b; CIA Minimization Procedures § 11.a and b.⁴⁵ The FISC, in considering the 2015 Certifications, appointed amicus curiae to help it evaluate these litigation hold provisions. The FISC agreed with the amicus's assessment that the revised litigation hold provisions "comport with the requirements of Section 1801(h) and strike a reasonable and appropriate

⁴⁴ As stated in the November 6, 2015 Opinion, the Court understands this provision to apply to destruction requirements arising under a FISC order, a FISC rule, or other FISC-approved procedures – e.g., the requirement that NSA destroy any communication acquired through the intentional targeting of a person reasonably believed to be a United States person or to be located in the United States, see NSA Targeting Procedures § IV.

⁴⁵ The FISC has ordered the government to submit a report at the end of each year identifying matters in which FBI, NSA or CIA is retaining Section 702-acquired information that would otherwise be subject to destruction in order to satisfy a litigation preservation obligation. See August 26, 2014 Opinion at 42. The Court has reviewed the litigation hold reports filed by the government in December 2015 and December 2016. The Court is reaffirming that reporting obligation and extending it to NCTC.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

balance between the retention limitations reflected in FISA and the government's need to comply with its litigation-related obligations." November 6, 2015 Opinion at 16.

The proposed NCTC Minimization Procedures, like NSA's and CIA's, include litigation hold provisions that address departures from destruction requirements arising under NCTC's minimization procedures and from other sources. See NCTC Minimization Procedures § B.5.

The government proposes now to expand the FBI Minimization Procedures to address the latter situation and to bring FBI's litigation hold provisions more closely into line with those of the other agencies. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In 2015, with the concurrence of a FISC-appointed amicus curiae, the FISC found these procedures appropriate as applied to NSA and CIA. November 6, 2015 Opinion at 16. The Court sees no basis for a contrary conclusion now with regard to the NCTC and FBI.

The Court emphasizes, however, the need promptly to notify and seek leave of the Court to retain information pursuant to such provisions. [REDACTED]

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~



at 2-3. The Court will not look favorably on similarly lengthy delays in deciding whether to comply with an otherwise applicable destruction requirement or seek FISC approval to retain information in anticipation of bringing criminal charges.

2. Clarification of Age-off Requirements for Encrypted Information Under the FBI Minimization Procedures

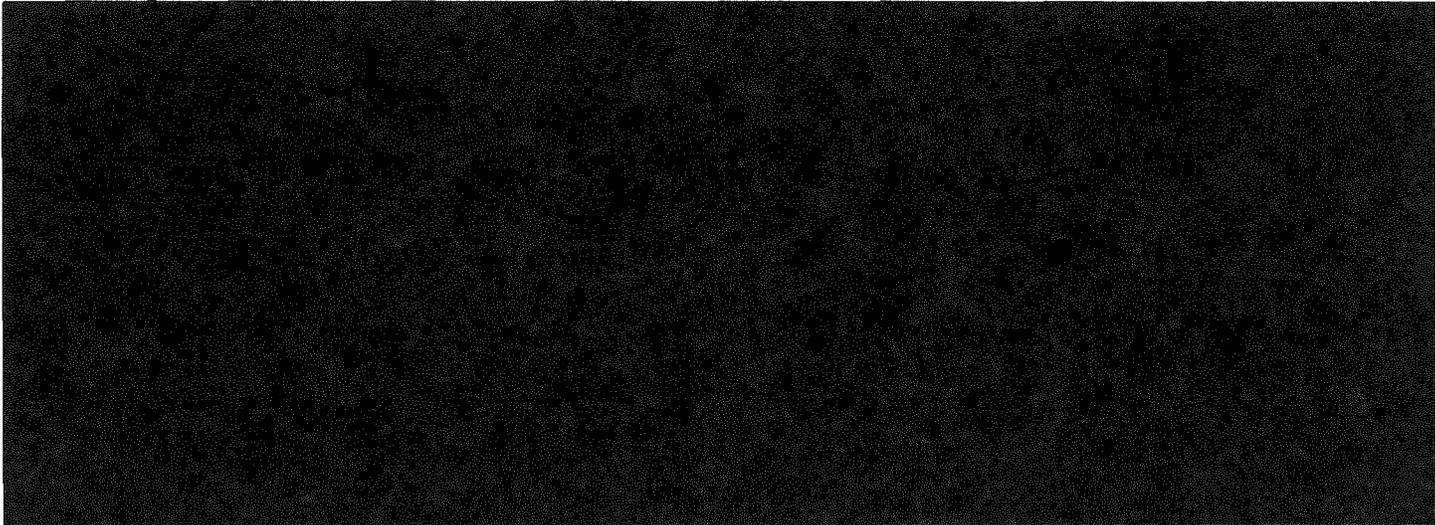
In its 2015 Submission, the government added a new provision to the FBI Minimization Procedures permitting the FBI to retain Section 702-acquired information that is encrypted or believed to contain secret meaning for any period of time during which such material is subject to, or of use in, cryptanalysis or otherwise deciphering secret meaning. Access to such information is restricted to FBI personnel engaged in cryptanalysis or deciphering secret meaning. See FBI Minimization Procedures § III.G.5. Nonpublicly available information concerning unconsenting United States persons retained under the provision cannot be used for any other purpose unless such use is permitted under a different provision of the minimization procedures. See id. Once information retained under this provision is decrypted or its secret meaning is ascertained, the generally-applicable retention rules apply. The government stated that it would calculate the age-off date for such information from the later of the date of decryption or the date of expiration of the certification pursuant to which the information was

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

acquired. See Docket Nos. [REDACTED] July 15, 2015, Memorandum Regarding Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request For an Order Approving Such Certifications and Amended Certifications at 18. But the procedures themselves were silent on this point.

When it approved the 2015 Certifications, the FISC encouraged the government to make this calculation methodology explicit in future versions of the procedures. November 6, 2015 Opinion at 20 n.19. The government has done so. The FBI Minimization Procedures now



3. Revisions to Minimization Provisions Permitting Compliance with Judicial or Legislative Mandates

The NSA and CIA minimization procedures approved in the November 6, 2015 Opinion each state that “[n]othing in these procedures shall prohibit the retention, processing, or dissemination of information reasonably necessary to comply with specific constitutional, judicial, or legislative mandates.” See November 6, 2015 Opinion at 21 (citing relevant provisions of procedures). The FISC took issue with the facial breadth of these provisions,

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

observing that “[a] provision that would allow the NSA and CIA to deviate from any of the[] restrictions [in their respective minimization procedures] based upon unspecified ‘mandates’ could undermine the Court’s ability to find that the procedures satisfy” statutory requirements. Id. at 22. The FISC addressed this issue in three ways. First, in order to avoid finding a deficiency in the procedures, it applied an interpretive gloss that the government had previously articulated with regard to similar language in another set of minimization procedures, to the effect that such provisions would be invoked sparingly and applied only to directives specifically calling for the information at issue, and not to Executive Branch orders or directives. Id. at 22. The FISC emphasized that it “must construe the phrase ‘specific constitutional, judicial, or legislative mandates’ to include only those mandates containing language that clearly and specifically requires action in contravention of an otherwise-applicable provision of the requirement of the minimization procedures.” Id. at 23. Second, to ensure that these provisions were actually applied in a manner consistent with the FISC’s understanding, the government was directed to report any action in reliance on this provision to the FISC promptly and in writing, along with a written justification for each such action. Id. at 23-24.⁴⁶ Finally, the government was encouraged to consider replacing these broadly-worded provisions with language more narrowly tailored to the above-described intent. Id. at 24 n.20.

The government proffered revisions to these provisions in the September 26, 2016 Submission. The provisions, as revised and incorporated in all of the agencies’ minimization

⁴⁶ This reporting requirement is carried forward by this Opinion and Order. The Court understands that this provision has not yet been invoked.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

procedures, now require that the departure be “necessary to comply with a specific congressional mandate or order of a court within the United States.” NSA Minimization Procedures § 1; FBI Minimization Procedures § I.G; CIA Minimization Procedures § 6.g; NCTC Minimization Procedures § A.6.d. The Court finds the revised language acceptable, but again wishes to emphasize that it expects this provision to be interpreted narrowly.

As described in the September 26, 2016 Memorandum at 6-7, the government has received requests from members of Congress, including 14 members of the House Judiciary Committee, for estimates of the number of communications of U.S. persons that have been acquired under Section 702. Responding to such requests would require NSA, and possibly other agencies, to structure queries designed to elicit information concerning U.S. persons with no foreign intelligence purpose, facially in violation of applicable minimization procedures. Such requests, which have not taken the form of a subpoena or other legal process, would not constitute legal mandates for purposes of the departure provision discussed above. Instead, the government submits that, in order to respond to such requests, it may take actions that contravene otherwise applicable minimization requirements pursuant to provisions of the minimization procedures that allow for performance of lawful oversight functions. For example, the NSA Minimization Procedures state that nothing in them shall restrict “NSA’s performance of lawful oversight functions of its personnel or systems, or lawful oversight functions” of NSD, ODNI, or relevant Inspectors General. NSA Minimization Procedures § 1; see also FBI Minimization Procedures § I.G (same); CIA Minimization Procedures § 6.f (same); NCTC Minimization Procedures § A.6.e (same). The government also undertook to notify the Court

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

“promptly” if it “uses this provision to respond to such congressional oversight inquiries.”

September 26, 2016 Memorandum at 7.⁴⁷

Although these provisions could more clearly address responses to requests from congressional overseers, the Court believes they can be fairly read to authorize actions necessary to respond to the requests described by the government. The Court directs the government to provide prompt written notification of any instance when an agency acts in contravention of otherwise applicable minimization requirements in order to respond to an oversight request from any outside entity other than those currently specified in its procedures. The Court expects the government to make such a submission regarding its response to the above-referenced congressional requests promptly upon completion of that response.

4. Amendment of FBI Targeting Procedures with Respect to 



⁴⁷ The government has since orally notified the Court that, in order to respond to these requests and in reliance on this provision of its minimization procedures, NSA has made some otherwise-noncompliant queries of data acquired under Section 702 by means other than upstream Internet collection.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~



The Court does not view this change, which deals with [REDACTED]

[REDACTED] agencies authorized to receive unminimized Section 702-acquired information, as problematic, provided that information is shared only with entities authorized to receive it (in the case of NCTC, information obtained pursuant to [REDACTED]). The legality of raw information sharing fundamentally rests on the foreign intelligence need to provide the information to the receiving agency and that agency's implementation of FISA-compliant minimization procedures.

Accordingly, the Court concludes that this change does not preclude it from finding that the FBI Targeting Procedures meet the requirements of Section 1881a(d)(1).

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

F. Conclusions

1. The NSA and FBI Targeting Procedures Comply With Statutory Requirements and Are Reasonably Designed to Prevent the Targeting of United States Persons

To summarize, the proposed changes to NSA's targeting procedures now make clear that acquisitions thereunder will be limited to communications to or from persons targeted for

acquisition under Section 702. FBI's revised targeting procedures allow it to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The Court has no difficulty finding that these changes, individually and taken together, do not detract from its earlier holdings with regard to the sufficiency and legality of the FBI and NSA targeting procedures.

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA Targeting Procedures and the FBI Targeting Procedures, as written, are reasonably designed, as required by Section 1881a(d)(1): (1) to ensure that any acquisition authorized under the 2016 Certifications is limited to targeting persons reasonably believed to be located outside the United States, and (2) 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. Moreover, for the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA and FBI Targeting Procedures, as written, are reasonably designed to prevent United States persons from

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

being targeted for acquisition – a finding that is relevant to the Court’s analysis, which is set out below, of whether the procedures are consistent with the requirements of the Fourth Amendment.

2. The FBI, NSA, CIA, and NCTC Minimization Procedures Comply With Statutory Requirements

For the reasons stated above and in the Court’s opinions in the Prior 702 Dockets, the Court similarly concludes that the NSA, FBI, CIA, and NCTC Minimization Procedures satisfy the definition of minimization procedures at Section 1801(h). In the November 6, 2015 Opinion, the FISC found that the minimization procedures accompanying the 2015 Certifications met statutory and constitutional standards. The FISC recommended two changes to the procedures in future submissions. In both instances, the government has acted on those suggestions, proposing changes to narrow the “legal mandate” exception to each agency’s minimization procedures and define more precisely the time limits placed on FBI’s retention of information believed to be encrypted or contain secret meaning. Both changes further cabin the relevant agencies’ discretion and enhance the protection of nonpublicly available information concerning unconsenting United States persons.⁴⁸

Other changes to minimization procedures pertain to FBI’s retention of information for “litigation hold” purposes and enable sharing [REDACTED] [REDACTED] with NCTC. (As noted above, NCTC’s revised procedures incorporate

⁴⁸ As discussed above, the NSA Minimization Procedures have been revised to eliminate acquisition of “abouts” communications and the most problematic forms of MCTs. As a result of that change, the Court no longer views the prohibition on U.S.-person queries in NSA upstream collection to be necessary to comport with the statute or, as discussed below, the Fourth Amendment.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

elements from various other procedures, with appropriate adaptations to fit the context of Section 702.) The Court concludes that none of the proposed changes to the agencies' minimization procedures, individually or collectively, precludes the Court from finding that such procedures comport with Section 1801(h).

Accordingly, the Court finds that the agencies' proposed minimization procedures meet the requirements of 50 U.S.C. § 1801(h). That finding is made in reliance on (1) the above-stated limitations on (a) the types of information that will, and will not, be shared in raw form with the FBI, CIA, and NCTC, and (b) NCTC's retention, use or disclosure of evidence of a crime and information received from other agencies for collection avoidance purposes; and (2) the expectation that the government will faithfully comply with the reporting requirements set forth below, in the procedures themselves, and in Rule 13 of the FISC Rules of Procedure.

G. The Targeting and Minimization Procedures Are Consistent with the Fourth Amendment

The Court must also assess whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A).

The Fourth Amendment states:

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.

U.S. Const. amend. IV.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Reasonableness is “the ultimate touchstone of the Fourth Amendment.” In re Certified Question of Law, Docket No. 16-01, Opinion at 31 (FISA Ct. Rev. Apr. 14, 2016) (per curiam) (“In re Certified Question”)⁴⁹ (quoting Riley v. California, 134 S. Ct. 2473, 2482 (2014)).⁵⁰ In assessing the reasonableness of a governmental intrusion under the Fourth Amendment, a court must “balance the interests at stake” under the “totality of the circumstances.” In re Directives at

20. Specifically, a court must “balance . . . the degree of the government’s intrusion on individual privacy” against “the degree to which that intrusion furthers the government’s legitimate interest.” In re Certified Question at 31. “The more important the government’s interest, the greater the intrusion that may be constitutionally tolerated.” In re Directives at 19-20.

If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in

⁴⁹ A declassified version of this opinion is available at: www.dni.gov/files/icotr/FISCR%Opinion%2016-01.pdf.

⁵⁰ Although “[t]he warrant requirement is generally a tolerable proxy for ‘reasonableness’ when the government is seeking to unearth evidence of criminal wrongdoing, . . . it fails properly to balance the interests at stake” when “the government is instead seeking to preserve the nation’s security from foreign threats.” In re Certified Question at 3. Accordingly, a warrant is not required to conduct surveillance “to obtain foreign intelligence for national security purposes . . . directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.” In re Directives Pursuant to Section 105B of FISA, Docket No. 08-01, Opinion at 18-19 (FISA Ct. Rev. Aug. 22, 2008) (“In re Directives”). (A declassified version of In re Directives is available at 551 F.3d 1004 (FISA Ct. Rev. 2008)). The FISC has repeatedly reached the same conclusion regarding Section 702 acquisitions. See, e.g., November 6, 2015 Opinion at 36-37; September 4, 2008 Opinion at 34-36; accord United States v. Hasbajrami, 2016 WL 1029500 at *7-*9 (E.D.N.Y. March 8, 2016); United States v. Mohamud, 2014 WL 2866749 at *15-*18 (D. Or. June 24, 2014).

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

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.

“Collecting foreign intelligence with an eye toward safeguarding the nation’s security serves . . . a particularly intense interest” that is “different from the government’s interest in the workaday enforcement of the criminal law.” In re Certified Question at 29 (internal quotation marks omitted); see also id. at 31 (noting “the paramount interest in investigating possible threats to national security”). For that reason, “the government’s investigative interest in cases arising under FISA is at the highest level and weighs heavily in the constitutional balancing process.”

Id. at 32.

On the other side of the balance is the degree of intrusion on individual privacy interests protected by the Fourth Amendment. The degree of intrusion here is limited by restrictions on how the government targets acquisitions under Section 702 and how it handles information post-acquisition. For reasons explained above, the Court has found that the targeting procedures now before it are reasonably designed to limit acquisitions to targeted persons reasonably believed to be non-United States persons located outside the United States, whose privacy interests are not protected by the Fourth Amendment. See, e.g., November 6, 2015 Opinion at 38; September 4, 2008 Opinion at 37 (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990)). That is not to say, however, that targeting non-United States persons located outside the United States for acquisition under Section 702 never implicates interests protected by the Fourth Amendment. Under the revised procedures, the government may acquire communications to

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

which United States persons and persons within the United States are parties when such persons communicate with a Section 702 target.⁵¹ Therefore it is necessary to consider how information from those communications will be handled.

Steps taken by the government to restrict the use or disclosure of information after it has been acquired can reduce the intrusiveness of the acquisition for purposes of assessing its reasonableness under the Fourth Amendment. See In re Certified Question at 35. In the Prior 702 Dockets, the FISC found that “earlier versions of the various agencies’ targeting and minimization procedures adequately protected the substantial Fourth Amendment interests that are implicated by the acquisition of communications of such United States persons.” November 6, 2015 Opinion at 38-39 (citing August 26, 2014 Opinion at 38-40; August 30, 2013 Opinion at 24-25). Specifically, “the combined effect of these procedures” was “to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated’ and to ensure that ‘non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary.’” November 6, 2015 Opinion at 39 (quoting August 26, 2014 Opinion at 40).

The November 6, 2015 Opinion included a careful analysis of the rules for querying Section 702 information using United States person identifiers under the minimization procedures for the NSA, the CIA, and especially the FBI. See November 6, 2015 Opinion at 24-

⁵¹ NSA’s elimination of “abouts” collection should reduce the number of communications acquired under Section 702 to which a U.S. person or a person in the United States is a party.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

36, 39-45. After receiving briefing and oral argument from an amicus curiae appointed under 50 U.S.C. § 1803(i)(2)(B), the FISC concluded that, although its review did not involve treating each query as a separate action subject to a test for Fourth Amendment reasonableness, the querying rules were relevant to its assessment of whether the procedures as a whole were reasonable under the Fourth Amendment. November 6, 2015 Opinion at 40-41. The FISC further determined that the querying rules did not preclude a finding that the procedures were consistent with the requirements of the Fourth Amendment. *Id.* at 44-45.

In the procedures now before the Court, the relevant provisions of the CIA and FBI minimization procedures remain unchanged, *see* CIA Minimization Procedures at § 4; FBI Minimization Procedures at §§ III.D, IV.D, and the NCTC procedures generally track the pertinent requirements of the CIA Minimization Procedures. *See* NCTC Minimization Procedures at § C.3.⁵²

With regard to the querying rules in the CIA and NCTC procedures, the Court adopts the analysis of the November 6, 2015 Opinion.

As discussed above, NSA's procedures now limit all acquisitions – including upstream Internet acquisitions – to communications to or from an authorized Section 702 target. That limitation places upstream Internet collection in a posture similar to other forms of Section 702 collection for the purpose of assessing reasonableness under the Fourth Amendment. The revised procedures subject NSA's use of U.S. person identifiers to query the results of its newly-

⁵² Unlike the CIA procedures, the NCTC procedures require that queries of Section 702 metadata, as well as contents, be reasonably designed to return foreign intelligence information. NCTC Minimization Procedures at § C.3.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

limited upstream Internet collection to the same limitations and requirements that apply to its use of such identifiers to query information acquired by other forms of Section 702 collection. See NSA Minimization Procedures § 3(b)(5). For that reason, the analysis in the November 6, 2015 Opinion remains valid regarding why NSA's procedures comport with Fourth Amendment standards of reasonableness with regard to such U.S. person queries, even as applied to queries of upstream Internet collection.

As discussed in the November 6, 2015 Opinion, the FBI's minimization procedures contemplate queries conducted to elicit foreign intelligence information and queries conducted to elicit evidence of crimes. With respect to the latter type of query, the FISC's approval of the FBI minimization procedures in 2015 was bolstered by the government's assessment that "FBI queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results" from Section 702 information. See November 6, 2015 Opinion at 44. To confirm the continued accuracy of that assessment, the FISC ordered the government to report on "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." Id. at 78.

The government has reported one set of queries as responsive to this requirement. On [REDACTED], an FBI analyst reviewing Section 702 information found an email message in which a person in the United States gave detailed descriptions of violent, abusive acts [REDACTED] committed [REDACTED] children. [REDACTED] Notice regarding FBI queries of Section 702-

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

acquired information designed to return evidence of a crime unrelated to foreign intelligence (“██████████ Notice”), at 2. In an effort to identify additional evidence of abuse, the FBI ran queries of Section 702 information using the names of the suspected abuser, the apparent victims, and other terms derived from that e-mail message. Those queries only retrieved the previously reviewed e-mail message from which the query terms were derived. Id. Pursuant to Section I.F of its minimization procedures, the FBI disseminated information about the child abuse to a local child protective services agency, ██████████ ██████████ Id.

The undersigned judge finds persuasive the November 6, 2015 Opinion’s analysis of the FBI’s querying rules. The single reported instance of queries that returned U.S. person information unrelated to foreign intelligence information does not detract from that analysis, especially since those queries did not result in any further intrusion on privacy: they merely retrieved information already known to the analyst who ran the queries.⁵³

For the reasons stated above, neither the NCTC’s receipt of unminimized information acquired regarding counterterrorism targets, subject to its applying the NCTC Minimization Procedures, nor the other above-described modifications to the targeting and minimization procedures, causes the Court to deviate from prior assessments that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

⁵³ The Court notes, however, that the FBI did not identify those queries as responsive to the Court’s reporting requirement until NSD asked whether any such queries had been made in the course of gathering information about the Section I.F dissemination. ██████████ Notice at 2. The Court is carrying forward this reporting requirement and expects the government to take further steps to ensure compliance with it.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

IV. THE COMPLIANCE AND IMPLEMENTATION ISSUES REPORTED BY THE GOVERNMENT DO NOT WARRANT A FINDING THAT, AS IMPLEMENTED, THE TARGETING AND MINIMIZATION PROCEDURES ARE DEFICIENT.

The FISC has consistently understood its review of targeting and minimization procedures under Section 702 to include examining how the procedures have been and will be implemented. See, e.g., November 6, 2015 Opinion at 7; August 30, 2013 Opinion at 6-11, 19-22; April 7, 2009 Opinion at 22-25. As the Foreign Intelligence Surveillance Court of Review has noted, FISC “supervision of the execution of pen register orders further reduces the risk that such measures will be employed under circumstances, or in a manner, that unreasonably intrudes on individuals’ privacy interests.” In re Certified Question at 36-37. The same conclusion applies to FISC examination of how the government implements the Section 702 procedures.

For purposes of this examination, “the controlling norms are ones of reasonableness, not perfection,” November 6, 2015 Opinion at 45, under both Section 702⁵⁴ and the Fourth Amendment.⁵⁵ The Court evaluates the reasonableness of “the program as a whole,” not of individual actions in isolation. November 6, 2015 Opinion at 40-41. The assessment of

⁵⁴ See 50 U.S.C. § 1881a(d)(1) (requiring targeting procedures that are “reasonably designed to” limit targeting to “persons reasonably believed to be located outside the United States” and to “prevent the intentional acquisition” of communications to which all parties are known to be in the United States); § 1881a(e)(1) (requiring minimization procedures as defined in §§ 1801(h)(1) or 1821(4), i.e., procedures “reasonably designed” to minimize acquisition and retention, and to prohibit dissemination, of information concerning United States persons, consistent with foreign intelligence needs).

⁵⁵ See, e.g., United States v. Knights, 534 U.S. 112, 118 (2001) (“The touchstone of the Fourth Amendment is reasonableness”); In re Directives at 34 (surveillances found to be reasonable under the Fourth Amendment where “the risks of error and abuse are within acceptable limits and effective minimization procedures are in place”).

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

reasonableness takes due account of the fact that implementing Section 702 is “a large and complex endeavor . . . effected through thousands of discrete targeting decisions for individual selectors,”⁵⁶ each of which implicates selector-specific pre-tasking and post-tasking requirements, November 6, 2015 Opinion at 45-46, and that for all information acquired under Section 702, minimization procedures impose “detailed rules concerning . . . retention, use, and dissemination” Id. at 46. As the FISC has previously observed:

Given the number of decisions and volume of information involved, it should not be surprising that occasionally errors are made. Moreover, the government necessarily relies on [REDACTED] processes in performing post-tasking checks, see, e.g., August 30, 2013 Opinion at 7-9, and in acquiring, routing, storing, and when appropriate purging Section 702 information. See, e.g., April 7, 2009 Opinion at 17-22. Because of factors such as changes in communications technology or inadvertent error, these processes do not always function as intended.

Id.

Overall, the Court concludes that the targeting and minimization procedures satisfy applicable statutory requirements and are reasonable under the Fourth Amendment, despite the reported instances of non-compliance in prior implementation. The Court bases this conclusion in large measure on the extensive oversight conducted within the implementing agencies and by the DOJ and ODNI. Due to those efforts, it appears that compliance issues are generally

⁵⁶ For example, NSA “reports that, on average, approximately [REDACTED] facilities were under task at any given time between December 1, 2016 and February 28, 2017.” March 17, 2016 Compliance Report at 1 (footnote omitted). Facilities tasked for acquisition include

[REDACTED]
Id. at 1 n.1. “Additionally, between December 1, 2016 and February 28, 2017, the [FBI] reports that it received and processed approximately [REDACTED] Id. at 1.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

identified and remedied in a timely and appropriate fashion.⁵⁷ Nonetheless, the Court believes it beneficial to discuss certain ongoing or recent compliance issues and, in some cases, direct the government to provide additional information.

A. Resolution of Issues Addressed in the November 6, 2015 Opinion

The November 6, 2015 Opinion discussed several significant compliance problems that were then pending. See November 6, 2015 Opinion at 47-77. With the exception of non-compliance with minimization procedures related to attorney-client privileged communications, which are discussed separately, those compliance issues have been resolved as described below.

1. Failure of Access Controls in FBI's [REDACTED]

[REDACTED] while the 2015 Certifications were pending, the government filed a notice (“[REDACTED] Notice”) indicating that a failure of access controls in an FBI database containing raw Section 702-acquired information resulted in [REDACTED] FBI employees improperly receiving access to such information. [REDACTED] Notice at 1. Specifically,

[REDACTED]

⁵⁷ Too often, however, the government fails to meet its obligation to provide prompt notification to the FISC when non-compliance is discovered. See FISC Rule of Procedure 13(b). For example, it is unpersuasive to attribute – even “in part” – an eleven-month delay in submitting a preliminary notice to “NSA’s efforts to develop remedial steps,” see April 7, 2017 Preliminary Notice (Mislabeling) at 1 n.1, 2, when the purpose of a preliminary notice is to advise the Court while investigation or remediation is still ongoing. See also, e.g., February 28, 2017 Notice of a Compliance Incident Regarding Incomplete Purges of Information Obtained Pursuant to Multiple FISA Authorities (“February 28, 2017 Notice”) at 1-2, n.3 (five-month delay attributed “to administrative issues surrounding the reorganization of NSA offices and personnel”). The Court intends to monitor closely the timeliness of the government’s reporting of non-compliance regarding Section 702 implementation.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED] allowed [REDACTED] users access to Section 702-acquired information, *id.*, when only [REDACTED] were cleared for such access. *Id.* at 1, n.1. This resulted in violations of Sections III.A. and III.B of the FBI's minimization procedures.⁵⁸ The government provided testimony on this issue at a hearing on

[REDACTED] filed a Supplemental Notice on [REDACTED] indicating that [REDACTED] FISA-acquired products were "exported" [REDACTED] users who were not authorized to access these products. [REDACTED] Notice at 2.

On [REDACTED], the government filed what was styled as a Final Notice on this issue [REDACTED] Notice"). That notice indicated that the FBI [REDACTED] [REDACTED] had not disseminated the FISA-acquired products; and all [REDACTED] users had deleted from their systems the raw FISA-acquired information they had exported. [REDACTED]

[REDACTED]
[REDACTED]

⁵⁸ As then in effect and as now proposed, Section III.A of the FBI Minimization Procedures requires the FBI to "retain all FISA-acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with [the FBI Minimization Procedures] and other applicable FBI procedures." FBI Minimization Procedures § III.A. Section III.B of the FBI Minimization Procedures further requires the FBI to grant access to raw Section 702-acquired information in a manner that is "consistent with the FBI's foreign intelligence information-gathering and information-sharing responsibilities, . . . [p]ermitting access . . . only by individuals who require access in order to perform their job duties[.]" *Id.* § III.B. It also requires users with access to FISA-acquired information to receive training on minimization requirements. *Id.* § III.B.4.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] In the Court's assessment, the government has appropriately remedied this incident.

2. NSA Failures to Complete Required Purges

On July 13, 2015, the Government filed a notice regarding NSA's purge processes for FISA-acquired information in its mission management systems ("July 13, 2015 Notice"). That notice indicated that the NSA had not been removing records associated with Section 702 data subject to purge from its [REDACTED] database. July 13, 2015 Notice at 3.

On October 5, 2015, the government filed a Supplemental Notice regarding NSA's purge processes for FISA-acquired information ("October 5, 2015 Notice"). That notice indicated that NSA had now removed from [REDACTED] all Section 702-acquired records that were marked as subject to purge. October 5, 2015 Notice at 2. On October 28, 2015, however, the government filed another Supplemental Notice regarding NSA's purge processes ("October 28, 2015 Notice") in which it reported that a technical malfunction in [REDACTED] had rendered the aforementioned purges incomplete. October 28, 2015 Notice at 2.

On January 14, 2016, the government filed a Supplemental Notice ("January 14, 2016 Notice") indicating that as of October 30, 2015, [REDACTED] was properly configured to remove records subject to purge and corresponding to identifiers on the MPL. January 14, 2016

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Notice at 2. At that time NSA had completed purging records that had been added to the MPL between 2011 and 2015. *Id.* On September 22, 2016, the government filed another Supplemental Notice (“September 22, 2016 Notice on [REDACTED] confirming that as of February 2016, the NSA had removed from [REDACTED] all historical Section 702-acquired records subject to purge.”⁵⁹ September 22, 2016 Notice on [REDACTED] at 2.

The July 13, 2015 Notice also reported “a compliance incident regarding FISA-acquired information subject to purge or age off that [was] being retained in two of NSA’s compliance mission management systems, [REDACTED] and [REDACTED] in a manner that is “potentially inconsistent with NSA’s FISA-related minimization procedures.” July 13, 2015 Notice at 2, 5. Subsequent communications between the government and FISC staff revealed that [REDACTED] and [REDACTED] may also have been retaining data, the use or disclosure of which could violate 50 U.S.C. § 1809(a)(2). The November 6, 2015 Opinion directed the government to provide additional information about NSA’s retention of certain categories of information in [REDACTED] and [REDACTED] November 6, 2015 Opinion at 78.

On December 18, 2015, the government filed a detailed description of its plan and timeline for remedying improper retention in [REDACTED] and [REDACTED] See Prior 702 Dockets, Verified Response to the Court’s Order Dated November 6, 2015, filed on Dec. 18,

⁵⁹ The government also disclosed in the January 14, 2016 Notice that [REDACTED] was not configured to age off all FISA-acquired information pursuant to relevant minimization procedures. January 14, 2016 Notice at 2. As of August 3, 2016, the NSA had removed from [REDACTED] all Section 702-acquired information identified as due for destruction under the retention periods set by the NSA Minimization Procedures, and prospectively, the NSA will remove Section 702-acquired information from [REDACTED] in compliance with those retention periods. September 22, 2016 Notice on [REDACTED] at 2.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

2015. On September 22, 2016, the government provided a written update on the NSA's efforts to remove from [REDACTED] and [REDACTED] information that was subject to purge or age-off under the NSA Minimization Procedures ("September 22, 2016 Notice on [REDACTED] and [REDACTED] As of February 17, 2016, NSA had removed from [REDACTED] and [REDACTED] all Section 702-acquired information subject to age-off under the five- and two-year retention periods set by the NSA Minimization Procedures. September 22, 2016 Notice on [REDACTED] and [REDACTED] at 2. As of September 9, 2016, the NSA had deleted from [REDACTED] and [REDACTED] all historical Section 702-acquired data potentially subject to § 1809(a)(2), and it had developed a plan to deal prospectively with information potentially subject to § 1809(a)(2). *Id.* at 3. Finally, as of September 9, 2016, the NSA had removed from [REDACTED] and [REDACTED] other categories of information that the November 6, 2015 Opinion had identified as not permissible for retention in [REDACTED] and [REDACTED] (e.g., attorney-client communications that do not contain foreign intelligence information or evidence of a crime). *Id.* at 3-4.

B. Issues Arising Under the NSA Targeting Procedures

NSA's targeting procedures require that analysts, before tasking a selector for acquisition, make a reasonable assessment that the user of the selector is a non-U.S. person located outside the United States. See NSA Targeting Procedures § 1. Post-tasking, analysts are required to take reasonable steps to confirm that the selector continues to be used by a non-U.S. person located outside the United States. See NSA Targeting Procedures § 2. Those requirements directly bear on statutory limitations on Section 702 acquisitions. See 50 U.S.C. § 1881a(c)(1)(A), (d)(1)(A)

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

(targeting procedures must be reasonably designed to ensure that acquisitions are limited to targeting persons reasonably believed to be outside the United States); § 1881a(b)(3), (4) (government may not intentionally target a United States person reasonably believed to be outside the United States or intentionally acquire any communication as to which the sender and all intended recipients are known at time of acquisition to be in the United States).

Compliance and implementation issues have arisen regarding these pre-tasking assessments and post-tasking reviews. While those issues merit discussion, the Court does not believe they are sufficiently serious or pervasive to warrant finding that the targeting procedures do not meet the above-described statutory requirements or are inconsistent with the Fourth Amendment.

1. Scope of Pre-Tasking Review of [REDACTED]

One of the measures taken by NSA analysts to fulfill pre-tasking obligations is to check

[REDACTED] for information that may be probative of [REDACTED]

[REDACTED] For example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

According to a notice filed by the government on August 24, 2016, NSA analysts often relied on the above-referenced [REDACTED] tool to [REDACTED] as part of those pre-tasking checks. August 24, 2016 Update Regarding the Scope of Section 702 Pre-Tasking Review of [REDACTED] at 2 (“August 24, 2016 Update”). The data returned [REDACTED] was

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

limited, as [REDACTED] only [REDACTED]
[REDACTED]
[REDACTED]. Id. In certain circumstances, the results from [REDACTED] could
have provided an incomplete and misleading impression of [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]. The government acknowledges
that the sufficiency of running a [REDACTED] [REDACTED] as the sole basis for a pre-tasking assessment
“depends upon the information known about the target from other sources and the nature of the
information returned by the [REDACTED] [REDACTED]. Id. Subsequent investigation revealed [REDACTED]
instances of improper taskings. See August 24, 2016 Update at 2, n.2. NSA placed on its MPL
information obtained as a result of these taskings. Id. at 2.⁶⁰

NSA has developed a new tool for analysts to use for pre-tasking checks [REDACTED]
[REDACTED]
[REDACTED] August 24,
2016 Update at 4. “In addition to [REDACTED], NSA’s new tool is also
[REDACTED]
[REDACTED] that will greatly enhance
analysts’ pre-tasking reviews.” Id.

⁶⁰ For discussion of the government’s processes for purging Section 702 information, see March 17, 2017 Compliance Report at 2-5.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

While the described functionality of the new tool improves on some of the limitations of [REDACTED] it should not be seen as a panacea. In the Court's view, the fundamental cause of these improper taskings was not the limitations of [REDACTED] or other [REDACTED] tools, but rather the failure of analysts in these particular cases to pursue reasonable lines of inquiry regarding [REDACTED] [REDACTED]. See, e.g., August 24, 2016 Update at 3 [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]. It remains the obligation of analysts to exercise due diligence in the particular circumstances of each pre-tasking review, rather than to presume that using a given [REDACTED] tool or protocol will suffice. The government acknowledges that sometimes, after deploying the new tool, "additional research will be necessary to satisfy the totality of the circumstances test [for pre-tasking reviews] contained in the NSA Targeting Procedures," *id.* at 5, and addresses in its training efforts how NSA analysts should understand and comply with this requirement. See October 4, 2016 Transcript at 19-20.

2. Frequency of Post-Tasking Review of Contents

While the government did not report the following information as involving non-compliance with the NSA's targeting procedures, the Court believes it bears significantly on how those procedures are implemented and therefore merits discussion.

The NSA's targeting procedures do not require analysts to review the contents of communications acquired from tasking a particular selector at fixed intervals. Instead, they provide that such content review "will be conducted according to analytic and intelligence

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

requirements and priorities.” See, e.g., NSA Targeting Procedures § II at 6.⁶¹ As previously described to the FISC, however, NSA follows a policy whereby such content review is performed no later than [REDACTED] days after the first acquisition and at intervals of no more than [REDACTED] days thereafter. See September 13, 2016, Update Regarding Post-Targeting Content Reviews (“September 13, 2016 Update”) at 2; Docket No. [REDACTED]

[REDACTED], Memorandum Opinion at 9-10 (FISA Ct. Oct. 24, 2014).

NSA and FBI analysts with access to Section 702 data are trained on this policy, while CIA analysts receive training that “is consistent with” the policy and are instructed “to review content as it is acquired.” September 13, 2016 Update at 3.⁶² According to a supplemental letter filed on March 13, 2017 (“March 13, 2017 Supp. Letter”), the government monitors compliance with the policy with regard to Section 702 data in an NSA repository called [REDACTED] but otherwise does not comprehensively monitor or verify whether analysts in fact conduct content reviews in conformance with that policy. March 13, 2017 Supp. Letter at 2.⁶³ For that reason,

⁶¹ This content review is in addition to other post-tasking steps to ascertain whether a tasked facility is being used inside the United States, such as [REDACTED]

[REDACTED] Id. § II at 6-7.

⁶² [REDACTED]

[REDACTED] See NSA Targeting Procedures § 2 at 7 n. 2-3.

⁶³ NSA routes most forms of Internet communications acquired under Section 702 to a repository called [REDACTED] March 13, 2017 Supp. Letter at 2. For review of communications in [REDACTED] NSA has [REDACTED] that monitors whether content checks are performed, sends prompts to analysts to conduct [REDACTED] and [REDACTED] reviews, and sends overdue notices. Id. at 1-2. NSA does not have such an alert system for other repositories containing

(continued...)

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

deviations from the policy may not be detected unless and until the circumstances are examined for other purposes. See September 13, 2016 Update at 3.

To address this concern, the government undertakes “to notify the Court . . . when, in connection with compliance incidents, the government also learns that content was not reviewed in accordance with the applicable policy.” Id. at 4. The government further undertakes to advise the FISC “of the total number of instances in which the government’s investigation into a potential [non-compliance] incident revealed that content review was not timely conducted in accordance with [this policy],” even if the government determines that, strictly speaking, there was no violation of the targeting procedures themselves. See id. That figure will be included in each of the government’s quarterly compliance reports. Id.

On March 13, 2017, the government reported the results of an examination of the performance of [REDACTED] and [REDACTED] content reviews for data in [REDACTED] during January-March 2016. March 13, 2017 Supp. Letter at 2. That examination revealed a compliance rate of approximately 79% for [REDACTED] reviews and 99% for [REDACTED] reviews. Id. NSA plans to issue an advisory to personnel reminding them of the policy. Id. at 3.

The Court intends to scrutinize the information submitted regarding future deviations from this policy. It also encourages the government to explore further measures, through

⁶³(...continued)

Section 702 information, though it has plans to develop systems for additional repositories by the end of 2017. Id. at 2-3. FBI and CIA do not have comparable systems. October 4, 2016 Transcript at 21, 24.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

██████ processes or otherwise, to prompt analysts to conduct content reviews in accordance with this policy, and to monitor or verify adherence to it.

C. Issues Arising Under the NSA Minimization Procedures

In addition to the improper use of U.S.-person identifiers to query the results of upstream Internet data discussed above, noteworthy compliance issues have arisen with regard to NSA's upstream collection of Internet communications and querying of Section 702-acquired data.

1. NSA Upstream Collection of Internet Communications

Under the pre-2017 Amendments version of the NSA Minimization Procedures, NSA is required to "take reasonable steps post-acquisition to identify and segregate through technical means" those MCTs that are particularly likely to involve communicants in the United States; specifically, those for which "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." NSA Minimization Procedures § 3(b)(4)a. (prior to the 2017 Amendments). Those procedures permit only certain 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" to access MCTs that have been segregated in the manner described above. § 3(b)(4)a.2. Information in a segregated MCT "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

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

sender and all intended recipients are reasonably believed to be located in the United States.” § 3(b)(4)a.2.(a).⁶⁴

Starting in April 2015, a [REDACTED] error affected NSA’s upstream collection [REDACTED]. See September 30, 2016 Supplemental Notice of Compliance Incident Regarding Collection Pursuant to Section 702 (“September 30, 2016 Supp. Notice”) at 1. The error was discovered on January 26, 2016, and corrected on a going-forward basis the next day. Id.

This [REDACTED] error led to two types of compliance problems. First, it resulted in the unauthorized acquisition of Internet “communications from facilities that only partially matched authorized Section 702 [selectors] (e.g., [REDACTED])” Id. at 1-2. It appears that the government has taken appropriate steps to identify and purge the improperly acquired information. Id. at 2-3. NSA has positively identified [REDACTED] “data objects” as having been subject to this over-collection. Id. In addition, based on the nature of the [REDACTED] error and the technical characteristics of information likely to have been improperly collected due to the error, NSA has identified in excess of [REDACTED] “data objects” that may have been over-collected. Id. at 3. Because it was not technically feasible for NSA to identify within that set any and all objects that actually had been over-collected, NSA has put [REDACTED]-plus objects, as well as the [REDACTED] objects positively identified as having been over-collected, on its MPL. Id.; see also March 17, 2017 Quarterly Report at 114-15.

⁶⁴ In practice, however, no analysts received the requisite training in order to work with the segregated MCTs. October 4, 2016 Transcript at 41-43.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

Second, the [REDACTED] error resulted in failures in the technical processes whereby NSA identified MCTs that are subject to the segregation regime described above. Specifically, some MCTs may have been wrongly identified and labeled as ones in which the active user was the target, which would have resulted in those MCTs not being segregated. September 30, 2016 Supp. Notice at 3-4. To the extent wrongly-identified MCTs were actually ones for which the active user is reasonably believed to have been located in the United States or for whom the active user's location was unknown, they should have been segregated and subject to the above-described heightened access controls. Any large-scale failure to identify and segregate MCTs subject to those heightened access controls would have threatened to undermine one of the safeguards on which the FISC relied in 2011 when it approved the procedures adopted by the government in response to the FISC's prior finding of deficiency. See November 30, 2011 Opinion at 11-15.

The Court did not find entirely satisfactory the government's explanations of the scope of those segregation errors and the adequacy of its response to them and addressed some of its concerns at the October 4, 2016 Hearing. See, e.g., October 4, 2016 Transcript at 35-38.⁶⁵ Questions about the adequacy of steps previously taken to respond to the errors, however, are no longer material to the Court's review of the NSA Minimization Procedures. Under the revised

⁶⁵ The government later reported it had inadvertently misstated the percentage of NSA's overall upstream Internet collection during the relevant period that could have been affected by this [REDACTED] error (the government first reported the percentage as roughly 1.3%, when it was roughly 3.7%). April 11, 2017 Notice of Material Misstatement and Supplemental Notice of Compliance Incidents Regarding Collection Pursuant to Section 702 at 2.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

NSA Minimization Procedures, the results of upstream Internet collection during the relevant timeframe must be segregated and destroyed.

2. Improper Querying [REDACTED] Communications

U.S. person identifiers may be used to query Section 702 data only if they are first “approved in accordance with [internal] NSA procedures, which must require a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information.” NSA Minimization Procedures § 3(b)(5).⁶⁶ In performing such queries, NSA analysts sometimes use a tool called “[REDACTED] [REDACTED]” can be used to query data repositories, including one called [REDACTED] September 30, 2016 Final Notice of Compliance Incidents Regarding Improper Queries (“September 30, 2016 Final Notice”) at 1. [REDACTED] [REDACTED] communications acquired pursuant to Section 702, as well as other FISA authorities. Id.

In May and June 2016, NSA reported to oversight personnel in the ODNI and DOJ that, since approximately 2012, use of [REDACTED] to query communications in [REDACTED] had resulted in inadvertent violations of the above-described querying rules for Section 702 information. Id. The violations resulted from analysts not recognizing the need to avoid querying datasets for which querying requirements were not satisfied or not understanding how to formulate [REDACTED] queries to exclude such datasets. Id. at 1-2.

⁶⁶ As previously noted, NSA may not use U.S.-person identifiers to query the results of upstream Internet collection until the 2017 Amendments take effect, but will be able to run such queries of the narrower form of upstream Internet collection contemplated under the 2017 Amendments, subject to the approval process described above.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

NSA examined all queries using identifiers for “U.S. persons targeted pursuant to Sections 704 and 705(b) of FISA using the [REDACTED] tool in [REDACTED] . . . from November 1, 2015 to May 1, 2016.” *Id.* at 2-3 (footnote omitted). Based on that examination, “NSA estimates that approximately eighty-five percent of those queries, representing [REDACTED] queries conducted by approximately [REDACTED] targeted offices, were not compliant with the applicable minimization procedures.” *Id.* at 3. Many of these non-compliant queries involved use of the same identifiers over different date ranges. *Id.* Even so, a non-compliance rate of 85% raises substantial questions about the propriety of using of [REDACTED] to query FISA data. While the government reports that it is unable to provide a reliable estimate of the number of non-compliant queries since 2012, *id.*, there is no apparent reason to believe the November 2015-April 2016 period coincided with an unusually high error rate.

The government reports that NSA “is unable to identify any reporting or other disseminations that may have been based on information returned by [these] non-compliant queries” because “NSA’s disseminations are sourced to specific objects,” not to the queries that may have presented those objects to the analyst. *Id.* at 6. Moreover, [REDACTED] query results are generally retained for just [REDACTED] *Id.*⁶⁷

The NSA has taken steps to educate analysts on the proper use of [REDACTED] it has provided a “reminder” to all analysts about the need “to limit queries across authorities in [REDACTED] with

⁶⁷ Information retrieved by an improper query might nonetheless satisfy the requirements for dissemination; indeed, absent a second violation of the minimization procedures, separate from the improper query, one would expect any disseminated information to have satisfied those requirements.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

an explanation of how different types of queries operate; it issued a separate “Compliance Advisory,” which further addressed querying practices using ██████ to all NSA target offices; and it revised a “banner” presented to users of ██████ to emphasize that U.S. person identifiers should never be used for a type of query (called a “selector query”) that runs “against all data [that] an analyst is authorized to access.” *Id.* at 1, 6.

At the October 4, 2016 Hearing, the government represented that, based on ongoing oversight efforts, those measures appear to have been effective in improving how analysts use ██████ to query Section 702 data. October 4, 2016 Transcript at 47-49. On April 3, 2017, the government reported to the Court that it had reaffirmed that assessment, based on discussions with NSA analysts and the absence of additional non-compliant queries using ██████ April 3, 2017, Supplemental Notice of Compliance Incidents Regarding Improper Queries, at 3. In view of these remedial steps, the Court believes that, notwithstanding the above-described non-compliance, the NSA Minimization Procedures meet the statutory definition of “minimization procedures” and are consistent with the requirements of the Fourth Amendment.

D. Issues Arising Under the FBI Minimization Procedures

The following violations of the FBI’s minimization procedures merit discussion.

1. Improper Disclosures of Raw Information

On March 9, 2016, DOJ oversight personnel conducting a minimization review at the FBI’s ██████ learned that the FBI had disclosed raw FISA information, including but not limited to Section 702-acquired information, to a ██████ ██████ ██████ Compliance Report at 92. ██████ is part of the ██████

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED] and “is largely staffed by private contractors” [REDACTED]
[REDACTED] certain [REDACTED] contractors had access to raw FISA
information on FBI storage systems [REDACTED] Id. The apparent purpose for the
FBI’s granting such access was to receive analytical assistance from [REDACTED] [REDACTED]
[REDACTED]

[REDACTED] Nonetheless, the [REDACTED] contractors had access to raw
FISA information that went well beyond what was necessary to respond to the FBI’s requests;
[REDACTED]

[REDACTED] The FBI discontinued the above-described access to raw FISA information as of April 18,
2016. [REDACTED]

The contractors in question received training on the FBI minimization procedures, stored
the raw information only on FBI systems, and did not disseminate it further. Id. at 93.
Nonetheless, the above-described practices violated the governing minimization procedures.
Section III.A of the FBI’s minimization procedures (as then in effect and as now proposed)
provides: “The FBI must retain all FISA-acquired information under appropriately secure
conditions that limit access to such information only to authorized users in accordance with these
and other applicable FBI procedures. These retention procedures apply to FISA-acquired
information retained in any form.” The FBI may disseminate Section 702-acquired information
only in accordance with Section V of those procedures. FBI Minimization Procedures § III.C.1.

Under Section V.D of those procedures, personnel working for another federal agency
such as [REDACTED] may receive raw information acquired under Section 702 in order to

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

provide technical or linguistic assistance to the FBI, but only if certain restrictions are followed.

See id. § V.D. Those restrictions were not in place with regard to the [REDACTED] contractors: their access was not limited to raw information for which the FBI sought assistance and access continued even after they had completed work in response to an FBI request. See [REDACTED]

Compliance Report at 93. At the October 4, 2016 Hearing, the government represented that it was investigating whether there have been similar cases in which the FBI improperly afforded non-FBI personnel access to raw FISA-acquired information on FBI systems. October 4, 2016 Transcript at 64.

In a separate violation of its minimization procedures, the FBI delivered raw Section 702-acquired information to a [REDACTED] contractor called [REDACTED]

[REDACTED] Compliance Report at 131. The information in question pertains to [REDACTED]

[REDACTED] accounts tasked under Section 702. Id. [REDACTED]

[REDACTED] as a federal agency, could receive raw Section 702-acquired information in order to provide technical assistance to the FBI, subject to the requirements of Section V.D of the FBI Minimization Procedures. See FBI Minimization Procedures § V.D (“FBI is authorized to

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

disclose FISA-acquired information to assisting federal agencies for further processing and analysis,” subject to specified restrictions) (emphasis added). [REDACTED] however, is not a federal agency and the [REDACTED] personnel who worked with the information were “not directly supervised by or otherwise under the direction and control of [REDACTED] Compliance Report at 132. For these reasons, the government concluded that the FBI had given the information to the private entity [REDACTED], not to an assisting federal agency. See id.⁶⁸



The government has not

explained why giving [REDACTED] personnel access to the raw information during installation of the tool would not involve a separate violation of the FBI Minimization Procedures. Accordingly, the Court is ordering the government to provide additional information regarding this second grant of access to raw Section 702 information.

These violations, when placed in the context of Section 702 acquisitions in their entirety, do not preclude a finding that the FBI Minimization Procedures meet the statutory definition of “minimization procedures” and are consistent with the requirements of the Fourth Amendment.

⁶⁸ In contrast, the above-described [REDACTED] contractors worked in a federal facility under the supervision of [REDACTED] Compliance Report at 93. It appears that the government views the above-described disclosures of information to the [REDACTED] contractors as disclosures to a federal agency, rather than to a private entity or private individuals. In any event, the government acknowledges that those disclosures were improper for other reasons, so the Court need not reach this question.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

The improper access previously afforded the [REDACTED] contractors has been discontinued, while the information disclosed to [REDACTED] pertains to just [REDACTED] tasked selectors.

The Court is nonetheless concerned about the FBI's apparent disregard of minimization rules and whether the FBI may be engaging in similar disclosures of raw Section 702 information that have not been reported.⁶⁹ Accordingly, the Court is directing the government to provide additional as described below.

2. Potential Over-Retention of Section 702 Information

Last year, in the context of approving the standard minimization procedures employed by the FBI for electronic surveillance and physical search conducted under Titles I and III of FISA, a judge of the FISC observed:

FBI personnel who develop storage systems for FISA-acquired information and decide under what circumstances FISA-acquired information is placed on those systems are bound by applicable minimization procedures and FISC orders, no less so than an agent conducting a FISC-authorized physical search or an analyst preparing a report for dissemination.

Docket No. [REDACTED], Opinion and Order at 45 (FISA Ct. May 17, 2016). Recent disclosures regarding [REDACTED] systems maintained by the FBI suggest that raw FISA

⁶⁹ The improper access granted to the [REDACTED] contractors was apparently in place [REDACTED] and seems to have been the result of deliberate decisionmaking. [REDACTED] Compliance Report at 92-93 ([REDACTED] access to FBI systems was the subject of an interagency memorandum of understanding entered into [REDACTED]). Despite the existence of an interagency memorandum of understanding (presumably prepared or reviewed by FBI lawyers), no notice of this practice was given to the FISC until 2016. Of course, such a memorandum of understanding could not override the restrictions of Section 702 minimization procedures.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

information, including Section 702 information, may be retained on those systems in violation of applicable minimization requirements. [REDACTED]⁷⁰



The government has not identified the provisions of the FBI Minimization Procedures it believes are implicated by the above-described retention practices. Based on the information

70



~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

provided, however, those practices appear inconsistent with the provisions governing retention on electronic and data storage systems, see FBI Minimization Procedures § III.G.1, on ad hoc systems, id. § IV.A-B, and in connection with litigation, id. § III.G.4. Nearly four months ago, the government undertook to address this indefinite retention of information on the above-described systems in a subsequent filing, see December 29, 2016 Report at 10-11, but has not done so. Accordingly, the Court is directing the government to provide pertinent information, as described below.

3. Review Teams for Attorney-Client Communications

The Section 702 minimization procedures

have specific rules for handling attorney-client communications. Because the FBI has law enforcement responsibilities and often works closely with prosecutors in criminal cases, its procedures have detailed requirements for cases in which a target is known to be charged with a federal crime. Unless otherwise authorized by the [National Security Division of DOJ], the FBI must establish a separate review team whose members have no role in the prosecution of the charged criminal matter to conduct the initial review of such a target's communications. When that review team identifies a privileged communication concerning the charged criminal matter, the original record or portion thereof containing that privileged communication is sequestered with the FISC and other copies are destroyed (save only any electronic version retained as an archival backup, access to which is restricted).

November 6, 2015 Opinion at 47-48 (citations and internal quotation marks omitted).

Failures of the FBI to comply with this "review team" requirement for particular targets have been a focus of the FISC's concern since 2014. See id. at 48-52; August 26, 2014 Opinion at 35-36. The government generally ascribed those failures to misunderstanding or confusion on the part of individuals – for example, when an agent is generally aware of the review team requirement but mistakenly believes that it does not apply when the charging instrument is under

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

seal. November 6, 2015 Opinion at 50. The government advised that it was emphasizing the review team requirement in ongoing training and oversight efforts, and that such emphasis had resulted in the identification and correction of additional cases in which review teams had not been properly established. Id. at 51.

[REDACTED]

[REDACTED] targets who have been subject to criminal charges [REDACTED] there was a delay of over two years in establishing review teams. See [REDACTED] Preliminary Notice of Compliance Incident Regarding [REDACTED] Section 702-Tasked Facilities (“ [REDACTED] Preliminary Notice”) at 2-3. The primary cause of this delay was that the responsible case agent was unaware of the review team requirement. That agent took the appropriate steps after reviewing an advisory that reminded FBI personnel about the requirement in [REDACTED] Id. at 3.⁷¹ The government also reported a delay of approximately one month during [REDACTED] before establishing a review team after a target was charged in a sealed complaint. The delay appears to have been the result of lack of coordination among FBI field offices. According to the government, the review teams have completed examination of communications acquired prior to

[REDACTED]

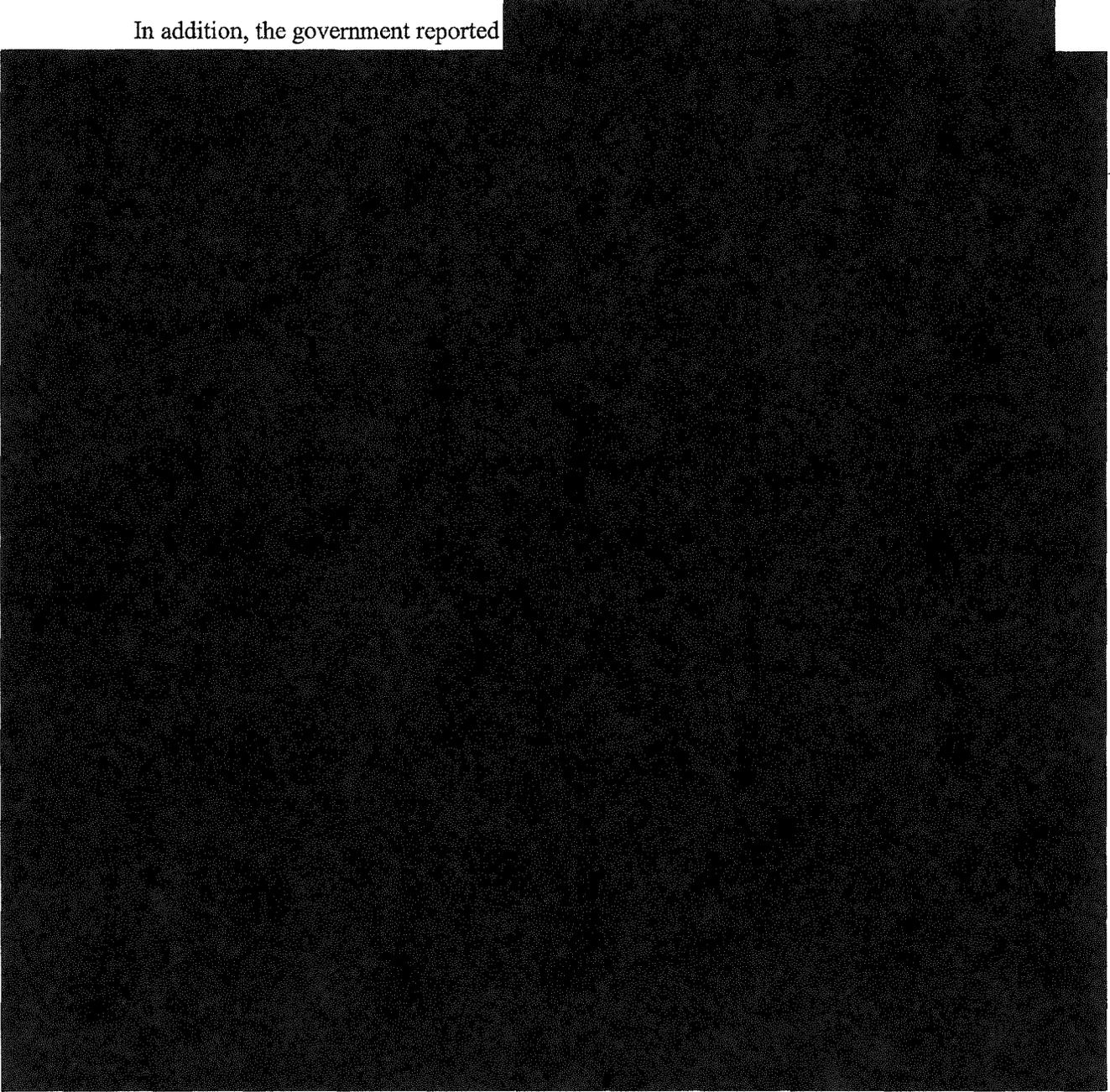
~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

their creation for both incidents and did not discover any privileged communications. [REDACTED]

[REDACTED] Compliance Report at 77, 105.

In addition, the government reported [REDACTED]



~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



A separate source of under-inclusiveness is when personnel do not identify and segregate communications for [REDACTED]



[REDACTED] FBI examination of the erroneously-excluded communications is ongoing and, so far, has not identified any attorney-client privileged communications concerning a charged matter. [REDACTED] Compliance Report at 119.

A different [REDACTED] problem affected [REDACTED] [REDACTED] accounts during November 28-30, 2016. That problem has been solved prospectively. Although some communications for

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

those tasked accounts were accessed before being segregated for the review team, none of them contained privileged information. Id. at 83 n.58.

In order to address some of the sources of such under-inclusiveness, the FBI has implemented a new [REDACTED] process for [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In addition, the FBI and NSA have taken steps to address the difficulties encountered with regard to [REDACTED] Id. at 4.

It seems clear that the review team requirement should continue to be a point of emphasis in the government's training and oversight efforts. The measures taken to improve processes for identifying and routing information subject to the review team requirement appear well-suited to address the described under-inclusiveness problems. In view of those efforts, and the fact that lapses to date appear to have resulted in few, if any, privileged communications concerning charged matters being reviewed by investigators other than review team members, errors in implementing the review team requirements do not preclude a finding that the FBI Minimization Procedures meet the statutory definition of "minimization procedures" and are consistent with the requirements of the Fourth Amendment.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

E. Issues Arising Under the CIA Minimization Procedures

In the course of investigating a separate compliance incident that occurred in December 2016,⁷² the CIA discovered several problems with its purge practices. First, the software script used to identify communications subject to purge requirements within a storage system [REDACTED]

[REDACTED] had not been identifying all communications subject to purge that had been acquired by

[REDACTED] December 28, 2016, Preliminary Notice of Compliance Incidents and Material Misstatements Regarding Collection Pursuant to Title I and Title III and Section 702 of FISA, at 4. As of March 29, 2017, CIA was in the process of remedying the incomplete purges. Supplemental Notice Regarding Incomplete Purges of Collection Acquired Pursuant to Section 702 of FISA, filed on March 29, 2017 (“March 29, 2017 Supp. Notice”) at 2.

Further investigation of the December 2016 incident revealed similar problems with scripts used to purge metadata from [REDACTED] CIA repositories [REDACTED]. March 29, 2017 Supp. Notice at 2-3. The government reports CIA has corrected those script problems and completed the required purges, except for certain information relating [REDACTED] facilities, for which remedial efforts are ongoing. *Id.* at 3 & n.4.

⁷² That incident appears to have been remedied, *see id.* at 3, and in and of itself does not merit discussion in this Opinion.

⁷³ [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

In late March 2017, also in the course of investigating the December 2016 incident, CIA discovered another form of purging error affecting [REDACTED] March 24, 2017, Notice of Compliance Incident Regarding Incomplete Age Off of Data Acquired Pursuant to Section 702 of FISA at 2. The government is examining the scope of that error. Id.

The government has not advised the Court for how long these various purge-related problems persisted before CIA discovered them in the course of investigating the separate incident. It appears that, having recognized the problems, CIA is taking reasonable steps to address them. Nonetheless, the Court encourages the government to take proactive measures to verify that the automated processes upon which it relies to implement minimization requirements are functioning as intended.

V. CONCLUSION

For the foregoing reasons, the Court finds that: (1) the 2016 Certifications, as amended by the 2017 Amendments, as well as the certifications in the Prior 702 Dockets as amended by those documents, contain all the required statutory elements; (2) the targeting and minimization procedures to be implemented regarding acquisitions conducted pursuant to the 2016 Certifications, as amended by the 2017 Amendments, comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment; and (3) the minimization procedures to be implemented regarding information acquired under prior Section 702 certifications comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment. Orders approving the amended certifications and use of the accompanying procedures are being entered contemporaneously herewith.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

For the reasons discussed above, it is HEREBY ORDERED as follows:

1. Raw information obtained by NSA's upstream Internet collection under Section 702 shall not be provided to FBI, CIA or NCTC unless it is done pursuant to revised minimization procedures that are adopted by the AG and DNI and submitted to the FISC for review in conformance with Section 702.

2. The government shall take steps to ensure that NCTC retains raw Section 702-acquired information that is determined to be evidence of a crime but not foreign intelligence information beyond the generally applicable age-off period specified in Section B.2 of the NCTC Minimization Procedures only as long as reasonably necessary to serve a law enforcement purpose and that NCTC does not use or disclose such information other than for a law enforcement purpose. The government shall report in writing on such steps when it seeks to renew or amend [REDACTED].

3. On or before December 31 of each calendar year, the government shall submit a written report to the FISC: (a) describing all administrative, civil or criminal litigation matters necessitating preservation by FBI, NSA, CIA or NCTC of Section 702-acquired information that would otherwise be subject to destruction, including the docket number and court or agency in which such litigation matter is pending; (b) describing the Section 702-acquired information preserved for each such litigation matter; and (c) describing the status of each such litigation matter.

4. The government shall promptly submit a written report describing each instance in which FBI, NSA, CIA or NCTC invokes the provision of its minimization procedures stating that

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

nothing in those procedures shall prohibit the “retention, processing, analysis or dissemination of information necessary to comply with a specific congressional mandate or order of a court within the United States[.]” See NSA Minimization Procedures § 1; CIA Minimization Procedures § 6.g; FBI Minimization Procedures § I.G; NCTC Minimization Procedures § A.6.d. Each such report shall describe the circumstances of the deviation from the procedures and identify the specific mandate on which the deviation was based.

5. The government shall promptly submit a written report describing any instance in which an agency departs from any provision in its minimization procedures in reliance in whole or in part on the provision therein for lawful oversight when responding to an oversight request by an entity other than the oversight entities expressly referenced in the agency’s procedures. See NSA Minimization Procedures § 1; CIA Minimization Procedures § 6.f; FBI Minimization Procedures § I.G; NCTC Minimization Procedures § A.6.e. Each such report shall describe the circumstances of the deviation from the procedures and identify the specific oversight activity on which the deviation was based.

6. No later than June 16, 2017, the government shall submit a written report:
- (a) describing the extent to which raw FISA information, including Section 702 information, is retained:



~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

- (b) assessing whether such retention complies with applicable minimization requirements; and
 - (c) to the extent that noncompliance is found, describing the steps the government is taking or plans to take to discontinue the above-described forms of retention or bring them into compliance with applicable minimization requirements.
-

7. No later than June 16, 2017, the government shall submit one or more written reports that provide the following:

(a) the results of the government's investigation of whether there have been additional cases in which the FBI improperly afforded non-FBI personnel access to raw FISA-acquired information on FBI systems; and

(b) a description of the installation of the [REDACTED] by [REDACTED] personnel on an FBI system, including:



8. At 90-day intervals, the government shall submit written updates on NSA's implementation of the above-described sequester-and-destroy process to information acquired on or before March 17, 2017, by upstream Internet collection under Section 702.

9. If the government intends not to apply the above-described sequester-and-destroy process to information acquired on or before March 17, 2017, by upstream Internet collection

~~TOP SECRET//SI//ORCON/NOFORN~~

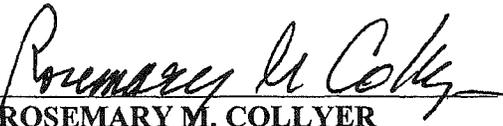
~~TOP SECRET//SI//ORCON/NOFORN~~

under Section 702 because the information is not contained in an “institutionally managed repository,” it shall describe the relevant circumstances in a written submission to be made no later than June 2, 2017; however, the government need not submit such a description for circumstances referenced in this Opinion and Order as ones in which NSA could retain such information.

10. The government shall promptly submit in writing a report concerning each instance 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. The report should include a detailed description of the information at issue and the manner in which it has been or will be used for analytical, investigative or evidentiary purposes. It shall also identify the query terms used to elicit the information and provide the FBI’s basis for concluding that the query was consistent with applicable minimization procedures.

ENTERED this 26 day of April, 2017, in Docket Nos. [REDACTED]

[REDACTED]


ROSEMARY M. COLLYER
Judge, United States Foreign
Intelligence Surveillance Court

I, [REDACTED], Chief Deputy Clerk,
FISC, certify that this document is a
true and correct copy of the original.

[REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

Exhibit 30

~~TOP SECRET//SI//NOFORN//20320108~~

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

EXHIBIT A

**PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING 3: 56
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

~~TOP SECRET//SI//NOFORN//20320108~~

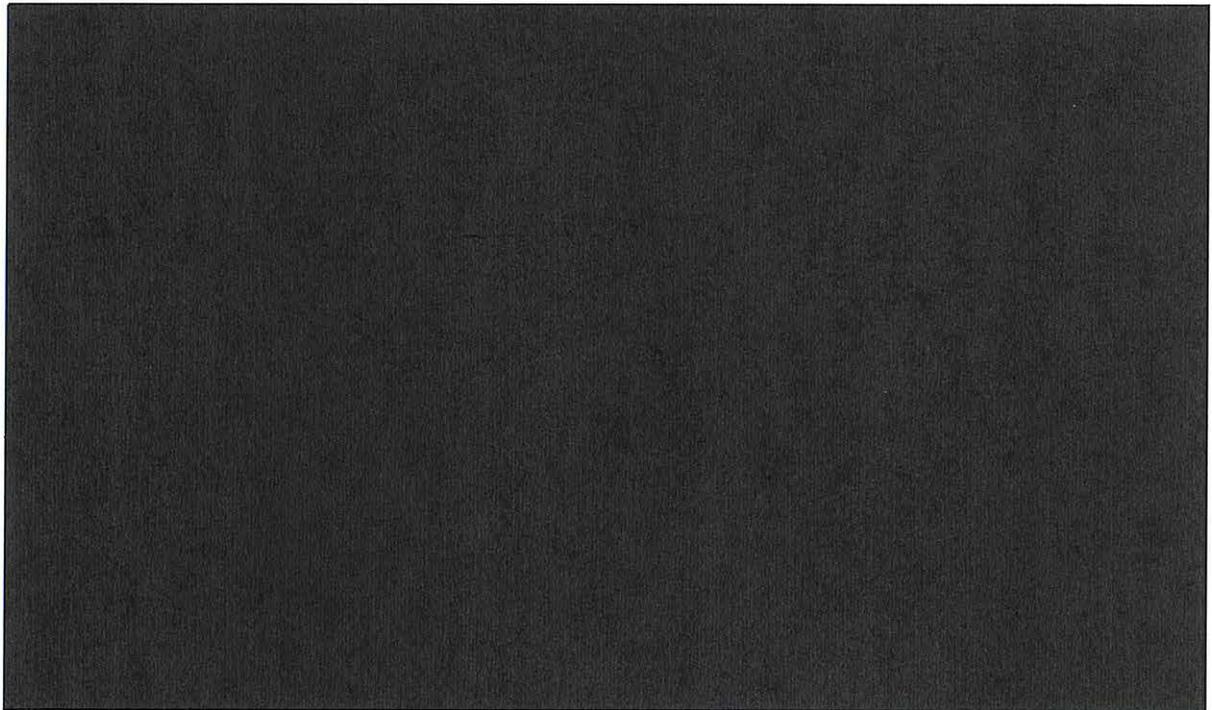
~~TOP SECRET//SI//NOFORN//20320108~~

~~(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:



(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].

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~

[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]

[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]

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~

[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:

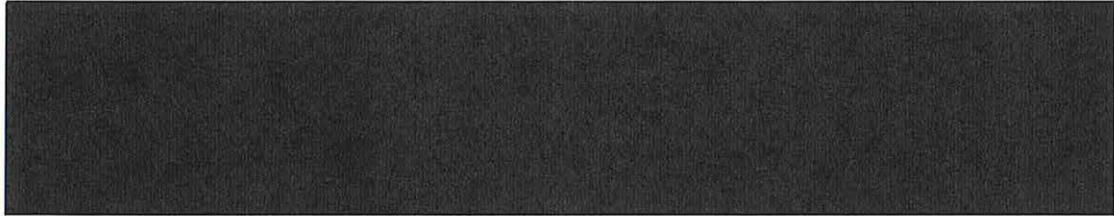
- [REDACTED]

¹ (TS//SI//NF) [REDACTED]

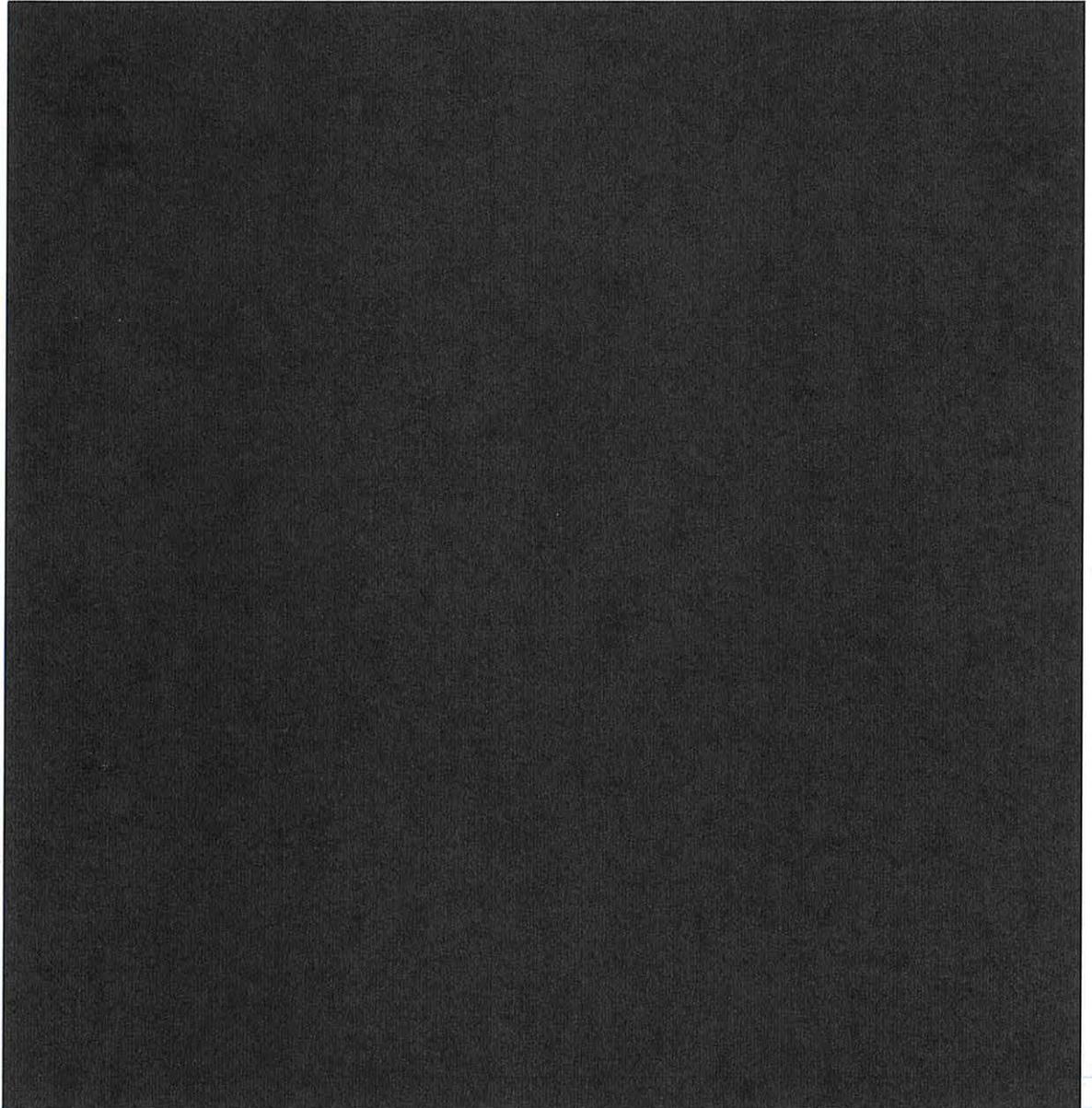
[REDACTED]

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~

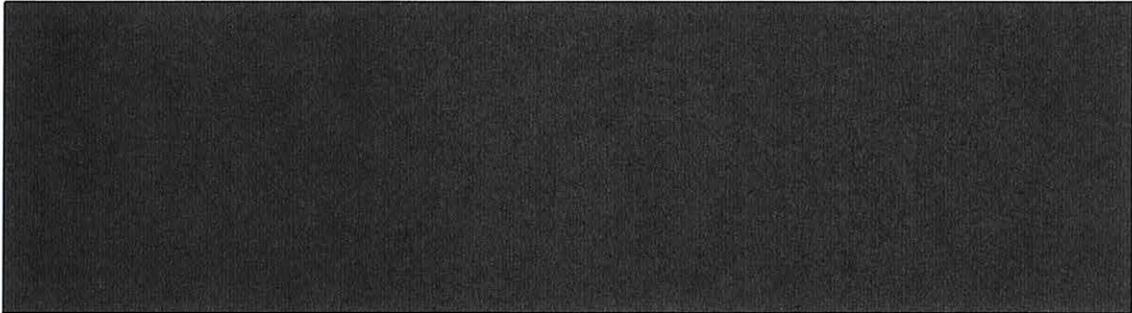


b. With respect to Internet communications:



~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~



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:



- 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]



~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~

[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]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

³ (S) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~

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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~

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.

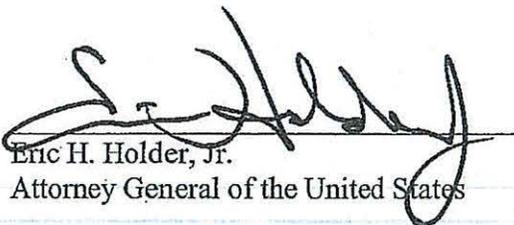
(S) In the event that NSA concludes that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person 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

~~TOP SECRET//SI//NOFORN//20320108~~