ATTACHMENT

~~TOP SECRET//SI//ORCON/NOFORN~~

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

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

CLASSIFIED DECLARATION OF GEORGE C. BARNES,
DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

(U) TABLE OF CONTENTS

I. (U) INTRODUCTION 1

II. (U) CLASSIFICATION OF DECLARATION 2

III. (U) SUMMARY 3

IV. (U) BACKGROUND 8

A. (U) The National Security Agency and Its Signals Intelligence Mission 8

B. (U) External Threats to the National Security of the United States 10

C. (U) Collection of Communications Content Pursuant to FISA Section 702 13

D. (U) Upstream Collection 17

E. (U) The Wikimedia Discovery Requests 22

V. (U) INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE 27

VI. (U) HARM OF DISCLOSURE OF PRIVILEGED INFORMATION 30

A. (U) Information Concerning Whether Communications of Wikimedia or of Other Entities or Individuals Have Been Subjected to Upstream Surveillance Activities 30

B. (U) Operational Details of the Upstream Collection Process 37

C. (U) Location(s) on the Internet Backbone Where Upstream Surveillance Is Conducted .. 44

D. (U) Categories of Internet-Based Communications Subject to Upstream Surveillance Activities 51

E. (U) Scope and Scale of Upstream Surveillance 54

F. (~~S//NF~~) NSA's Capabilities, or Lack Thereof, to Decrypt, Circumvent, or Defeat Communications Security Protocols 58

G. (U) Additional Categories of Classified Information Contained in Opinions, Orders, and Court Submissions Concerning Upstream Surveillance 60

VII. (U) CONCLUSION 65

(U) I, George C. Barnes, for my declaration pursuant to 28 U.S.C. § 1746, depose and say as follows:

I. (U) INTRODUCTION

1. **(U)** I am the Deputy Director of the National Security Agency ("NSA"), an intelligence agency within the Department of Defense. I have held this position since May 1, 2017. Prior to serving as Deputy Director, I served as the Director, Workforce Support Activities Directorate, and have been an NSA employee since 1987. I have served in a variety of roles at the Agency, including as NSA's Special United States Liaison Officer in London, where I supported our cryptologic partnership with the United Kingdom and interacted regularly with key U.K. intelligence and cybersecurity leadership, as well as the Chief of Data Acquisition, overseeing NSA's signals intelligence access, collection, and exploitation. I have been designated an original TOP SECRET classification authority under Executive Order No. 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Manual No. 5200.1, Vol. 1, Information and Security Program (Feb. 24, 2012).

2. **(U)** The purpose of this declaration is to support an assertion of the military and state secrets privilege (hereinafter, "state secrets privilege") by the Director of National Intelligence ("DNI") in his capacity as head of the Intelligence Community, as well as the DNI's assertion of a statutory privilege under the National Security Act of 1947, *see* 50 U.S.C. § 3024(i)(1), to protect the information described below. The information in question is sought in discovery by the Plaintiff in the above-captioned case, Wikimedia Foundation ("Wikimedia"), and concerns critical NSA intelligence-gathering activities and capabilities. This information is classified, extraordinarily sensitive, and its disclosure reasonably could be expected to cause exceptionally grave damage to the national security of the United States. Through this declaration, I also

hereby invoke and assert the NSA's statutory privilege set forth in Section 6 of the National Security Agency Act of 1959, Public Law No. 86-36 (codified at 50 U.S.C. § 3605(a)), to protect information related to NSA intelligence activities as described herein.

3. **(U)** The statements made herein are based on my personal knowledge of NSA activities and operations, and on information made available to me in my official capacity as the Deputy Director of NSA.

II. (U) CLASSIFICATION OF DECLARATION

4. **(U)**This declaration is classified TOP SECRET//SI//ORCON/NOFORN pursuant to the standards in Executive Order No. 13526. *See* 75 Fed. Reg. 707 (Dec. 29, 2009). Under Executive Order No. 13526, information is classified "TOP SECRET" if unauthorized disclosure of the information reasonably could be expected to cause exceptionally grave damage to the national security of the United States; "SECRET" if unauthorized disclosure of the information reasonably could be expected to cause serious damage to national security; and "CONFIDENTIAL" if unauthorized disclosure of the information reasonably could be expected to cause identifiable damage to national security. At the beginning of each paragraph of this declaration, the letter or letters in parentheses designate(s) the level of classification of the information the paragraph contains. When used for this purpose, the letters "U," "C," "S," and "TS" indicate respectively that the information is either UNCLASSIFIED, or is classified CONFIDENTIAL, SECRET, or TOP SECRET.

5. **(U)** Additionally, this declaration contains Sensitive Compartmented Information (SCI), which is "information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods." 28

C.F.R. § 17.18(a). Because of the exceptional sensitivity and vulnerability of such information, these safeguards and access requirements exceed the access standards that are normally required for information of the same classification level. Specifically, this declaration references communications intelligence ("COMINT"), also referred to as special intelligence ("SI"), which is a subcategory of SCI. COMINT or SI identifies SCI that was derived from exploiting cryptographic systems or other protected sources by applying methods or techniques, or from foreign communications.

6. **(U)** Finally, the "ORCON" designator means that the originator of the information controls to whom it is released. In addition to the fact that classified information contained herein and that is contained within the accompanying documents may not be revealed to any person without authorization pursuant to Executive Order 13526, this declaration and many of the accompanying documents contain information that may not be released to foreign governments, foreign nationals, or non-U.S. citizens without permission of the originator and in accordance with DNI policy. This information is labeled "NOFORN."

7. **(U)** Accordingly, none of the information in this declaration can be removed from classified channels without prior classification review by NSA.

III. (U) SUMMARY

8. **(U)** I have been informed that Wikimedia alleges that a technique employed by the NSA to gather foreign intelligence information under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), known as Upstream surveillance,[1] exceeds the Government's

[1] ~~(TS//SI//NF)~~ [redacted]

authority under FISA, violates the Constitution, and should be permanently enjoined. It is my understanding that the question now before the Court for resolution is whether Wikimedia has legal standing to assert these claims. In an effort to prove its standing, Wikimedia has served a total of 84 discovery requests on the Government, including interrogatories, requests for admission, and document requests. Wikimedia has also taken the deposition of a designated NSA official under Federal Rule of Civil Procedure 30(b)(6). Wikimedia's discovery requests and deposition questions are apparently intended to uncover direct and indirect evidence to support Wikimedia's standing to challenge Upstream surveillance.

9. **(U)** It is my understanding that although the NSA and the other Defendant Government agencies responded to many of Wikimedia's discovery requests, the Government also objected in whole or in part to certain requests based, *inter alia*, on the classified, privileged, and extraordinarily sensitive nature of the national security information Wikimedia sought. The Government also objected to and refused to answer certain deposition questions because they, too, called for classified, privileged, and extraordinarily sensitive national security information. In particular, the Government has objected to any discovery requests or deposition questions that would tend to reveal whether Wikimedia's communications have been subject to Upstream surveillance; operational details of Upstream surveillance; the locations on the Internet backbone where Upstream surveillance is or has been conducted; the types of communications collected through Upstream surveillance; the scope of Upstream surveillance; NSA's cryptanalytic capabilities; and certain additional categories of classified information contained in opinions by, orders from, and submissions to, the Foreign Intelligence Surveillance Court ("FISC") regarding

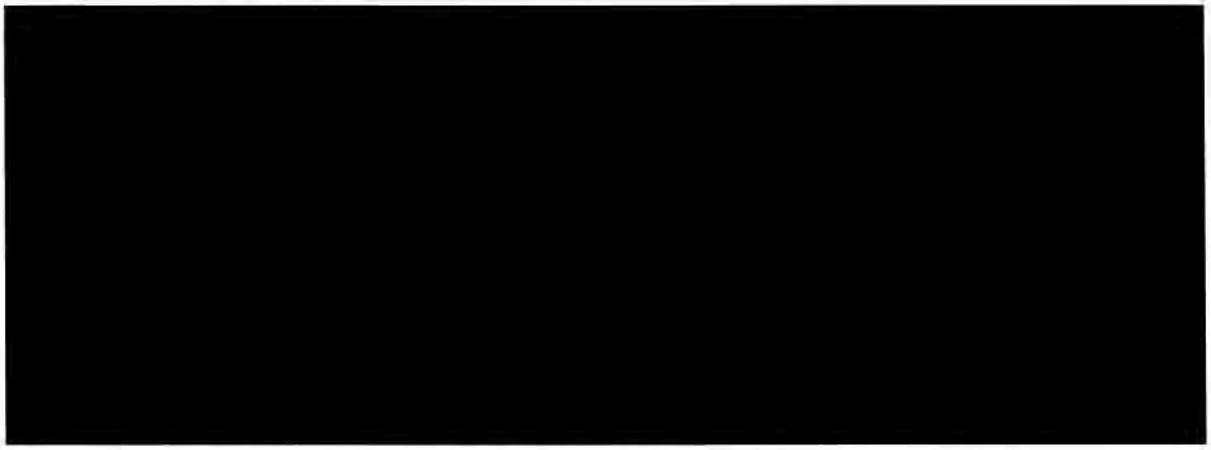
Upstream surveillance. Wikimedia has now moved to compel the disclosure of this classified, privileged, and extraordinarily sensitive national security information.

10. **(U)** This declaration supports the assertion of the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1) by the DNI over the classified information that Wikimedia seeks, whether in response to Wikimedia's pending discovery requests, in response to any further discovery requests Wikimedia may serve in this case, or as otherwise may be necessary to litigate Wikimedia's claims or the Government's defenses in this case. I also assert herein the NSA's statutory privilege under 50 U.S.C. § 3605(a) over the same categories of information. As set forth in the accompanying public declaration of the DNI, and explained in classified detail below, the disclosure of the information and documents that Wikimedia seeks could reasonably be expected to cause exceptionally grave damage to the national security of the United States, and therefore must be protected from disclosure and excluded from this case.

11. **(~~TS//SI//NF~~)** [redacted]

[redacted]

[2] **(~~TS//SI//NF~~)** [redacted]



12. **(U)** The facts at issue include, first, whether or not any of Wikimedia's communications, or of other individuals and entities, have been subject to Upstream surveillance. As a matter of course, the Government cannot publicly confirm or deny whether any individual or organization is or has been subject to NSA intelligence-gathering activities, because to do so would tend to reveal to our adversaries who are the NSA's actual targets of surveillance and who are not, which channels of communication are free from NSA surveillance and which are not, and other sensitive intelligence methods and sources, thereby helping our adversaries evade detection and capitalize on limitations in the NSA's surveillance capabilities.

13. **(U)** As further explained below, it is also essential to protect information concerning the operational details of Upstream surveillance, as well as the location(s) on the Internet "backbone" where Upstream surveillance is conducted; the types of communications collected through Upstream surveillance; the scale and scope of Upstream surveillance; NSA's cryptanalytic capabilities; and additional categories of classified information contained in opinions, orders, and submissions to the FISC concerning Upstream surveillance that Wikimedia seeks in discovery. Notwithstanding the Government's disclosure of certain facts, in order to promote transparency and public understanding about the Upstream program, the additional

disclosure of the information Wikimedia seeks to compel could reasonably be expected to cause exceptionally grave damage to national security.

14. **(U)** Most obviously, the disclosure of the information Wikimedia seeks would reveal to foreign adversaries the NSA's operational methods and capabilities (or lack thereof), and specific channels of communication from which the NSA has in the past and continues today to obtain intelligence information, thus enabling them to evade particular channels that are being monitored, to exploit channels that are not subject to NSA collection, to target for hostile action the facilities where the NSA obtains critical foreign intelligence, and to exploit the NSA's sources and methods of surveillance for their own purposes. In addition, the information that Wikimedia seeks would also tend to reveal the identities of specific foreign targets of foreign intelligence surveillance that NSA conducts pursuant to Section 702, alerting them that their activities have been detected by the U.S. Intelligence Community. In all cases, these disclosures would risk exceptionally grave damage to national security.

15. **(U)** For all of these reasons and others explained below, I support the DNI's assertion of the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1) to prevent the disclosure of information falling within the categories described herein. I also assert the NSA's statutory privilege under Section 6 of the National Security Agency Act, 50 U.S.C. § 3605(a), over the same information, which concerns NSA intelligence functions. The information Wikimedia seeks must be protected from disclosure and excluded from this case to avoid risking exceptionally grave damage to the national security of the United States

IV. (U) BACKGROUND

A. (U) The National Security Agency and Its Signals Intelligence Mission

16. **(U)** The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. The NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate signals intelligence ("SIGINT") information, of which COMINT is a significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations. *See* Executive Order 12333, § 1.7(c), as amended.[3]

17. **(U)** SIGINT consists of three subcategories: (1) COMINT; (2) electronic intelligence ("ELINT"); and (3) foreign instrumentation signals intelligence ("FISINT"). COMINT is defined as "all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients." 18 U.S.C. § 798. COMINT includes information derived from the interception of foreign and international communications, such as voice, facsimile, and computer-to-computer information conveyed via a number of means (*e.g.*, microwave, satellite links, high frequency/very high frequency ("HF/VHF") broadcast). ELINT is technical intelligence information derived from foreign non-communications electromagnetic radiations except atomic detonation or radioactive sources—in essence, radar systems affiliated with military weapons platforms (*e.g.*, anti-ship) and civilian systems (*e.g.*, shipboard and air traffic control radars). FISINT is derived from the

[3] **(U)** Executive Order 12333, reprinted as amended in 50 U.S.C § 3001 note, generally describes the NSA's authority to collect foreign intelligence not subject to FISA's definition of electronic surveillance, including activities undertaken abroad. Section 1.7(c) of E.O. 12333, as amended, specifically authorizes the NSA to "[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information for foreign-intelligence and counterintelligence purposes to support national and departmental missions."

intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems.

18. **(U)** The NSA's SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities set forth in E.O. 12333, § 1.7(c)(2), as amended, and 50 U.S.C. § 3038(b)(1). In performing its SIGINT mission, the NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications and related information. The technological infrastructure that supports the NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated electronic data collection and processing technology.

19. **(U)** There are two primary reasons for gathering and analyzing foreign intelligence information. The first, and most important, is to gain information required to direct U.S. resources as necessary to counter external threats and in support of military operations. The second reason is to obtain information necessary to the formulation and promotion of U.S. foreign policy. Foreign intelligence information provided by the NSA is thus relevant to a wide range of important issues, including military order of battle; threat warnings and readiness; cybersecurity; arms proliferation; international terrorism; counterintelligence; and foreign aspects of international narcotics trafficking.

20. **(U)** The NSA's ability to produce foreign intelligence information depends on its access to foreign and international electronic communications. Foreign intelligence produced by COMINT activities, of which NSA's acquisition of foreign communications pursuant to FISA (to include Upstream 702 collection) is a subset, is an extremely important part of the overall foreign intelligence information available to the United States and is often unobtainable by other

means. Public disclosure of either the capability to collect specific communications or the substance of the information derived from such collection itself can easily alert targets to the vulnerability of their communications. Disclosure of even a single communication holds the potential of revealing intelligence collection techniques that are applied against targets around the world. Once alerted, targets can frustrate COMINT collection by using different or new encryption techniques, by disseminating disinformation, or by utilizing a different communications link. Such evasion techniques may inhibit access to the target's communications and therefore deny the United States access to information crucial to the defense of the United States both at home and abroad. COMINT is provided special statutory protection under 18 U.S.C. § 798, which makes it a crime to knowingly disclose to an unauthorized person classified information "concerning the communication intelligence activities of the United States or any foreign government." Disclosure of the NSA's Upstream collection techniques would also negatively impact the Agency's ability to execute COMINT activities pursuant to E.O. 12333, given the overlap in the technical and operational details of both sets of collection activities.

B. (U) External Threats to the National Security of the United States

21. **(U)** The threat of international terrorism originally gave rise to the NSA intelligence activities challenged in this lawsuit. As a result of the unprecedented attacks of September 11, 2001, the United States found itself immediately propelled into a conflict with al Qaeda and its associated forces, and later their successors, groups that still possess the evolving capability and intention of inflicting further attacks on the United States.

22. **(~~S//NF~~)** [redacted]

[redacted]

[redacted]

23. (~~TS//SI//NF~~) [redacted]

[redacted]

24. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

25. **(U)** Protecting U.S. national security against our foreign adversaries therefore presents critical challenges for the Nation's communications intelligence capabilities. One advantage enjoyed by the NSA in meeting these challenges stems from the fact that the United States long has been and remains a critical hub for the transmission and routing of electronic

[4] **(~~S//NF~~)** [redacted]

communications traveling on the global telecommunications network. Because of the United States' position as a global communications hub, hostile foreign actors often communicate using providers or services based in the United States, but, even when the NSA's foreign intelligence targets use foreign-based providers or services, their communications are often routed through the United States regardless of their country of origin or their ultimate destination. NSA SIGINT activities in the United States seek to exploit this "home field" advantage to discover and intercept our adversaries' communications in order to provide the timely, insightful, and precise intelligence needed to take decisive action against these external threats to our security.

26. (~~S//NF~~) [redacted]

[redacted]

C. (U) Collection of Communications Content Pursuant to FISA Section 702

27. **(U)** In July 2008, Congress enacted the Foreign Intelligence Surveillance Act Amendments Act of 2008 (the "FAA"), Pub. L. 110-261, 122 Stat. 2436. The FAA added a new section 702 to FISA, 50 U.S.C. § 1881a ("Section 702"), which created new statutory authority permitting the targeting of non-United States persons reasonably believed to be outside of the United States to acquire foreign intelligence information without individualized orders or warrants from the FISC. More specifically, Section 702 generally provides that, upon the FISC's

approval of a "certification" submitted by the Government, the Attorney General and the DNI may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a), (h).[5] Although the statute does not require the government to identify the specific facilities, places, premises, or property at which an authorized acquisition will be directed, the government must certify that an acquisition involves obtaining foreign intelligence information "from or with the assistance of an electronic communication service provider." *Id.* § 1881a(h)(2)(A)(vi).

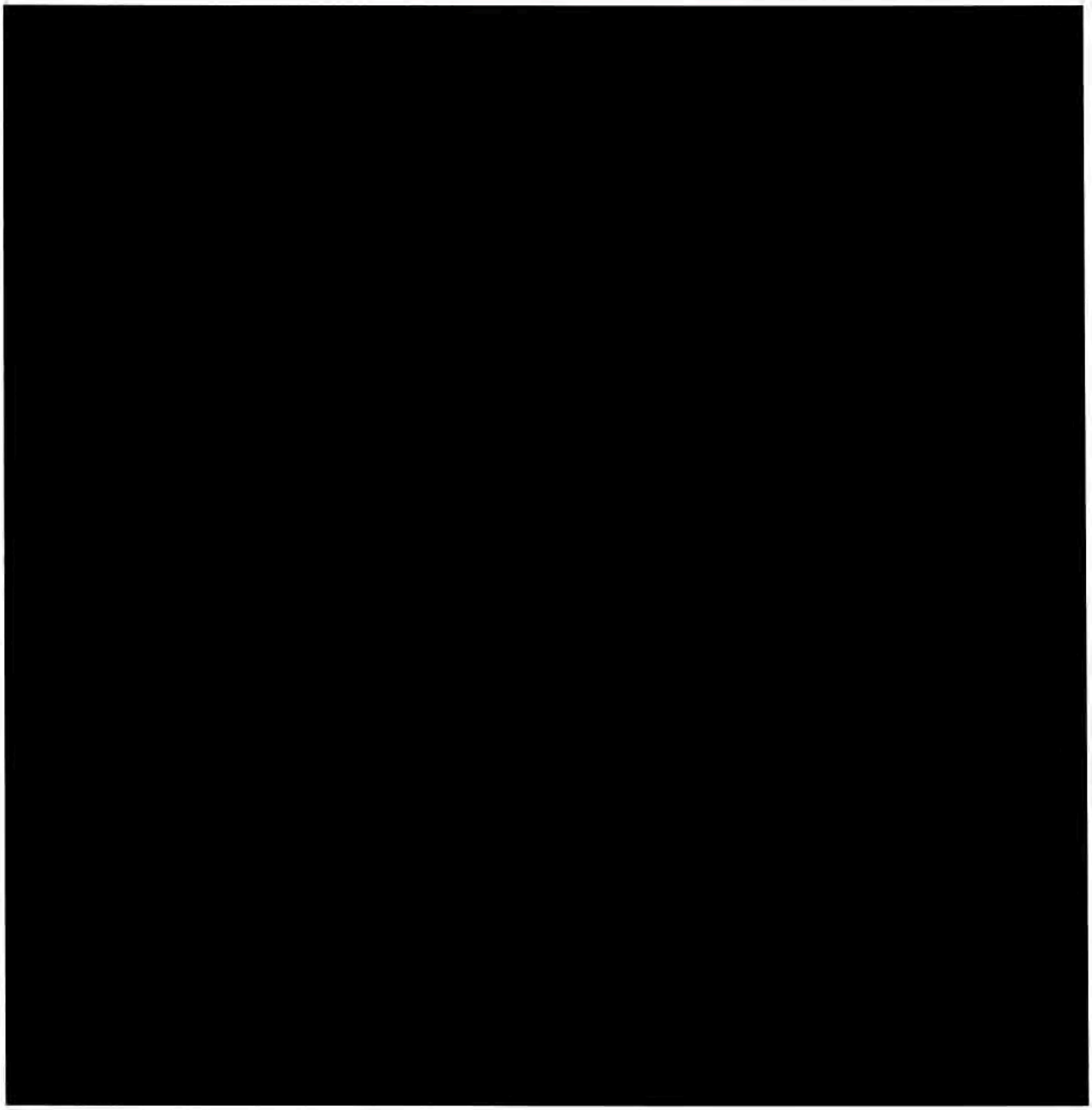
28. **(U)** Accordingly, under Section 702, the Attorney General and the DNI submit annual certifications to the FISC for its approval, as required under the statute, to authorize the targeting of non-U.S. persons reasonably believed to be located outside of the United States to acquire foreign intelligence information. These certifications identify categories of foreign intelligence information authorized for acquisition, but do not identify the particular non-U.S. persons who will be targeted. Instead, the certifications include targeting procedures, approved

[5] **(U)** Section 702 has always imposed four requirements that must be met for FISC approval of a Section 702 certification. First, the Attorney General and the DNI must certify, *inter alia*, that a significant purpose of the acquisitions is to obtain foreign-intelligence information, as that term is defined under FISA, and the FISC must find that the Attorney General and DNI's certification contains all of the required statutory elements. 50 U.S.C. § 1881a(h)(2)(A)(iv), (j)(2)(A). Second, the FISC must find that the Government's targeting procedures are reasonably designed to ensure that acquisitions conducted under the authorization are limited to targeting non-U.S. persons reasonably believed to be located outside the United States, and will not intentionally acquire communications known at the time of acquisition to be purely domestic. *Id.* § 1881a(j)(2)(B). Third, the FISC must find that the Government's minimization procedures meet FISA's requirements. *Id.* §§ 1801(h), 1821(4), 1881a(j)(2)(C). And fourth, the FISC must find that the Government's targeting and minimization procedures are consistent, not only with FISA, but also with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A). Following passage of the FISA Amendments Reauthorization Act of 2017 earlier this year, the FISC must now also find that the Government's querying procedures meet the statutory requirements and are consistent with the Fourth Amendment. *Id.* § 1881a(j)(2)(D); (j)(3)(A).

by the Attorney General, which must, among other things, be reasonably designed to ensure that any Section 702 acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of wholly domestic communications. In addition, the targeting procedures specify the manner in which the Intelligence Community determines whether a person is a non-U.S. person reasonably believed to be located outside the United States who is likely to possess, receive, or communicate foreign intelligence information authorized for acquisition by a certification.

29. ~~(S//NF)~~ [redacted]

30. ~~(TS//SI//NF)~~ [redacted]



[6] **(U)** Generally speaking, the Internet "backbone" refers to the interconnected networks of providers' long-haul terrestrial, fiber-optic cables that carry large volumes of Internet communications over long distances, usually between large metropolitan areas, and interchange communications traffic around the world. The Internet backbone also includes the high-capacity submarine telecommunications cables that carry Internet communications between different parts of the globe.

31. (~~S//NF~~) [redacted]

[redacted]

D. (U) Upstream Collection

32. (~~S//NF~~) [redacted]

[redacted]

33. **(U)** Over the past several years, the Government has declassified and publicly released thousands of pages of materials pertaining to Section 702 collection activities, including

Upstream surveillance, such as redacted memorandum opinions and orders issued by the FISC and certain of NSA's Section 702 targeting and minimization procedures. In addition, two Government reports have been issued that address Section 702 activities, including Upstream surveillance. In April 2014, the NSA's Civil Liberties and Privacy Office released a report on the NSA's implementation of FISA Section 702, which included a high-level unclassified description of Upstream. A short time later, in July 2014, the Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent Executive Branch agency established pursuant to statute, 42 U.S.C. section 2000ee, issued its report on the Government's implementation of Section 702, which also included an unclassified description of the Upstream program. *See* PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("PCLOB Section 702 Report").

34. **(U)** While these declassified documents and unclassified reports describe the Upstream acquisition process in general terms, they are necessarily incomplete because certain operational details of Upstream acquisition remain highly classified.

35. **(~~TS//SI//NF~~)** [redacted]

[7] **(~~TS//SI//NF~~)** [redacted]

[redacted]

36. (~~TS//SI//NF~~) [redacted]

[redacted]

---

[8] (~~TS//SI//NF~~) [redacted]

[9] (~~TS//SI//NF~~) [redacted]

[redacted]

37. (~~TS//SI//NF~~) [redacted]

[redacted]

38. (~~TS//SI//NF~~) [redacted]

[redacted]

[10] **(U)** IP addresses identify devices on the Internet or other computer networks, and are used to route packets between destinations on a computer network. Public IP addresses are allocated to organizations (*e.g.*, companies, governments, universities, etc.), who register the basic ownership details (to include country) with a regional registry. The organizations that are allocated IP addresses may have network devices outside of the country listed in regional registry entry, thereby enabling IP addresses to be associated with network devices outside of the registered country. IP filtering refers to blocking or selecting communications to or from particular groups of IP addresses (which may include single IP addresses).

[redacted]

39. (~~TS//SI//NF~~) [redacted]

[redacted]

40. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

41. **(U)** It is against this backdrop that the risks of disclosing the information that Wikimedia seeks to compel the Government to reveal should be assessed.

E. (U) The Wikimedia Discovery Requests

42. **(U)** As discussed above, Wikimedia, seeking evidence with which to establish its legal standing to bring a legal challenge to Upstream surveillance, served 84 separate discovery requests on the Government. I am advised that Wikimedia has moved to compel further responses by the Government to 53 of those requests, and that it divides them into three categories.

43. **(U)** The first category Wikimedia describes as "direct evidence" that it "has been surveilled" in the course of Upstream surveillance, i.e., that at least some of its communications have been copied, scanned, retained, or otherwise "interacted with" by the NSA. The Government has refused to confirm or deny, however, whether the NSA has copied, scanned, retained, or otherwise "interacted with" Wikimedia communications in the course of Upstream surveillance (see Wikimedia Requests for Admission ("RFA") Nos. 34-36); has refused to confirm or deny the authenticity of purported Power Point slides that, according to Wikimedia, express NSA interest in surveilling its communications (RFA Nos. 16-21); and has refused to confirm or deny whether the NSA possesses any communications of Wikimedia's acquired in the course of Upstream surveillance, or any other documents concerning interactions with Wikimedia communications during the Upstream collection process (Wikimedia Requests for Production ("RFP") Nos. 23-24). Disclosure of this information reasonably can be expected to cause exceptionally grave damage to the national security of the United States.

44. **(U)** The second category of information that Wikimedia seeks in its motion to compel is described therein as "[k]ey terms used in describing Upstream surveillance to the public." This category includes information responsive to interrogatories asking the Government to describe its understanding of the "definitions" of a list of terms and phrases used in unclassified public documents to discuss various aspects of Upstream surveillance. *See* Wikimedia Interrogatory Nos. 1-9. In response the Government set forth its understanding of most of these terms and phrases, so far as it could do so without revealing classified information regarding the sources and methods and technical operational details of Upstream surveillance.

45. **(U)** The Government was unable to provide any unclassified response, however, to Wikimedia's Interrogatory Nos. 1 and 7. Interrogatory No. 1 sought the Government's understanding of the term "international Internet link," as used by the FISC in an October 3, 2011, memorandum opinion concerning Upstream surveillance. "International Internet link" is not a term commonly used in the telecommunications industry. The Government has its own understanding of what the FISC meant when the FISC used that term, but, because that understanding is based on still-classified portions of the FISC's October 3, 2011, opinion, the Government cannot explain its understanding of what the FISC meant by the term "international Internet link" without revealing classified information.

46. **(U)** Interrogatory No. 7 asks the Government to state its understanding of the common features of Internet packets that comprise an "Internet transaction." "Internet transaction" is also not a term commonly used in the telecommunications industry, but a term defined in the NSA's Section 702 Minimization Procedures to help explain that the NSA's Upstream collection devices do not necessarily acquire just single communications but packets of communications data that may form either a single, discrete communication, or multiple

communications. The Government, however, was unable to state the common features of the packets of data constituting an Internet transaction, as Wikimedia requested, without revealing, or tending to reveal, classified information about the design and operation of the NSA's Upstream surveillance equipment.

47. **(U)** Wikimedia also includes in its second category of discovery RFP Nos. 21 and 22, which ask the Government to produce all FISC, Foreign Intelligence Surveillance Court of Review, and Supreme Court opinions and orders concerning Upstream surveillance, and all submissions to these courts concerning Upstream surveillance,[11] since the enactment of Section 702 in July 2008, regardless of whether they include any of the information otherwise sought by the requests in this category. The Government objected to producing these documents on the grounds that, among other reasons, their disclosure could reasonably be expected to cause exceptionally grave damage to the national security of the United States. In addition, I am told that the volume of documents called for by RFP Nos. 21 and 22 exceeds 10,000 pages, and thus the Government also objected to the burden of producing unclassified versions of such a large body of classified materials.

48. **(U)** The third and largest category of discovery requests to which Wikimedia seeks to compel responses is labeled in Wikimedia's motion to compel as "Evidence concerning the scope and breadth of Upstream surveillance." The requests in this wide-ranging category ask the Government (i) to state the percentage of international Internet circuits and submarine cables that were "monitored" in the course of Upstream surveillance during each of the years 2015-2017 (Interrogatory Nos. 16-17); (ii) to admit whether the NSA conducts Upstream surveillance

[11] **(U)** The Government has not made submissions to the FISC-R or the Supreme Court specifically concerning Upstream collection and nor has either Court issued an opinion or order specifically concerning Upstream collection.

on multiple Internet backbone circuits, chokepoints, and international Internet links (RFA Nos. 13-15); (iii) to admit the authenticity of documents that, according to Wikimedia, indicate locations on the Internet backbone where the NSA conducts Upstream surveillance (RFA Nos. 25-30, 39); (iv) to state the amount of Internet communications traffic that was "filtered" and "scanned" in the course of Upstream surveillance during each of the years 2015-2017 (Interrogatory Nos. 18-19); (v) to admit whether the contents of Internet web traffic (HTTP and HTTPS communications) are now and previously were scanned in the course of Upstream surveillance (RFA Nos. 37-38); (vi) to admit whether the NSA, in conducting Upstream surveillance, copies, and reviews in bulk the contents of Internet communications that are in transit and neither to nor from Upstream surveillance targets (RFA Nos. 6-10); (vii) to describe the entire process by which the contents of Internet communications are in any way "interacted with" during the Upstream process, including any inaccuracies in the description provided in the PCLOB Section 702 Report (Interrogatory Nos. 14-15); and (viii) to identify the protocols used to encrypt Internet communications that the NSA is capable of decrypting (Interrogatory No. 20; RFA No. 40).

49. **(U)** Wikimedia also includes in this third category eight separate requests for the production of documents, seeking (i) documents sufficient to show the total number of circuits on which Upstream surveillance was conducted, the total bandwidth of those circuits, and the total number of Internet transactions acquired, during each of the years 2010-2017 (RFP Nos. 10, 13, 14); (ii) documents sufficient to show the number of "international Internet links" that were "monitored" in the course of Upstream surveillance during each of the years 2015-2017 (RFP No. 15); (iii) documents sufficient to show the number of international Internet "chokepoints" at which the NSA has allegedly conducted Upstream surveillance at any time since Section 702

was enacted in July 2008 (RFA No. 16); and (iv) the targeting procedures applied for purposes of implementing Upstream surveillance in the years 2009, 2015, and 2017 (RFP No. 18). In addition, Wikimedia includes in this "scope and breadth" category RFP Nos. 21 and 22, which call for the production of more than 10,000 pages of classified orders and opinions issued by and submissions made to the FISC, regardless of whether they contain any of the information otherwise sought in category three.

50. **(U)** The Government was able to provide partial, unclassified responses to Wikimedia's RFA Nos. 6, 8, and 10 (concerning the review of communications during the Upstream collection process), and partial responses to several of the document requests in this category. But because of the highly classified and extraordinarily sensitive nature of the documents and information sought in Wikimedia's third category of discovery requests, it was otherwise necessary for the Government to object to producing the documents and information sought in this category in order to protect classified information whose disclosure could reasonably be expected to cause exceptionally grave damage to national security.

51. **(U)** In addition to the foregoing three categories of discovery requests, Wikimedia also seeks to compel further testimony from an NSA official who was deposed on April 16, 2018, who had been designated to testify on behalf of the NSA on the following topics: (i) the definitions and meaning, as understood by the NSA, of terms that have been used in official public disclosures to describe Upstream surveillance; (ii) the ways in which the NSA (or telecommunications service providers acting on the NSA's behalf) access or interact with Internet communications in the course of Upstream surveillance; (iii) the number and type of Internet communications or transactions intercepted, accessed, copied, filtered, reviewed, screened, scanned, ingested, and/or retained by the NSA in the course of Upstream surveillance;

(iv) the number of circuits, international Internet links, and Internet backbone checkpoints on or at which the NSA conducts and has conducted Upstream surveillance; and (v) the facts related to Upstream surveillance that the NSA has disclosed, or authorized disclosure of, to the FISC, the Foreign Intelligence Surveillance Court of Review, the Supreme Court, and/or the PCLOB, and that it has subsequently declassified.

52. **(U)** The designated deponent, Rebecca J. Richards, has served as the Director of Civil Liberties and Privacy at NSA since February 2014. As NSA's Chief Transparency Officer, Ms. Richards works to communicate with the public about the value of signals intelligence and the tools NSA needs to conduct its mission, while maintaining protection over NSA's vital sources and methods. These duties and responsibilities require that she maintain a high level of familiarity with the operational details of a wide range of NSA intelligence activities, including Upstream surveillance. I have been advised that Ms. Richards was questioned for approximately seven hours on the record on topics concerning Upstream surveillance that were largely coextensive with the subjects covered by Wikimedia's written discovery requests. I understand that because the questions posed by Wikimedia's counsel consistently called for classified details about the sources, methods and operational details of Upstream surveillance, it was necessary throughout the deposition for the Government to object to Wikimedia's questions, and to withhold information, in whole or in part, in response thereto, in order to protect classified information whose disclosure could reasonably be expected to cause exceptionally grave damage to the national security of the United States.

V. (U) INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE

53. **(U)** As discussed above, the Government has officially declassified and publicly disclosed certain information about the existence and nature of NSA Upstream surveillance.

However, the additional information that Wikimedia seeks to compel the Government to disclose in response to its discovery requests and certain deposition questions remains properly classified, and is subject to the DNI's assertions of the state secrets privilege, to the DNI's assertion of the statutory privilege under 50 U.S.C. § 3024(i)(1), and to my own assertion herein of the NSA's statutory privilege under 50 U.S.C. § 3605(a). Although, as discussed above, I have been advised that Wikimedia divides the classified information it seeks into the three categories discussed above, for purposes of understanding the exceptionally grave risks to national security that would flow from disclosing this information, the information sought is best understood as falling into the seven separate categories identified below. For the Court's ease of reference, I note below each of Wikimedia's written discovery requests that calls for, or implicates, classified information in each category. I have been informed that the classified information that Wikimedia sought to elicit during Ms. Richards's deposition falls into all seven categories. The information encompassed by these categories would remain classified, and privileged, regardless of whether it is sought in response to pending or future discovery requests served by Wikimedia, or may become necessary for any other purposes associated with the litigation of Wikimedia's claims or the Government's defenses in this case.

54. **(U)** Accordingly, in general and unclassified terms, the DNI's assertion of the state secrets privilege, of the statutory privilege under 50 U.S.C. § 3024(i)(1), and my assertion of the NSA's statutory privilege under 50 U.S.C. § 3605(a), encompass the following categories of still-classified information and properly protected national security information concerning NSA Upstream surveillance:

A. **(U) Entities subject to Upstream surveillance activities:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that indicate or may tend to indicate whether communications of Wikimedia, and/or of other individuals and entities, have been subject to Upstream surveillance activities [RFA Nos. 16-21, 34-36; RFP Nos. 21-24];

B. **(U) Operational details of the Upstream collection process:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified technical details concerning the methods, processes, and devices employed (including the design, operation, and capabilities of the devices employed) to conduct Upstream surveillance [Interrogatory Nos. 3-5, 14, 15; RFA Nos. 6-10, 37, 38; RFP Nos. 21, 22];

C. **(U) Locations at which Upstream surveillance is conducted:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about any specific location(s), or the nature of the location(s), on the Internet backbone network(s) of U.S. electronic communication service provider(s) at which Upstream surveillance is conducted [Interrogatory Nos. 1, 2; RFA Nos. 13-15, 25-30, 39; RFP Nos. 13, 15, 16, 18, 21, 22];

D. **(U) Categories of Internet-based communications subject to Upstream surveillance activities:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about the specific types or categories of communications either subject to or acquired in the course of the Upstream collection process [Interrogatory Nos. 6-8; RFA Nos. 16-18; RFP No. 22];

E. **(U) The scope and scale on which Upstream surveillance is or has been conducted:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about (i) the volume or proportion of Internet communications traffic, including international Internet communications, either subject to or acquired in the course of the Upstream collection process, (ii) the number, proportion, and/or bandwidth of any circuit, international submarine or terrestrial cable, or other Internet backbone link, on which Upstream surveillance

is or has been conducted; and (iii) any other measure of the scope or scale on which Upstream surveillance is or has been conducted [Interrogatory Nos. 9, 16-19; RFP Nos. 10, 14];

F. **(U) NSA's cryptanalytic capabilities:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about the NSA's capability, or lack thereof, to decrypt, circumvent, or defeat specific types of communications security protocols [Interrogatory No. 20; RFA No. 40]; and

G. **(U) Additional categories of classified information contained in opinions and orders issued by, and in submissions made to, the FISC:** The additional categories of classified information contained in the documents responsive to Wikimedia RFP Nos. 21 and 22, not already encompassed by categories A-F, above, as set forth in the privilege log served by Defendant U.S. Department of Justice on March 19, 2018 [RFP Nos. 21, 22]

VI. (U) HARM OF DISCLOSURE OF PRIVILEGED INFORMATION

A. (U) Information Concerning Whether Communications of Wikimedia or of Other Entities or Individuals Have Been Subjected to Upstream Surveillance Activities [RFA Nos. 16-21, 34-36; RFP Nos. 21-24]

55. **(U)** The first category of information as to which I am supporting the DNI's assertions of privilege, and asserting the NSA's statutory privilege, concerns documents and information that would reveal or tend to reveal whether communications of Wikimedia or of other entities or individuals have been subject to any stage of the Upstream collection process.

56. **(U)** As discussed above, Wikimedia seeks to compel the Government to admit or deny whether the NSA has copied, reviewed the content of, and/or retained at least one Wikimedia communication in the course of Upstream surveillance; to produce any Wikimedia communications the NSA has copied, reviewed, or otherwise interacted with; and to produce any documents concerning such NSA "interaction" with Wikimedia communications. See RFA Nos. 34-36, RFP Nos. 23-24. In addition, Wikimedia seeks to compel the Government to confirm or deny the authenticity of purportedly classified documents indicating, according to Wikimedia,

that the NSA targets its communications for Upstream surveillance. RFA Nos. 16-21. These matters were also the subjects of questions propounded by Wikimedia to the NSA's designated deposition witness, who was instructed for reasons of privilege that she should not answer. Documents responsive to Wikimedia RFP Nos. 21 and 22, regarding court orders, opinions, and submissions concerning Upstream surveillance, also include information about the nature or specific identities of individual Upstream surveillance targets, and of entities about which the NSA seeks to acquire intelligence information. See, e.g., Department of Justice Privilege Log dated March 19, 2018 ("DOJ Privilege Log") at Nos. 18, 23, 29, 31. For the reasons set forth below, disclosure of such information by the NSA reasonably could be expected to cause exceptionally grave damage to national security, because it would reveal information as to whether particular entities have been subject to surveillance, as well as the nature, scope, and extent of NSA Upstream surveillance activities.

57. **(U)** As a matter of course, the NSA cannot publicly confirm or deny whether particular individuals or entities are or have been subject to intelligence-gathering activities, because to do so would tend to reveal actual targets or subjects. The harm of revealing the identities of persons or organizations who are the actual targets or subjects of foreign-intelligence gathering is relatively straightforward. If individuals or organizations knew or suspected they are targets of subjects of U.S. intelligence activities, they would naturally tend to alter their behavior to take new precautions against such scrutiny. In addition, revealing which individuals or entities are not targets or subjects of intelligence gathering would indicate who has avoided surveillance or collection, and which channels of communication may be secure. Such information could allow actual or potential adversaries, secure in the knowledge that they are not under government scrutiny, to convey information necessary or useful to the execution of hostile

acts against the United States and its interests. Alternatively, such individuals or entities may be unwittingly utilized or even forced by foreign adversaries to convey information through secure channels. Revealing which channels are free from surveillance and which are not could also reveal sensitive intelligence methods, and thereby help an adversary evade detection and capitalize on limitations in the NSA's surveillance capabilities.

58. **(U)** Similar harms would result from confirming or denying whether the communications of particular persons or entities have been subject to collection, even where it may be assumed that they are law-abiding and not likely to be actual targets or subjects of such activity. This is so because, if the NSA were to confirm that specific individuals or entities have not been targets of or subject to collection (*i.e.*, that their communications have not been intercepted), but later refuse to comment (as it would have to) in situations involving actual targets or subjects, actual or potential adversaries of the United States could then easily deduce that the persons in the latter instances are or have been targets of or subject to surveillance. In addition, disclosing whether communications of particular persons or organizations have or have not been targeted, or intercepted through the targeting of third parties, would reveal whether particular channels of communication are secure, and also reveal to third-party targets whether their own communications may be secure. Moreover, each occasion where the Government confirms (even if compelled to confirm) that certain persons or organizations have or have not been subjects of surveillance makes it more difficult in the future to withhold information about the surveillance status of other individuals or entities. This could result in a cascading effect of disclosures.

59. **(U)** To appreciate the national security risks associated with disclosing whether the NSA, through Upstream surveillance, has copied, reviewed, retained, or otherwise interacted

with Wikimedia's communications, it is necessary to understand that Wikimedia has placed three types of its communications at issue in this case: (i) online communications between Wikimedia websites and individuals who read, contribute to, or edit the contents of those websites, using the HTTPS and HTTP protocols; (ii) Wikimedia's internal "logs" of such communications with its websites, whose logs are transmitted from its servers in Amsterdam to its servers in the United States; and (iii) electronic communications of Wikimedia's U.S. staff with Wikimedia staff, contractors, and volunteers located in other countries. Disclosing (be it through admission, or the production of documents) whether Wikimedia communications have been subject to copying, reviewing, or any other alleged form of "interaction" in the Upstream collection process, would entail confirmation of whether Wikimedia's HTTPS/HTTP communications, its "log" communications, and/or its staff communications have been subjected to Upstream surveillance.

60. (~~TS//SI//NF~~) [redacted]

[redacted]

61. (~~TS//SI//NF~~) [redacted]

[redacted]

62. **(U)** Revealing whether the NSA, in the course of Upstream surveillance, has collected or otherwise interacted with the online communications of Wikimedia's U.S. staff, or the personnel of any organization that communicates routinely over the Internet, could reveal to targeted individuals or entities in communication with that organization that they may be subject to NSA surveillance. That is especially the case were the Government actually to produce any communications with the subject organization that it has acquired, as has been demanded here. The presence or absence, among the disclosed communications, of exchanges with targets that

had been in contact with the subject organization could alert them to surveillance of which they had been unaware, or provide assurance that their communications are secure. In either event, national security could be imperiled. The presence or absence of communications to or from particular countries could also alert other potential targets within those countries to whether NSA seeks to collect communications to or from that country.

63. **(U)** In search of "direct evidence" that its communications have been subject to Upstream surveillance, Wikimedia also demands that the Government confirm or deny whether two purportedly classified Power Point slides (reproduced on page four of its motion to compel) are in fact genuine NSA documents indicating that the NSA targets Wikimedia communications (and HTTP communications generally) for Upstream surveillance. For the reasons just discussed, including the dangers of alerting our adversaries to the types of communications on which the NSA does or does not focus its surveillance efforts, the Government cannot confirm or deny the authenticity of the so-called "NSA slides" without damaging national security.

64. **(U)** Specifically, RFA Nos. 16-18 refer to a slide, entitled: "Why are we interested in HTTP?" while RFA Nos. 19-21 relate to a slide, entitled: "Fingerprints and Appids." Wikimedia requests the Government to admit that both documents are "genuine" NSA documents containing statements by NSA "employees on matters within the scope of their employment during the course of their employment," and that these NSA employees were "authorized to make statements on the subjects of the statements within the document."

65. **(~~TS//SI//NF~~)** [redacted]

[redacted]

66. (~~TS//SI//NF~~) [redacted]

[redacted]

67. (~~TS//SI//NF~~) [redacted]

68. (~~TS//SI//NF~~) [redacted]

[redacted]

69. (~~TS//SI//NF~~) [redacted]

70. **(U)** Finally, as reflected in the DOJ Privilege Log, a substantial number of the classified orders, opinions, and court submissions concerning Upstream surveillance that are responsive to Wikimedia's RFP Nos. 21 and 22 contain information about the nature or specific identities of individual Upstream surveillance targets, and of entities about which the NSA seeks to acquire intelligence information under Section 702. For the reasons discussed herein, the Government cannot disclose such information about the nature and identities of the NSA's actual surveillance targets without risking exceptionally grave damage to national security.

71. **(U)** For all of the above-noted reasons, disclosing information tending to confirm or deny whether communications of Wikimedia, or of other entities or individuals, have been subject to any stage of the Upstream collection process could reasonably be expected to cause exceptionally grave damage to the national security of the United States.

B. (U) Operational Details of the Upstream Collection Process [Interrogatory Nos. 3-5, 14-15; RFA Nos. 6-10, 37, 38; RFP Nos. 21, 22]

72. (~~S//NF~~) [redacted]

[redacted]

73. **(U)** As discussed above, the Government has officially acknowledged the existence of Upstream surveillance and has publicly released a limited amount of information describing, at a high level of generality, how Upstream collection operates. The Government has produced this now-unclassified information about Upstream's operation in response to Wikimedia's discovery requests. Wikimedia now seeks additional technical details about the Upstream collection process, information that remains classified in the interests of national security.

74. **(U)** Specifically, Wikimedia's Interrogatory Nos. 3-5 ask the Government to describe its understanding of the terms "filtering mechanism," "scanned," and "screened" as used to describe aspects of the Upstream collection process in previous Government filings in this case. The Government did so in its responses to the extent possible without revealing classified operational details about the Upstream collection process. Similarly, Wikimedia's RFA Nos. 6, 8, and 10 ask the Government to admit or deny that the NSA "reviews the contents of Internet communications" in various ways during Upstream surveillance. The Government also responded to these requests to the extent possible without revealing classified information. Wikimedia now insists, however, on disclosures of additional technical details about the "filtering mechanism[s]" employed and the "scann[ing]," "screen[ing]" and content review of communications during Upstream surveillance.

75. **(U)** The Government could provide no response to Wikimedia's Interrogatory Nos. 14-15 and RFA Nos. 7, 9, and 37-38, because any response would have required the disclosure of classified operational details about Upstream surveillance. Interrogatory No. 14 asks the Government to describe the entirety of the process by which communications are allegedly copied, filtered, scanned, or otherwise "interacted with" during Upstream collection. Interrogatory No. 15 asks the Government to identify any inaccuracies in the PCLOB's unclassified description of the Upstream collection process, which also would have necessarily required the Government to provide highly technical and classified information about any changes in the sources and methods or operational details of Upstream surveillance since the PCLOB issued its report in July 2014.

76. ~~(TS//SI//NF)~~ [redacted]



[redacted]

77. (~~TS//SI//NF~~) [redacted]

[redacted]

78. (~~S//NF~~) [redacted]

[redacted]

[12] **(U)** As described at greater length in previous filings, *e.g.*, Mem. in Supp. of Defs.' Mot. to Compel, ECF No. 126-1, to send a communication via the Internet, the transmitting device first converts the communication into one or more "packets," relatively small bundles of



79. **(U)** Thus, Wikimedia seeks to compel disclosures concerning classified operational details about the entirety of the Upstream collection process that would reveal to foreign adversaries the NSA's operational methods and capabilities (or lack thereof), enabling them to evade particular types of surveillance and to exploit the NSA's sources and methods of surveillance for their own purposes, in both cases risking exceptionally grave damage to national security.

80. **(~~S//NF~~)**

---

digital information. This process is governed by the use of standardized protocols, including, for web pages, the HTTP and HTTPS protocols. Each "packet" is configured with so-called "layers" containing different types of information, some of which provide the address and routing information necessary to send the packet from its origin to its destination over the Internet. The "application layer," by contrast, generally contains a portion of the content of the original communication.

[redacted]

81. (~~TS//SI//NF~~) [redacted]

[redacted]

82. (~~TS//SI//NF~~) [redacted]

[redacted]

83. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

84. (~~S//NF~~) [redacted]

[redacted]

85. (~~S//NF~~) [redacted]

[redacted]

C. (U) Location(s) on the Internet Backbone Where Upstream Surveillance Is Conducted
[Interrogatory Nos. 1, 2; RFA Nos. 13-15, 25-30, 39; RFP Nos. 13, 15, 16, 18, 21, 22]

86. **(U)** I am also supporting the DNI's assertions of privilege and asserting the NSA's statutory privilege over documents and information that would tend to reveal the nature and number of the location(s) on the Internet backbone where Upstream surveillance is conducted.

87. **(U)** As discussed above, the Government has publicly acknowledged that, as part of Upstream surveillance, the NSA collects communications from one or more circuits at one or more points on the Internet backbone. However, to protect sensitive sources and methods of Upstream surveillance, and the identities of assisting electronic communication service providers, the Government has not acknowledged any further details about the number, nature, or specific locations of the sites where Upstream surveillance is conducted.

88. **(~~TS//SI//NF~~)** [redacted]

[redacted]

89. **(U)** Wikimedia Interrogatory No. 2 asks for the Government's understanding of the definition of the term "circuit," as used by the PCLOB in its Section 702 Report. In response to Interrogatory No. 2, the Government has provided an accepted definition of "circuit" as that term is used by the telecommunications industry. The NSA's designated witness also testified that the NSA has no specialized understanding of the term "circuit" that it applies in the context of Upstream surveillance, other than its accepted meaning in the telecommunications industry. In responding, however, to this request for a definition of the term "circuit," the Government has objected to providing classified information about the specific type(s) and/or location(s) of the circuit(s) on which Upstream surveillance is now or in the past has been conducted.

90. **(U)** Wikimedia RFA Nos. 13-15 ask the Government to admit that the NSA conducts Upstream surveillance on "multiple Internet backbone circuits," "multiple international Internet links," and "multiple Internet backbone chokepoints." RFP Nos. 13, 15, and 16 seek documents sufficient to show or estimate the "number of circuits," "number of international Internet links" and the "number of Internet chokepoints" at which Upstream surveillance is conducted.

91. **(~~TS//SI//NF~~)** [redacted]

[redacted]

92. **(U)** Additionally, Wikimedia's request for tens of thousands of pages of classified court orders, opinions, and submissions concerning Upstream surveillance (RFP Nos. 21 and 22) include documents identifying certain telecommunications service providers that at one time or another have been compelled to assist the NSA in Upstream collection activities.

93. **(U)** For the reasons that follow, public release of the documents and information sought by the foregoing could reasonably be expected to cause exceptionally grave damage to national security.

94. **(~~TS//SI//OC/NF~~)** [redacted]

[redacted]

95. (~~TS//SI//OC/NF~~) [redacted]

96. (~~TS//SI//OC/NF~~) [redacted]

[redacted]

97. ~~(TS//SI//OC/NF)~~ [redacted]

[redacted]

98. ~~(TS//SI//OC/NF)~~ [redacted]

[redacted]

[redacted]

99. (~~TS//SI//OC/NF~~) [redacted]

[redacted]

100. (~~TS//SI//NF~~) [redacted]

D. (U) Categories of Internet-Based Communications Subject to Upstream Surveillance Activities
[Interrogatory Nos. 6-8; RFA Nos. 16-18; RFP No. 22]

101. **(U)** I am likewise supporting the DNI's assertions of privilege, and asserting the NSA's statutory privilege, over still-classified documents and information that would reveal or tend to reveal the types of Internet communications that are subject to any stage of the Upstream collection process, and those that are not.

102. **(U)** In this regard, Wikimedia seeks to compel the Government to describe at greater, and classified, length its understanding of the terms "discrete communication," "single communication transaction" and "multi-communication transaction," and of the common features of Internet packets comprising an "Internet transaction." Interrogatory Nos. 6-8. Wikimedia's request that the Government confirm or deny the authenticity of the so-called "NSA slide" headed "Why Are We Interested in HTTP?" also implicates information in this category, as do a significant number of the court submissions concerning Upstream surveillance that are responsive to RFP No. 22. In deposition, Wikimedia also propounded questions to the NSA's designated witness (which she was instructed for reasons of privilege not to answer) concerning the categories of Internet-based communications that are subject to Upstream collection activities, including whether the devices used are configured to exclude various types of encrypted communications.

103. **(~~TS//SI//NF~~)** [redacted]

[redacted]

104. (~~TS//SI//NF~~) [redacted]

105. **(U)** So far as Wikimedia's discovery requests in this category are concerned, the first, Interrogatory No. 6, seeks the NSA's understanding of the "definition" of the term "discrete communication" as used in the NSA's 2014 Section 702 Minimization Procedures. Given the innumerable, ever-increasing, and ever-changing means by which to convey information electronically, there is no single, commonly accepted technical definition of a "communication" in the telecommunications industry, and the NSA has not developed a particularized definition of

the term that it uses in connection with Upstream surveillance, or otherwise. Therefore, in responding to Interrogatory No. 6 that the term "discrete communication" means a single communication, the Government has already given the most complete answer to this interrogatory that it is reasonably capable of providing. (To respond in any further detail would require the NSA to reveal the types of communications it collects via Upstream, which inevitably would induce our foreign adversaries to avoid those forms of online communications in order to defeat the NSA's attempts to capture their communications.) So far as Interrogatory No. 8 is concerned, the Government has already responded, straightforwardly that a "single communication transaction" is an Internet transaction containing only a single, discrete communication, and that a "multi-communication transaction" is an Internet transaction that contains multiple discrete communications. (Again, any further response would require the NSA to disclose examples of the kinds of communications it collects today via Upstream—that information is currently and properly classified.) The root of Wikimedia's dissatisfaction with the Government's responses to Interrogatory Nos. 6-8 apparently lies, therefore, with the Government's refusal to provide its understanding, in response to Interrogatory No. 7, of the common features of the Internet "packets" that constitute a single Internet transaction (or communication) for purposes of Upstream surveillance.

106. (~~TS//SI//NF~~) [redacted]

[redacted]

107. (~~S//NF~~) [redacted]

[redacted]

108. **(U)** Accordingly, the Government cannot disclose classified information falling within this category, whether in response to Wikimedia's pending discovery requests or otherwise, without risking exceptionally grave damage to the national security of the United States.

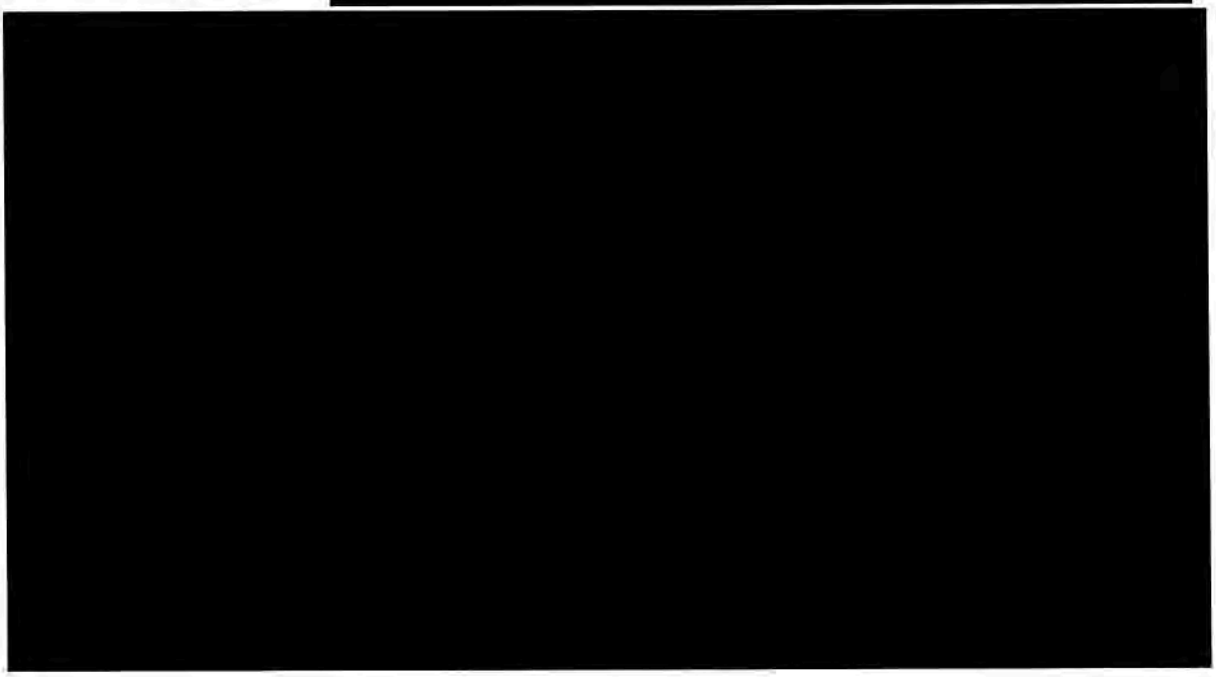
E. (U) Scope and Scale of Upstream Surveillance [Interrogatory Nos. 9, 16-19; RFP Nos. 10, 14]

109. **(U)** I am also supporting the DNI's assertions of privilege and asserting the NSA's statutory privilege over still-classified facts concerning the scope and scale of Upstream

surveillance, the disclosure of which would likely motivate foreign adversaries and others to intensify their efforts to avoid such surveillance.

110. **(U)** As discussed above, Wikimedia seeks to compel the Government to reveal the scope of its Upstream surveillance by describing (i) the "body of international communications" that is subject to the surveillance (Interrogatory No. 9); (ii) the approximate percentage of circuits and international submarine cables carrying international Internet traffic into and out of the United States that the NSA is monitoring (Interrogatory Nos. 16-17); and (iii) the approximate amount of Internet traffic subject to each stage of the Upstream process (Interrogatory Nos. 18-19). Wikimedia also seeks the disclosure of documents showing the total bandwidth of the circuits on which Upstream surveillance was conducted, and number of Internet transactions acquired by the NSA, during each of the years 2010-2017 (RFP Nos. 10, 14). These matters were also the subjects of questions propounded by Wikimedia to the NSA's designated deposition witness, which on the basis of privilege the Agency declined to answer.

111. **(~~TS//SI//NF~~)** [redacted]



[redacted]

112. (~~TS//SI//OC//NF~~) [redacted]

113. (~~TS//SI//NF~~) [redacted]

114. (~~TS//SI//NF~~) [redacted]

[redacted]

115. (~~TS//SI//NF~~) [redacted]

[redacted]

116. (~~TS//SI//NF~~) [redacted]

[redacted]

F. (~~S//NF~~) NSA's Capabilities, or Lack Thereof, to Decrypt, Circumvent, or Defeat Communications Security Protocols [Interrogatory No. 20; RFA No. 40]

117. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

118. **(U)** In particular, Wikimedia's Interrogatory No. 20 asks the Government to describe any Internet Protocols subject to Upstream surveillance that the NSA is able to decrypt. RFA No. 40 asks a related but narrower question: whether the NSA has the ability to decrypt any portion of HTTPS communications that may be subject to Upstream surveillance. Wikimedia asked similar questions during the deposition of the NSA's designated witness.

119. **(~~TS//SI//NF~~)** [redacted]

120. **(~~TS//SI//NF~~)** [redacted]

[redacted]

G. (U) Additional Categories of Classified Information Contained in Opinions, Orders, and Court Submissions Concerning Upstream Surveillance [RFP Nos. 21-22]

121. **(U)** Finally, as discussed herein, Wikimedia RFP Nos. 21 and 22 ask the Government to produce all FISC, Foreign Intelligence Surveillance Court of Review, and Supreme Court opinions and orders concerning Upstream surveillance, and all submissions to these courts concerning Upstream surveillance, since the enactment of Section 702 in 2008.[13] I am also supporting the DNI's assertions of privilege, and asserting the NSA's statutory privilege, over the additional categories of classified information contained in the more than 10,000 pages of documents responsive to RFP Nos. 21 and 22.

122. **(~~TS//SI//NF~~)** [redacted]

[13] **(U)** As noted earlier, neither the Foreign Intelligence Court of Review, nor the Supreme Court, has issued any opinions or orders, nor has the Government made any filings in either court, concerning Upstream surveillance.

[redacted]

123. (~~TS//SI//NF~~) [redacted]

[redacted]

124. (~~TS//SI//NF~~) [redacted]

[redacted]

125. (~~TS//SI//NF~~) [redacted]

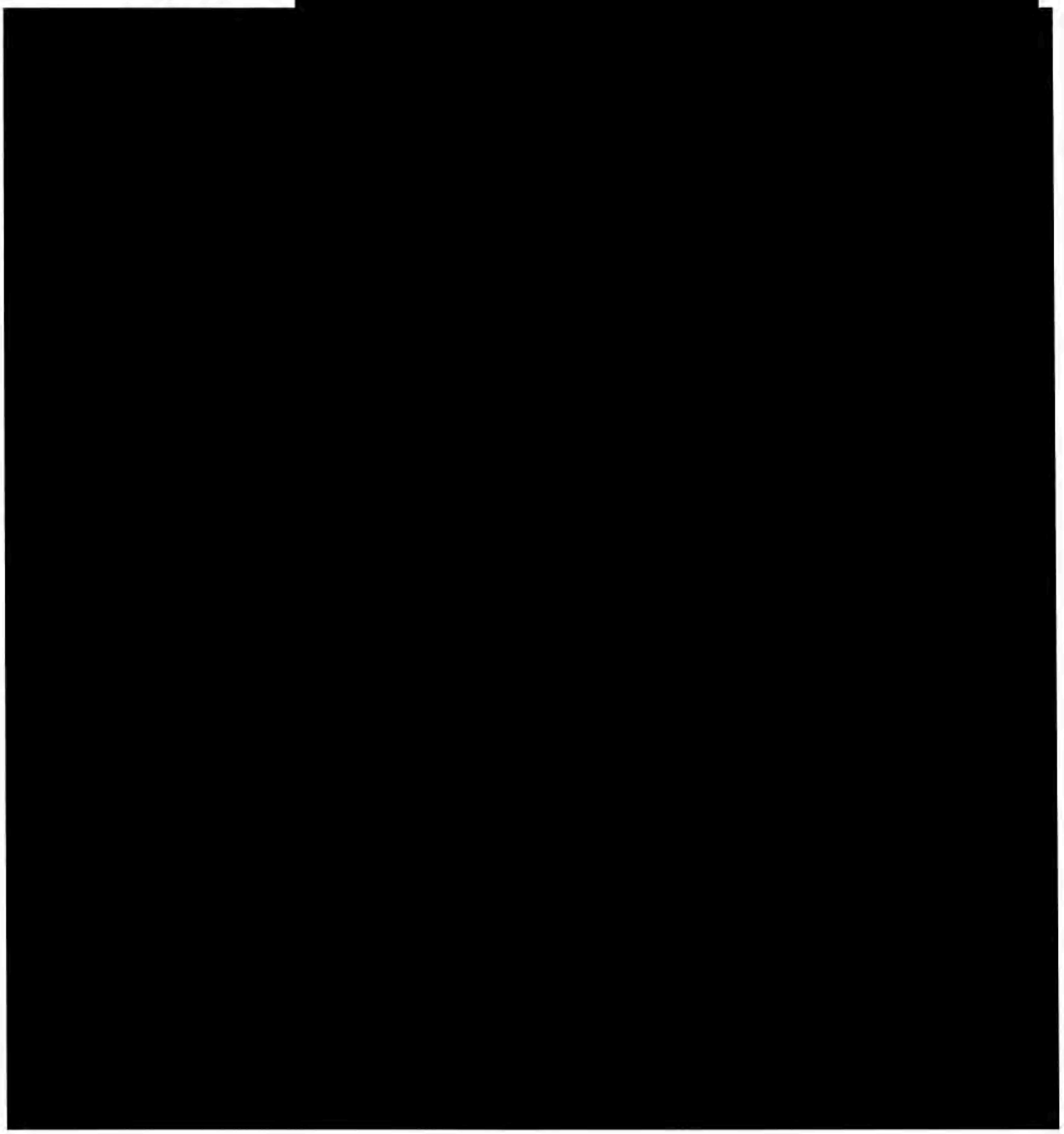
126. (~~TS//SI//NF~~) [redacted]

[redacted]

127. (~~TS//SI//NF~~) [redacted]

[redacted]

128. (~~S//OC//NF~~) [redacted]



129. (U) For the reasons discussed above, disclosure of the aforementioned categories of classified information contained in documents responsive to Wikimedia's RFP Nos. 21 and 22

could reasonably be expected to cause exceptionally grave harm to the national security of the United States.

VII. (U) CONCLUSION

130. **(U)** Set forth in this declaration is the NSA's support for the assertion by the DNI of the state secrets privilege, of the statutory privilege under 50 U.S.C. § 3024(i)(1), and the NSA's assertion herein of the privilege under 50 U.S.C. § 3605(a), over the foregoing seven categories of classified information, whether sought in response to Wikimedia's pending discovery requests, in response to any future discovery requests Wikimedia may serve in this case, or as otherwise may become necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this case. The information contained in the above-described categories concerns critical NSA intelligence-gathering functions, is classified, and extraordinarily sensitive. Its disclosure could cause exceptionally grave damage to the national security of the United States. For the reasons explained above, I therefore support the assertion by the DNI of the state secrets privilege over this information, of the statutory privilege under 50 U.S.C. § 3024(i)(1), and I assert NSA's privilege under Section 6 of the National Security Agency Act, 50 U.S.C. § 3605(a).

~~TOP SECRET//SI//ORCON/NOFORN~~

I declare under penalty of perjury, pursuant to 28 U.S.C § 1746, that the foregoing is true and correct to the best of my knowledge and belief.

Executed on April 24, 2018

[redacted]

GEORGE C. BARNES, Deputy Director
National Security Agency