

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

---

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

---

**EXHIBIT B**

**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.	)	

---

**PUBLIC DECLARATION OF DANIEL R. COATS,  
DIRECTOR OF NATIONAL INTELLIGENCE**

I, DANIEL R. COATS, do hereby state and declare as follows:

**INTRODUCTION**

1. I am the Director of National Intelligence (“DNI”) and have held this position since March 16, 2017. As the DNI, I oversee the United States Intelligence Community (“IC”) and serve as the principal intelligence advisor to the President. Prior to commencing my role as the DNI, I held various positions within the United States Congress. Specifically, from 1981 to 1999, I served in the U.S. House of Representatives and then in the U.S. Senate. During this tenure, I served on the Senate Armed Services Committee and the Senate Select Committee on Intelligence where I worked to strengthen our nation’s defense and security. Following my time in Congress, I was named U.S. Ambassador to the Federal Republic of Germany, where I served as the Ambassador from 2001 to 2005. As a U.S. Ambassador and Chief of Mission, I was responsible for leading the embassy’s charge to ensure that U.S. foreign policy goals were advanced; the embassy served American interests and values, and all executive branch agencies attached to the embassy did likewise; and executive, legislative, and judicial responsibilities were

carried out. Further, in my role as Chief of Mission, I was directly responsible for the security of the mission, including security from terrorism and protection of all U.S. Government personnel on official duty. After my tenure as U.S. Ambassador to the Federal Republic of Germany, I returned to the U.S. Senate in 2011 and again served on the Senate Select Committee on Intelligence, where I was charged with overseeing intelligence activities and programs of the U.S. Government.

2. The position of the DNI was created by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, §§ 1011(a) and 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending sections 102 through 104 of Title I of the National Security Act of 1947). Subject to the authority, direction, and control of the President, the DNI serves as the head of the IC and as the principal adviser to the President and the National Security Council for intelligence matters related to national security. *See* 50 U.S.C. § 3023(b)(1)-(2).

3. The IC includes the Office of the Director of National Intelligence; the National Security Agency (“NSA”); the Central Intelligence Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Office of Intelligence and Analysis of the Department of the Treasury; the Office of Intelligence and Analysis of the Department of Homeland Security; and such other elements of any other department or agency as may be designated by the President, or jointly

designated by the DNI and heads of the department or agency concerned, as an element of the IC. *See* 50 U.S.C. § 3003(4); *see also* Executive Order 12333 § 3.5.

4. The National Security Act of 1947, as amended, provides that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” 50 U.S.C. § 3024(i)(1). By this language, Congress expressed its determination that disclosure of intelligence sources or methods is potentially harmful to national security and directed the DNI to protect them.

5. By virtue of my position as the DNI, unless otherwise directed by the President, I have access to all intelligence related to the national security that is collected by any department, agency, or other entity of the United States. 50 U.S.C. § 3024(b).

6. I make the following statements based on my personal knowledge and on information made available to me in my official capacity. Moreover, I have read and personally considered the information contained in the *In Camera, Ex Parte* Declaration of George C. Barnes, Deputy Director, NSA, executed on April 24, 2018 (hereinafter “Classified NSA Declaration”).

7. In the course of my official duties, I have been advised of the above-captioned lawsuit and the allegations by the plaintiff, Wikimedia Foundation (“Wikimedia”), concerning NSA’s “Upstream” surveillance, a technique employed by the NSA to gather foreign intelligence information under section 702 of the Foreign Intelligence Surveillance Act (“FISA”). I have also been advised of Wikimedia’s motion to compel the Government to disclose certain documents and information responsive to Wikimedia’s discovery requests (“Motion to Compel”). The purpose of this declaration is to formally assert, in my capacity as DNI and head of the IC, the state secrets privilege and my statutory privilege under the National Security Act in order to

protect intelligence information, sources, and methods that are at risk of disclosure in this case as a result of Wikimedia's Motion to Compel. *See* 50 U.S.C. § 3024(i)(1). This assertion of privilege is over highly sensitive and classified national security information concerning NSA's Upstream surveillance and falling within the categories described herein. This information must be protected because its disclosure reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

### SUMMARY

8. As detailed in this declaration and in the Classified NSA Declaration, disclosure of the documents and information that Wikimedia seeks to compel the Government to disclose reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States. This information should be protected from disclosure to Wikimedia and excluded from any use in this case.

9. Accordingly, as set forth further below, I am asserting the state secrets privilege and the DNI's statutory authority to protect intelligence sources and methods pursuant to 50 U.S.C. § 3024(i)(1) to protect against the disclosure of highly classified and important intelligence information, sources, and methods regarding Upstream surveillance that Wikimedia has sought to compel the Government to disclose in response to Wikimedia's discovery requests (and certain deposition questions) and 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. Such information is vital to the national security of the United States and covers the following seven categories: (A) information that would tend to confirm what individuals or entities are subject to Upstream surveillance activities; (B) information concerning the operational details of the Upstream collection process; (C) the

location(s) at which Upstream surveillance is conducted; (D) the categories of Internet-based communications collected through Upstream surveillance activities; (E) information concerning the scope and scale of Upstream surveillance; (F) NSA cryptanalytic capabilities; and (G) additional categories of classified information regarding Upstream surveillance contained in opinions and orders issued by, and submissions made to, the Foreign Intelligence Surveillance Court (“FISC”).

10. I make these assertions of privilege mindful of the public disclosures—both authorized and unauthorized—of information about classified NSA intelligence programs, including the IC’s declassification and public release of certain materials concerning NSA’s Upstream surveillance, which is the program that is challenged in this lawsuit. However, it has remained necessary to withhold considerable details about Upstream surveillance, even from publicly released documents, to protect highly sensitive intelligence information, sources and methods, such as particular subjects of surveillance and methods of collecting and analyzing intelligence information. Therefore, notwithstanding prior disclosures, it is my judgment that additional disclosure of the highly sensitive and still-classified documents and information that Wikimedia has sought to compel the Government to disclose in this case would cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

11. Furthermore, my assertions of privilege have not been made to conceal a violation of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency of the Government; to restrain competition; or to prevent or delay the release of information that does not require protection in the interests of national security.

12. For these reasons, as set forth further below, I request that the Court uphold the state secrets and statutory privilege assertions that I make herein, as well as the statutory privilege assertion made by the NSA pursuant to Section 6 of the National Security Agency Act (50 U.S.C. § 3605(a)), and protect from disclosure the information that Wikimedia now seeks to compel the Government to disclose.

**BACKGROUND OF THE CHALLENGED UPSTREAM PROGRAM**

13. In July 2008, Congress enacted the Foreign Intelligence Surveillance Act Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436. This Act 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 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). Although the statute does not require the IC 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).

14. 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 by the Attorney General in consultation with the DNI, 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 IC determines whether a person is a non-U.S. person reasonably believed to be located outside the United States who is likely to possess or receive foreign intelligence information authorized for acquisition by a certification.<sup>1</sup>

15. There are two types of Section 702 acquisition: what has been publicly referred to as “PRISM” collection and “Upstream” collection. I understand that this case involves a legal challenge to Upstream collection. In unclassified terms, in the course of the Upstream collection process, certain Internet transactions transiting the Internet backbone network(s) of certain electronic communication service provider(s) are filtered for the purpose of excluding wholly domestic communications and are then scanned to identify for acquisition those transactions that

---

1. Four requirements must be met for FISC approval of a Section 702 certification. First, the Attorney General and the DNI must certify, among other things, 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)(v), (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 (a) are limited to targeting non-U.S. persons reasonably believed to be located outside the United States, and (b) 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(j)(3)(A). Following passage of the FISA Amendments Reauthorization Act of 2017, 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).



are to or from (or, prior to early 2017, to, from, or “about”) persons<sup>2</sup> targeted in accordance with the applicable NSA targeting procedures; only those transactions that pass through both the filtering and the scanning are ingested into Government databases. While the Upstream collection process has been described in general terms in this declaration and in declassified documents and unclassified reports, certain operational details of Upstream collection remain highly classified as described in the Classified NSA Declaration.

**ASSERTION OF THE STATE SECRETS PRIVILEGE**

16. After careful and actual personal consideration of the matter, based upon my own knowledge and on information obtained in the course of my official duties, including the information contained in the Classified NSA Declaration, I have determined that Wikimedia’s Motion to Compel implicates highly sensitive and classified state secrets concerning intelligence information, sources, and methods. Disclosure of such information—as set forth herein and described in more detail in the Classified NSA Declaration—reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States. This information must be protected from disclosure and excluded from use in this case. Therefore, as to the information Wikimedia seeks to compel the Government to disclose, I formally assert the state secrets privilege.

**ASSERTION OF STATUTORY PRIVILEGE UNDER NATIONAL SECURITY ACT**

17. Through this declaration, I also hereby invoke and assert a statutory privilege held by the DNI under the National Security Act of 1947, as amended, to protect the information described herein and in the Classified NSA Declaration, *see* 50 U.S.C. § 3024(i)(1). My

---

2. When the NSA targets a non-U.S. person under Section 702, it must identify a specific communications identifier, known as a “selector.” A selector cannot be the name of the individual or a keyword.

assertion of this statutory privilege for intelligence sources and methods is coextensive with my state secrets privilege assertion.

**INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE**

18. In general and unclassified terms, documents and information responsive to Wikimedia's discovery requests that Wikimedia has sought to compel the Government to disclose are subject to my state secrets and statutory privilege assertions because they contain the following seven categories of classified information:

- A. *Individuals or 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;
- B. *Operational Details of the Upstream Collection Process:* Documents and information (not already encompassed by other categories herein) responsive to Wikimedia's pending discovery requests or 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;
- C. *Location(s) 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;

- D. *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;
- E. *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;
- F. *NSA Cryptanalytic Capabilities (or Lack Thereof):* 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; and
- G. *Additional Categories of Classified Information Contained in Opinions and Orders issued by, and submissions made to, the FISC Concerning Upstream:* The additional categories of classified information contained in the documents responsive to Wikimedia’s discovery Requests for Production numbered 21 and 22 (and not already encompassed by categories A-F, above) as set forth in the privilege log served by Defendant United States Department of Justice on March 19, 2018.

**HARM OF DISCLOSING INFORMATION SUBJECT TO PRIVILEGE**

19. As discussed in detail in the Classified NSA Declaration, protection of these categories of information is key to the NSA's ability to produce foreign intelligence information, which depends on its access to foreign and international electronic communications. Foreign intelligence information produced by communications intelligence activities, such as Upstream surveillance, is an extremely important part of the overall foreign intelligence information available to the United States. Indeed, communications intelligence is often the only means by which the United States can learn the existence of particular threats or the identities of particular individuals who are involved in hostile activities. Communications intelligence is thus essential to the ability of the IC to identify adversaries and to detect and disrupt their plans for attacks and other hostile acts against the United States. Against that backdrop, the risks of disclosing the specific categories of information described herein are especially grave.

20. Below, I describe each of these categories, and the harm that reasonably could be expected to result from disclosure, in unclassified terms. Much of the harm, however, necessarily must be described in classified terms, and, as such, is set forth in the Classified NSA Declaration.

**A. Information That May Tend to Confirm or Deny Whether or Not the Communications of Wikimedia or Other Individuals or Entities Have Been Subjected to Upstream Surveillance Activities.**

21. The first category of information over which I am asserting privilege is information that would tend to reveal whether particular individuals or entities, including Wikimedia, have been subjected to Upstream surveillance activities. Disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

22. My privilege assertion over information that may tend to confirm or deny whether or not the communications of Wikimedia, or other individuals or entities, have been subject to Upstream surveillance includes, for example, Wikimedia's attempt to compel the Government to confirm or deny whether or not NSA has copied, reviewed the content of, and/or retained at least one Wikimedia communication in the course of Upstream surveillance, and Wikimedia's attempt to compel the Government to confirm or deny the authenticity of purportedly classified documents which Wikimedia believes indicate that the NSA targets its communications for Upstream surveillance.

23. The Government cannot publicly confirm or deny whether any particular individual or entity is subject to intelligence-gathering activities, no matter how likely or unlikely it might appear that the individual or entity would be subject to surveillance. If the Government were to reveal that an individual or entity is the target or a subject of intelligence-gathering, the collection capability relating to that individual or entity would certainly be compromised. On the other hand, if the Government were to reveal that an individual or entity is not the target or subject of intelligence-gathering, adversaries would know that a particular individual has avoided scrutiny and is a secure source for communicating. Moreover, providing assurances to those individuals who (or entities which) are not targets or subjects quickly becomes unworkable when faced with a situation in which an individual (or entity) has in fact been a target or subject. If the Government were to confirm that any specific individual or entity is not a target or subject of intelligence-gathering, but later refuse to confirm or deny that fact in a situation involving an actual target or subject, it would be apparent that intelligence-gathering was occurring in the latter case. The only recourse for the Government is to neither confirm nor deny whether someone (or some entity) has been targeted by or subject to NSA intelligence-gathering

activities, regardless of whether the individual or entity has been a target or subject or not. To say otherwise when challenged in litigation would result in the frequent, routine exposure of intelligence information, sources, and methods, and would severely undermine surveillance activities in general.

24. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**B. Operational Details of the Upstream Collection Process.**

25. The second category of information over which I am asserting privilege is still-classified information concerning the operational details of the Upstream collection process, as discussed in greater detail in the Classified NSA Declaration (and where such information is not already encompassed by other categories of privileged information described elsewhere in this declaration). Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

26. My privilege assertion over the operational details of the Upstream collection process includes, for example, Wikimedia's request for additional technical details concerning "filtering mechanisms" employed by NSA and the "scanning," "screening," and content review of communications during Upstream surveillance. Although the IC has publicly acknowledged the existence of the Upstream surveillance program and has publicly released a limited amount of information describing, at a high level of generality, how Upstream operates, additional technical details about the Upstream collection process remain classified.

27. As discussed in greater detail in the Classified NSA Declaration, disclosure of still-classified operational details regarding Upstream surveillance, either directly or indirectly, would reveal to our adversaries the extent of the ability of the United States to monitor and track their activities and communications, thereby helping our adversaries evade detection, which would seriously compromise, if not destroy, important and vital ongoing intelligence operations.

28. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**C. The Location(s) Where Upstream Surveillance is Conducted.**

29. The third category of information over which I am asserting privilege is information that would, directly or indirectly, tend to reveal the location(s) on the Internet backbone where Upstream surveillance is conducted. Public disclosure of such information, even at a general level, reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

30. My privilege assertion over the location(s) on the Internet backbone where Upstream surveillance is conducted includes information regarding the number and nature of such Upstream surveillance point(s). For example, Wikimedia has sought disclosure of information sufficient to show the “number of circuits” and “number of Internet chokepoints” at which Upstream surveillance is conducted. Although the IC has publicly acknowledged that Upstream surveillance is conducted on one or more points on the Internet backbone, we have not acknowledged any further details regarding the location of these one or more points or any information about the nature or number of these one or more points.

31. As discussed in greater detail in the Classified NSA Declaration, disclosing information on the location(s) where Upstream surveillance is conducted would assist foreign adversaries in trying to evade particular channels of communications that are being monitored, exploit any particular channels of communications that are not being monitored, and target location(s) where the NSA obtains critical foreign intelligence information for hostile action.

32. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration), either directly or indirectly, would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**D. Categories of Internet-Based Communications Subject to Upstream Surveillance Activities.**

33. The fourth category of information over which I am asserting privilege is information that would tend to reveal categories of Internet-based communications subject to and not subject to Upstream surveillance activities. Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

34. My privilege assertion over information that would tend to reveal the types of communications collected through Upstream surveillance includes, for example, information sought by Wikimedia in deposition questions it asked NSA's designated witness concerning whether NSA collection devices are configured to exclude various types of encrypted communications. However, as discussed in greater detail in the Classified NSA Declaration, disclosing information on the types of communications collected through Upstream surveillance would induce our foreign adversaries to avoid those forms of online communications in order to defeat NSA's attempts to capture their communications.



35. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**E. Information Concerning the Scope and Scale of Upstream Surveillance.**

36. The fifth category of information over which I am asserting privilege is information concerning the scope and scale of Upstream surveillance. Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

37. My privilege assertion over the scope and scale of Upstream surveillance includes, for example, Wikimedia's requests that the Government describe the approximate amount of Internet traffic subject to each stage of the Upstream collection process and that the Government admit that the NSA conducts Upstream surveillance on "multiple international Internet links." The IC has publicly acknowledged that (a) NSA is monitoring at least one circuit carrying international Internet communications and (b) the Upstream process necessarily involves the NSA having access to a larger body of communications than those that contain the targeted selectors in order to filter and scan that larger body to ingest into NSA repositories only those communications containing the selectors. However, any additional facts about the scope and scale of the Upstream surveillance program remain classified.

38. As discussed in greater detail in the Classified NSA Declaration, disclosing information regarding the scope and scale of Upstream surveillance would inform foreign adversaries whether they should increase or decrease their efforts to avoid such surveillance.

39. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**F. NSA Cryptanalytic Capabilities (or Lack Thereof).**

40. The sixth category of information over which I am asserting privilege is information concerning NSA's capabilities, or lack thereof, to decrypt, circumvent, or defeat communications security protocols. Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

41. My privilege assertion over the NSA's cryptanalytic capabilities includes, for example, Wikimedia's request that the Government describe any Internet Protocols subject to Upstream surveillance that NSA is able to decrypt, as well as Wikimedia's request that the Government admit whether NSA has the ability to decrypt any portion of HTTPS (HyperText Transfer Protocol Secure) communications that may be subject to Upstream surveillance.

42. As discussed in greater detail in the Classified NSA Declaration, NSA's capabilities against communications security protocols are exceptionally fragile. Public disclosure of information concerning NSA's capabilities, or lack thereof, to decrypt, circumvent, or defeat communications security protocols would cause adversaries to shift their communications to less susceptible protocols. NSA's resulting loss of foreign intelligence information would cause irreparable damage to national security.

43. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would

compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**G. Additional Categories of Classified Information Contained in Opinions and Orders Issued by, and Submissions Made to, the FISC Concerning Upstream Surveillance.**

44. Finally, the seventh category of information over which I am asserting privilege is information contained in opinions and orders issued by, and submissions made to, the FISC concerning Upstream surveillance (where such information is not already encompassed by other categories of privileged information described elsewhere in this declaration). Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

45. My privilege assertion over information contained within opinions and orders issued by, and submissions made to, the FISC concerning Upstream surveillance stems from Wikimedia's request that the Government produce every such opinion, order, or submission concerning Upstream surveillance in its entirety. Although the IC has already publicly released some of these documents in redacted form—including a release of significant FISC opinions concerning FISA Section 702—additional information in these documents remains classified.

46. Because Wikimedia has nonetheless sought disclosure of every opinion, order, and submission concerning Upstream, its expansive request necessarily implicates multiple categories of information, which cannot be described further on the public record but are set forth in the Classified NSA Declaration. The release of this information would be devastating to NSA's mission and collection efforts pursuant to Upstream surveillance, as described in the Classified NSA Declaration.

47. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would

compromise important and critical information, sources, and methods, causing serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

**CONCLUSION**

48. In sum, I am asserting the state secrets privilege and the DNI's statutory privilege set forth in 50 U.S.C. § 3024(i)(1) to protect classified documents and information regarding Upstream surveillance that Wikimedia has sought to compel the Government to disclose in response to Wikimedia's discovery requests (and certain deposition questions), as well as 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 have set forth, in general and unclassified terms, as much as I can say on the public record concerning the highly sensitive and classified intelligence information, sources, and methods covered by my privilege assertions and the harm that would result from their disclosure; for a more detailed, classified description of such information, I respectfully refer the Court to the Classified NSA Declaration.

49. I respectfully request that the Court take all steps necessary to protect the intelligence information, sources, and methods described herein in order to prevent serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: April 25, 2018

  
\_\_\_\_\_  
DANIEL R. COATS  
Director of National Intelligence