No. 19-16066

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

CAROLYN JEWEL, et al.,

Plaintiffs-Appellants,

v.

NATIONAL SECURITY AGENCY, et al.,

Defendants-Appellees.

On Appeal from the United States District Court
for the Northern District of California

APPELLEES' SUPPLEMENTAL EXCERPT OF RECORD

JOSEPH H. HUNT
Assistant Attorney General

DAVID L. ANDERSON
United States Attorney

H. THOMAS BYRON III
JOSEPH F. BUSA
Attorneys, Appellate Staff
Civil Division, Room 7537
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 305-1754

APPELLEES' SUPPLEMENTAL EXCERPT OF RECORD

INDEX

[1] Electronic Case File numbers in *Jewel v. NSA*, No. 08-cv-04373 (N.D. Cal.)

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
Trial Attorneys

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

Attorneys for the Government Defendants
Sued in their Official Capacities

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants,	No. 08-cv-4373-JSW **PUBLIC DECLARATION OF SUSAN M. GORDON, PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE** No Hearing Date Scheduled) Courtroom 11, 19th Floor Judge Jeffrey S. White

I, SUSAN M. GORDON, do hereby state and declare as follows:

INTRODUCTION

1. I am currently the Principal Deputy Director of National Intelligence (PDDNI) and have held this position since August 7, 2017. As PDDNI, I assist the Director of National Intelligence (DNI), Daniel R. Coats, in his role as head of the Intelligence Community (IC) and

principal intelligence advisor to the President of the United States. Additionally, as PDDNI, I also oversee management of the Office of the Director of National Intelligence (ODNI). Prior to assuming the position of PDDNI, I served in a variety of leadership roles spanning numerous intelligence organizations and disciplines. From 2015 to 2017, I served as the Deputy Director of the National Geospatial-Intelligence Agency (NGA) where I helped the Director of NGA lead the agency and manage the National System of Geospatial Intelligence. Prior to my assignment with NGA, I served for 27 years at the Central Intelligence Agency (CIA). In 1980, I joined the CIA as an analyst in the Office of Scientific and Weapons Research, and went on to serve as the Director of the Office of Advanced Analytic Tools, Director of Special Activities in the Directorate of Science and Technology, Director for Support, and ultimately in concurrent roles as Director of the Information Operations Center and the CIA Director's senior advisor on cyber. In 1998, I designed and drove the formation of In-Q-Tel, a private, non-profit company whose primary purpose is to deliver innovative technology solutions for the CIA and the IC. I have been recognized for my performance through numerous awards, including the Presidential Rank Award at the distinguished level. Additionally, I hold a Bachelor of Science degree in zoology (biomechanics) from Duke University.

2. The position of the DNI and PDDNI were 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 U. S. Intelligence Community 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). Pursuant to Section 103A of the National Security Act of 1947 as amended, in the DNI's absence, the PDDNI becomes the Acting DNI and shall act for, and exercise the powers of the DNI. See 50 U.S.C. § 3026(a)(6). The DNI is currently overseas and unavailable to perform various duties, including reviewing and signing this document, and as such I am currently performing the dual roles of both the Acting DNI and PDDNI.

3. The IC includes the Office of the Director of National Intelligence; the Central Intelligence Agency (CIA); the National Security Agency (NSA); 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 Intelligence Community. 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 and methods is potentially harmful and directed the DNI to protect them.

5. By virtue of my position as the PDDNI, and unless otherwise directed by the DNI and 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 upon my personal knowledge and on information made available to me in my official capacity.

7. The purpose of this declaration is to formally assert, in my capacity as Acting DNI, the PDDNI, and Acting Head of the IC, the state secrets privilege and a statutory privilege under the National Security Act of 1947, as amended, *see* 50 U.S.C. § 3024(i)(1), in order to protect intelligence sources and methods that are at risk of disclosure in the above-captioned case. This assertion of privilege is consistent with prior DNI assertions of privilege in this

litigation over still-classified information concerning the scope and operational details of various National Security Agency (NSA) activities, including but not limited to information that would tend to confirm whether particular persons were targets of or subject to NSA intelligence activities, or whether particular telecommunications service providers assisted the NSA in conducting intelligence activities. My current assertion of privilege encompasses the specific classified materials containing such information that the Government will be providing to the Court *in camera* and *ex parte* in response to the plaintiffs' pending discovery requests on the issue of standing, and the Court's related order that the Government marshal all evidence bearing on the standing issue. This information must be protected, because the disclosure of these materials reasonably could be expected to cause extremely grave damage to the national security of the United States.

SUMMARY

8. In the course of my official duties, I have been advised of this lawsuit and the allegations at issue in the plaintiffs' complaint in the *Jewel* action. Moreover, I have read and personally considered the information contained in the *In Camera, Ex Parte* Declaration of Admiral Michael S. Rogers, Director, National Security Agency, executed on February 16, 2018. (hereafter "Classified NSA Declaration"). Furthermore, I am also familiar with prior DNI classified declarations of April 3, 2009; September 11, 2012; and December 20, 2013, assertions of privilege in this litigation. Disclosure of the materials being provided for the Court's *in camera, ex parte* review, including the information contained in the Classified NSA Declaration, in the additional documents responsive to plaintiffs' requests for production of documents, and in any further classified documents and information that may later be provided to the Court in response to plaintiffs' requests, reasonably could be expected to cause exceptionally grave damage to the national security of the United States and, therefore, those materials should be protected from disclosure to the plaintiffs and excluded from any use in this case.

9. I reach this conclusion, and make these assertions of privilege, mindful of the public disclosures of information about classified NSA intelligence programs, both authorized and unauthorized, that have taken place since June 2013. The wave of unauthorized public

disclosures of classified information regarding NSA intelligence activities that began in June 2013 was extremely damaging to the national security of the United States, threatening the ability of the IC to conduct operations effectively and keep our country safe. At the same time, owing to the great public interest that these disclosures generated in the NSA's use of its surveillance authorities to gather intelligence, DNI James Clapper, at the direction of President Barack Obama, declassified and publicly released numerous documents disclosing the existence of, and a number of details about, the NSA's collection of certain international communications, and its prior bulk collection of telephony and Internet metadata, pursuant both to presidential authorization and to provisions of the Foreign Intelligence Surveillance Act (FISA). As he explained at the time, DNI Clapper took these steps after concluding (in light of the unauthorized disclosures) that promoting informed public debate about the value and appropriateness of these programs outweighed the potential for additional damage to national security.

10. As explained, however, in DNI Blair's and DNI Clapper's prior classified declarations, including the December 20, 2013 classified declaration submitted in this matter, it has remained necessary to withhold certain information about these programs, even from publicly released documents, to protect sensitive sources and methods, such as particular targets and subjects of surveillance, and methods of collecting and analyzing intelligence information. Public disclosure of this information would likely cause even graver damage to national security than has already been done by the unauthorized disclosures that have occurred since June 2013. For the reasons set forth in this declaration and in the Classified NSA Declaration, the same is true with respect to the highly sensitive and still-classified materials that the Government Defendants are providing to the Court for its *in camera, ex parte* review, and that the Government Defendants may later provide to the Court in response to plaintiffs' discovery requests. Therefore, notwithstanding the unauthorized disclosures and the official declassification and release of information about NSA intelligence programs that have taken place since June of 2013, it is my judgment that disclosure of the classified, privileged, national security information contained in materials now being or that may later be provided to the Court in response to plaintiffs' discovery requests, as described herein and in greater detail in the

Classified NSA Declaration, will risk further and exceptionally grave damage to the national security of the United States.

11. Accordingly, as set forth further below, I am asserting the state secrets privilege and the DNI's authority to protect intelligence sources and methods pursuant to 50 U.S.C. § 3024(i)(l) to protect against the disclosure of highly classified and important intelligence information, sources, and methods contained in the materials being produced to the Court *ex parte* and *in camera*, many of which are vital to the national security of the United States, including: (a) information that would tend to confirm whether or not particular individuals have been subject to any of the NSA intelligence activities challenged in this case; (b) information concerning the scope or operational details of the challenged activities; and (c) information that may tend to confirm whether or not specific telecommunications carriers have provided assistance to the NSA in connection with any of the challenged activities.

12. I specifically concur with the NSA that public speculation about alleged NSA intelligence activities above and beyond what has been officially disclosed does not diminish the need to protect intelligence sources and methods from further exposure, and that official confirmation and disclosure of the classified, privileged, national security information contained in the classified materials being provided to the Court for *in camera, ex parte* review can be expected to cause exceptionally grave damage to the national security. 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, see 50 U.S.C. § 3605(a), and protect from disclosure the materials being provided to the Court for its *in camera, ex parte* review.

BACKGROUND OF THE CHALLENGED NSA INTELLIGENCE ACTIVITIES

13. In the aftermath of the September 11, 2001, terrorist attacks on the United States, President Bush authorized the Secretary of Defense to employ the capabilities of the Department of Defense, including the NSA, to collect foreign intelligence by electronic surveillance in order to detect and prevent acts of terrorism within the United States. Starting on October 4, 2001, President Bush authorized the NSA to collect (1) the contents of certain international

communications, a program that was later referred to and publicly acknowledged by President Bush as the Terrorist Surveillance Program (TSP), and (2) telephony and Internet non-content information (referred to as "metadata") in bulk, subject to various conditions. Collectively, these activities are referred to as the President's Surveillance Program ("PSP").

14. President Bush issued authorizations of the PSP approximately every 30-60 days. Although the precise terms changed over time, each presidential authorization required the minimization of information collected concerning American citizens to the extent consistent with the effective accomplishment of the mission of detection and prevention of acts of terrorism within the United States. The NSA also applied additional internal constraints on the presidentially authorized activities.

15. Over time, the presidentially authorized activities transitioned to the authority of the FISA. The collection of communications content pursuant to presidential authorization ended in January 2007 when the U.S. Government transitioned the TSP to the authority of FISA under orders of the FISC. In August 2007, Congress enacted the Protect America Act ("PAA") as a temporary measure. The PAA expired in February 2008 and was replaced by the FISA Amendments Act of 2008 ("FAA"), which was enacted in 2008 and remains in effect today. Today, content collection is conducted pursuant to section 702 of FISA ("Section 702"), enacted by the FAA, which authorizes the targeting of non-U.S. persons located outside the United States for the purpose of obtaining foreign-intelligence information. The metadata activities also were transitioned to orders of the FISC. The bulk collection of telephony metadata transitioned to the authority of FISA in May 2006, and was discontinued in November 2015 in accordance with the provisions of the USA-FREEDOM Act, Pub. L. 114-23, 129 Stat. 268. The bulk collection of Internet metadata was transitioned to the authority of FISA in July 2004 and was collected pursuant to section 402 of FISA. In December 2011, the U.S. Government decided not to seek re-authorization of the bulk collection of Internet metadata under section 402.

16. As a result of the declassification of the information described above, the U.S. Government is no longer asserting privilege over the existence of these programs, whether conducted under presidential authority or FISC authorization. It has remained necessary,

however, to withhold certain information about these programs, even from the publicly released documents, to protect sensitive sources and methods, such as particular targets of surveillance, and methods of collecting and analyzing intelligence information, because public disclosure of this information would likely cause even graver damage to national security than has already been done by the unauthorized disclosures that have occurred since June 2013. As explained in great detail herein, and in the accompanying Classified NSA Declaration, the same is true with respect to the highly sensitive and still classified materials that the Government Defendants are providing to the Court for its *in camera, ex parte* review.

18. Accordingly, notwithstanding the unauthorized disclosures and the official declassification and release of information about NSA intelligence programs that have taken place since June of 2013, it is my judgment that disclosure of the classified, privileged national security information contained in the materials being provided to the Court, and described in greater detail in the Classified NSA Declaration, will risk further and exceptionally grave damage to the national security of the United States.

ASSERTION OF THE STATE SECRETS PRIVILEGE

19. After careful and actual personal consideration of the matter, based upon my own knowledge and information obtained in the course of my official duties, including the information contained in the Classified NSA Declaration, I have determined that sensitive state secrets concerning NSA sources, methods, and activities are contained in the materials responsive to plaintiffs' discovery requests that are now being and may later be provided to the Court for *in camera, ex parte,* review, and that the disclosure of those materials—as set forth herein and described in more detail in the Classified NSA Declaration—can be expected to cause exceptionally grave damage to the national security of the United States, and therefore those materials must be protected from disclosure and excluded from this case. Thus, as to the materials being provided to the Court for *in camera, ex parte,* review, I formally assert the state secrets privilege.

ASSERTION OF STATUTORY PRIVILEGE UNDER NATIONAL SECURITY ACT

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

INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE

21. In general and unclassified terms, materials responsive to plaintiffs' discovery requests that are now being or may later be provided to the Court for *in camera, ex parte* review, are subject to my state secrets and statutory privilege assertions because they contain the following categories of still-classified information:

A. *Persons Subject to Intelligence Activities*: information that would tend to confirm or deny whether particular individuals, including the named plaintiffs, have been subject to any NSA intelligence activities;

B. *Operational Information Concerning NSA Intelligence Activities:* information concerning the scope and operational details of NSA intelligence activities, including:

(1) *Communications Content Collection:* information concerning the scope and operational details of NSA intelligence activities related to the collection of Internet communications content under the PSP, transitional FISA authority, or FISA Section 702;

(2) *Communications Metadata Collection:* information concerning the scope or operational details of NSA intelligence activities relating to the bulk collection of telephony and Internet non-content communications metadata under the PSP, or authority of FISA;

and

C. *Telecommunications Provider Identities:* information that would tend to confirm or deny whether any telecommunications carrier has provided assistance to the NSA in connection with any intelligence activity, including the activities at issue in this litigation.

HARM OF DISCLOSING INFORMATION SUBJECT TO PRIVILEGE

22. Broadly speaking, classified materials responsive to plaintiffs' discovery requests that are now being or may later be provided to the Court for its *in camera, ex parte* review contain three categories of information subject to my assertion of privilege. Below, I describe each category, and the harm that reasonably could be expected to result from its disclosure, in unclassified terms.

23. 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 produced by communications intelligence activities is an extremely important part of the overall foreign intelligence information available to the United States, and is often unobtainable by other means. Disclosure of either the capability to collect specific communications or the information derived from such collection can easily alert targets to the vulnerability of their communications. Once alerted, targets can frustrate collection by using different or new encryption techniques, by disseminating disinformation, or by utilizing different means of collection. Disclosing operational details about the manner in which the NSA collects communications data would facilitate such evasion techniques, further inhibiting access to a target's communications, and thereby deny the Government access to information crucial to the defense of the United States both at home and abroad.

24. Moreover, disclosure of information that would compromise or destroy the NSA's intelligence-gathering operations would be especially damaging in the NSA's efforts against foreign terrorist organizations and other foreign adversaries that threaten the national security of the United States. Communications intelligence is essential to the ability of the Intelligence Community to identify enemy actors and to detect and disrupt their plans for further attacks and other hostile acts against the United States. Communications intelligence is often the only means by which the United States can learn the identities of particular individuals who are involved in terrorist or other hostile activities, or the existence of particular threats. Against that backdrop, the risks of disclosing the above-described categories of information are especially grave.

A. Information That May Tend To Confirm or Deny Whether Particular Individuals, Including the Named Plaintiffs, Have Been Subject to NSA Intelligence Activities.

25. I am asserting privilege over information that would tend to reveal whether particular individuals, including the named plaintiffs in this lawsuit, have been subject to NSA intelligence activities implicated by plaintiffs' allegations. Disclosure of such information can be expected to cause exceptionally grave damage to the national security.

26. The NSA cannot publicly confirm or deny whether any particular individual is subject to intelligence-gathering activities, no matter how likely or unlikely it might appear that the individual would be subject to surveillance. If the NSA were to reveal that an individual is the target or a subject of intelligence-gathering, the collection capability relating to that individual would certainly be compromised. On the other hand, if the NSA were to reveal that an individual 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 are not targets or subjects quickly becomes unworkable when faced with a situation in which an individual has in fact been a target or subject. If the NSA were to confirm that any specific individual 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 NSA is to neither confirm nor deny whether someone has been targeted by or subject to NSA intelligence-gathering activities, regardless of whether the individual has been a target or subject or not. To say otherwise when challenged in litigation would result in the frequent, routine exposure of NSA information, sources, and methods, and would severely undermine surveillance activities in general.

B. Information Concerning the Scope or Operational Details of NSA Intelligence Activities, Including NSA Sources or Methods.

27. Furthermore, I am asserting privilege over any other still-classified facts concerning the scope or operational details of any NSA intelligence activities included in the materials provided for the Court's *in camera, ex parte* review. As noted above, my privilege

assertion encompasses (1) facts concerning the operation of the now-defunct TSP, including any facts needed to demonstrate that the TSP was limited to the interception of the content[1] of one-end foreign communications reasonably believed to involve a member or agent of al-Qa'ida or an affiliated terrorist organization, (2) facts concerning the operation of the collection of one-foreign communications of non-U.S. persons located abroad under FISA, including FISA Section 702; and (3) still classified information concerning the scope or operational details of NSA intelligence activities involving the collection of bulk communications metadata, as discussed in greater detail in the Classified NSA Declaration.

28. As the NSA indicates, *see* Classified NSA Declaration, the NSA's collection of the content of communications under the TSP was directed at international communications in which a participant was reasonably believed to be associated with al-Qa'ida or an affiliated organization. Its collection of communications content under FISA Section 702 is directed at the one-end foreign communications of non-U.S. persons reasonably believed to be located outside the United States, for the purpose of collecting foreign-intelligence information as defined under the statute. Thus, as the U.S. Government has previously stated in this case, plaintiffs' allegation that the NSA has indiscriminately collected the content of millions of communications sent or received by people inside the United States, whether under the TSP, FISA Section 702, or otherwise, is false. I concur with the NSA that to the extent materials responsive to the plaintiffs' discovery requests that are now being or may later be submitted to the Court for *in camera, ex parte* review demonstrate that the TSP was not the content dragnet surveillance plaintiffs allege, or demonstrate that the NSA has not engaged in a content dragnet surveillance under Section 702, those materials contain highly classified details about the scope and operation of NSA intelligence activities, including NSA intelligence sources and methods, and their disclosure would risk exceptional harm to national security.

[1] The term "content" is used herein to refer to the substance, meaning, or purport of a communication, as defined in 18 U.S.C.§ 2510(8).

29. Based on my personal consideration and judgment as to the harm disclosure can be expected to cause to national security, my privilege assertion includes, but is not limited to, the following information discussed in the Classified NSA Declaration.

30. I assert privilege over still-classified facts contained in materials responsive to plaintiffs' discovery requests that are now being or may later be provided to the Court for *in camera, ex parte,* review concerning: the scope and operation of the TSP, and the fact that the TSP was limited to the interception of certain one-end communications (*i.e.*, to or from the United States) reasonably believed to involve a member or agent of al-Qa'ida or an affiliated terrorist organization; the scope and operation of the collection of communications content under FISA section 702, and the fact that surveillance under Section 702 is targeted at one-end foreign communications of non-U.S. persons reasonably believed to be located outside the United States; and the fact that the NSA does not otherwise conduct a dragnet of content surveillance as the plaintiffs allege. Such facts include those concerning (a) the selection of targets under the TSP, and Section 702; (b) the specific sources and methods used under the TSP, and Section 702, to intercept the content of communications; (c) the nature and identities of targets or subjects of surveillance under the TSP, or Section 702; and (d) any additional classified details about the operation of the TSP, or of content collection under Section 702 that would be necessary to respond to the plaintiffs' discovery requests or otherwise have bearing on the plaintiffs' standing. *See* Classified NSA Declaration. In my judgment, revealing or risking disclosure of the foregoing NSA intelligence activities, sources, and methods reasonably can be expected to cause exceptionally grave harm to national security by disclosing to our adversaries the ability of the United States to monitor and track their activities and communications.

31. I also assert privilege over still-classified facts contained in materials responsive to plaintiffs' discovery requests that are now being or may later be provided *in camera, ex parte,* to the Court that describe the scope or operational details of other NSA intelligence activities, including but not necessarily limited to metadata collection activities. *See* Classified NSA Declaration. In my judgment, the NSA is unable to disclose information about the scope or operation of the NSA's prior bulk collection of Internet or telephony metadata (whether

conducted under presidential or FISC authority), beyond that which has already been officially acknowledged by the U.S. Government, without risking exceptionally grave harm to national security. Disclosing or confirming further details about these activities could seriously undermine an important tool—metadata collection and analysis—for tracking possible terrorist plots or other threats to national security. Disclosure also could reveal methods by which NSA has targeted and continues to target its intelligence-gathering activities, thus helping foreign adversaries evade detection, and otherwise undermining ongoing intelligence operations conducted under E.O. 12333 and FISC authorization.

32. In my judgment, disclosure of still-classified details regarding these intelligence-gathering activities, either directly or indirectly, would seriously compromise, if not destroy, important and vital ongoing intelligence operations. After personal consideration of the matter, it is my judgment that disclosing the information described herein and by the NSA would compromise important and critical activities, sources, and methods, thereby helping our adversaries evade detection and causing exceptionally grave damage to the national security of the United States.

C. Information That May Tend To Confirm or Deny Whether Any Particular Telecommunications Carrier Has Provided Assistance To the NSA In Connection With Any Intelligence Activity.

33. In addition, I am asserting privilege over information responsive to plaintiffs' discovery requests that is now being or may later be submitted for *ex parte, in camera* review that may tend to confirm whether or not plaintiffs' alleged telecommunications providers, or to the extent necessary, any other particular telecommunications provider, has assisted any NSA intelligence activity, including but not necessarily limited to the intelligence activities challenged in this case. The disclosure of any information that would tend to confirm or refute allegations of such assistance can be expected to cause exceptionally grave harm to the national security, for a variety of reasons.

34. Confirming or denying such allegations would reveal to foreign adversaries whether or not the NSA utilizes particular intelligence sources and methods and, thus, either compromise actual sources and methods or disclose that the NSA does not utilize a particular

source or method. For example, revealing that a particular company assists the NSA would compromise a range of intelligence activities by providing confirmation that certain channels of communications are vulnerable to NSA interception. Confirmation or denial of a carrier's assistance would replace speculation with certainty for hostile foreign adversaries who are balancing the risk that a particular channel of communication may not be secure against the need to communicate efficiently.

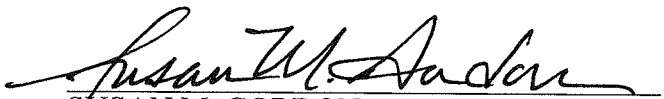
35. That remains so, in my judgment, notwithstanding the U.S. Government's declassification of a now-expired April 25, 2013, FISC order directing Verizon Business Network Services (VBNS) to produce bulk telephony metadata to the NSA. Although the U.S. Government, in acknowledging the existence of the bulk telephony metadata program carried out under FISC authorization, also confirmed the participation of VBNS in that program for the time period covered by that order (April 25 through July 19, 2013), it has not otherwise confirmed or denied the identities of any carriers participating in that or any other NSA intelligence program, during that period or at any other time.

CONCLUSION

36. 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 materials responsive to plaintiffs' discovery requests that are now being or may later be provided to the Court for its *in camera, ex parte* review. I respectfully request that the Court not only protect those materials from disclosure, but take all steps necessary to protect the intelligence information, sources, and methods described herein in order to prevent 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: February 16, 2018



SUSAN M. GORDON
Principal Deputy Director of National Intelligence

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
OLIVIA SCOTT HUSSEY
Trial Attorneys

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W., Room 7320
Washington, D.C. 20001
E-mail: rodney.patton@usdoj.gov
Phone: (202) 305-7919
Fax: (202) 616-8470

Attorneys for the Government Defendants
Sued in their Official Capacities

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 4:08-cv-04373-JSW **NOTICE OF FILING OF REDACTED VERSION OF THE CLASSIFIED DECLARATION THE GOVERNMENT DEFENDANTS LODGED WITH THE COURT *IN CAMERA* AND *EX PARTE* ON FEBRUARY 16, 2018** Hon. Jeffrey S. White Courtroom 5, 2nd Floor Oakland Courthouse

Defendants National Security Agency (NSA), the Department of Justice, the United States of America, Donald J. Trump, in his official capacity as President of the United States; Daniel Coats, in his official capacity as Director of National Intelligence; Admiral Michael S. Rogers, in his official capacity as Director of the NSA; and Jefferson B. Sessions, III, in his

official capacity as Attorney General of the United States (collectively, the "Government Defendants"), hereby give notice that they are filing, as an attachment hereto, a redacted, unclassified version of the Classified Declaration of Michael S. Rogers, Director of the National Security Agency, which was lodged with the Court Information Security Officer on February 16, 2018, for the Court's *in camera, ex parte* consideration. *See* Government Defendants' Notice of Submission of Their Classified and Unclassified Responses to the Court's May 22, 2017 Order, ECF No. 388.

Dated: March 30, 2018

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

/s/ Rodney Patton
RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
Trial Attorneys

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W., Room 7320
Washington, D.C. 20001
E-mail: rodney.patton@usdoj.gov
Phone: (202) 305-7919
Fax: (202) 616-8470

Attorneys for the Government Defendants Sued in their Official Capacities

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
Trial Attorneys

U.S. Department of Justice
20 Massachusetts Avenue, N.W.
Washington, D.C. 20530
Phone: 202-514-3358
E-mail: james.gilligan@usdoj.gov

Counsel for the United States Government
Defendants Sued in Their Official Capacities

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 4:08-cv-4373-JSW **CLASSIFIED DECLARATION OF ADMIRAL MICHAEL S. ROGERS, DIRECTOR, NATIONAL SECURITY AGENCY** ***EX PARTE, IN CAMERA* SUBMISSION** Hon. Jeffrey S. White No hearing scheduled

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

(U) TABLE OF CONTENTS

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

I, Michael S. Rogers, for my declaration pursuant to 28 U.S.C. § 1746, depose and say as follows:

I. (U) INTRODUCTION

1. **(U)** I am the Director of the National Security Agency ("NSA" or "Agency"), an intelligence agency within the Department of Defense. I have held this position since April 2, 2014. In addition to serving as the Director of the NSA, I serve as the Chief, Central Security Service, and as the Commander, U.S. Cyber Command. Since becoming a flag officer in 2007, I have served as the Director for Intelligence of both the Joint Chiefs of Staff and the U.S. Pacific Command, and, most recently, as Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet. As the Director of the NSA, I am responsible for planning, organizing, directing, and managing all NSA-assigned missions and resources. I am accountable to the Director of National Intelligence ("DNI"), the Under Secretary of Defense for Intelligence, and the Department of Defense Chief Information Officer. Further, by specific charge of the President and the DNI, I am ultimately responsible for protecting NSA activities and intelligence sources and methods. 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 twofold. First, the information contained in section V of this *ex parte, in camera* declaration, and the accompanying documents also being made available for the Court's *ex parte, in camera* review, together constitute the Government Defendants' classified responses to Plaintiffs' discovery requests on the issue of standing, in accordance with the Court's May 22, 2017, order to "marshal all evidence" on the standing issue. Second, this declaration supports an assertion of the military and state secrets privilege (hereinafter, "state secrets privilege") by the Principal Deputy DNI ("PDDNI"), in her capacity as Acting DNI and acting head of the Intelligence Community, as well as the PDDNI'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 provided below, in the accompanying documents, and that may hereafter be made available to the Court in response to Plaintiffs' discovery requests. That information concerns critical NSA intelligence-gathering activities and capabilities, is classified, and is extraordinarily sensitive. Its disclosure would 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. § 3601 *et seq.*), to protect the information related to NSA intelligence activities as described herein, in the accompanying documents, and any further information that may be made available to the Court in response to Plaintiffs' requests.

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 Director of the NSA. Specifically, the information contained in section V of this declaration, furnished in response to Plaintiffs' interrogatories and requests for admission, is based on searches of available communications data, information gleaned from documents located after an extensive search, and the current recollections of personnel still employed by the NSA who have been involved with the challenged intelligence programs. While I have no reason to doubt the accuracy of the information presented in section V, below, it represents the best efforts of the Government Defendants to reconstruct the details of events and activities that in some cases occurred long ago, on the basis of incomplete memory and documentation.

II. (U) CLASSIFICATION OF DECLARATION AND ACCOMPANYING DOCUMENTS

4. ~~(S//SI//NF)~~ [redacted]

[redacted]

5. **(U)** Additionally, this declaration and many of the accompanying documents contain 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 and many of the accompanying documents reference 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.[1]

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

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

7. (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 [redacted]

[2] (U) Controlled access programs are kept to "an absolute minimum" and are established and maintained when required by statute or "upon a specific finding that: (1) the vulnerability of, or threat to, specific information is exceptional; and (2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from authorized disclosure." Executive Order No. 13526, § 4.3.

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."

III. (U) SUMMARY

8. **(U)** Plaintiffs in this case allege that, following the terrorist attacks of September 11, 2001, the NSA, pursuant to presidential authorization and with the assistance of Plaintiffs' telecommunications companies, indiscriminately and unlawfully intercepted the content of and obtained metadata about the communications of millions of ordinary Americans as part of alleged "dragnet" communications surveillance. They level similar complaints of unlawful "dragnet" surveillance against NSA content-acquisition and metadata collection activities conducted under authority of the Foreign Intelligence Surveillance Act ("FISA"). In an effort to prove their legal standing to pursue these claims, Plaintiffs have served a total of 160 discovery requests on the Government Defendants, including interrogatories, requests for admission, and document requests. Plaintiffs' discovery requests are apparently intended to uncover direct and indirect evidence to support Plaintiffs' standing to challenge six different NSA intelligence programs conducted over the past 16 years—three as part of the President's Surveillance Program ("PSP"), and three under authority of FISA—involving the collection of international (one-end-foreign) online communications, and the bulk collection of non-content telephony and Internet metadata, for counter-terrorism and foreign-intelligence purposes.

9. **(U)** The Government Defendants have separately filed unclassified objections and responses to Plaintiffs' discovery requests on the public record of the case, as directed by the Court, based in principal part on the classified, privileged, and extraordinarily sensitive nature of the information Plaintiffs seek. Anticipating the Government's objections, the Court has directed the Government Defendants to submit the classified information responsive to Plaintiffs'

requests to the Court for *ex parte, in camera* review, and in doing so to "marshal all evidence" pertinent to the standing issue, so that the Court may determine whether this classified information can be disclosed to Plaintiffs without placing national security at risk. *See* May 22, 2017, Minute Order (ECF No. 356).

10. **(U)** This declaration serves two essential purposes. First, following a background discussion of the NSA, its mission, the challenged intelligence programs, and the threats to national security that they are intended to address, section V of the declaration—together with the documents also being made available for the Court's *ex parte, in camera* review—sets forth the classified information, responsive to Plaintiffs' discovery requests, called for by the Court's May 22, 2017, Order. In so doing, this declaration compiles and presents, in expansive detail, (i) information as to whether Plaintiffs' communications (or metadata associated with them) have been subjected to the challenged NSA intelligence-gathering activities, (ii) information concerning the sources, methods, and technical operational details of the challenged activities, so far as it provides circumstantial evidence regarding Plaintiffs' standing, and (iii) information concerning whether Plaintiffs' telecommunications service providers have provided assistance to the NSA in conducting these programs.

11. **(U)** Second, this declaration supports the assertion of the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1) by PDDNI Susan M. Gordon, in her capacity as Acting DNI, over the classified information presented in this declaration, in the additional materials being provided for the Court's *in camera, ex parte* review, and in any additional classified information the Government may later provide, in response to Plaintiffs' discovery requests. As set forth in PDDNI Gordon's public declaration, and explained in classified detail below, the disclosure of this declaration and these documents would cause exceptionally grave damage to the national security of the United States, and therefore this

declaration and the accompanying documents must be protected from disclosure and excluded from this case.

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

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

Pages 8-10 – Redacted in their Entireties

[redacted]

19. **(U)** These facts include, first, whether or not any of Plaintiffs' communications, or information about their communications, have been subject to NSA intelligence-gathering activities. As a matter of course, the NSA cannot publicly confirm or deny whether any individual is or has been subject to intelligence-gathering activities, because to do so would tend to reveal to our enemies 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 perhaps also sensitive intelligence methods and sources, and thereby help our adversaries evade detection and capitalize on limitations in the NSA's surveillance capabilities.

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

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

[redacted][4]

22. **(U)** For all of these reasons and others further explained below, I support the PDDNI's assertion, in her capacity as Acting DNI, of the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1) to prevent the disclosure of the information described and detailed herein. I also assert the NSA's statutory privilege under Section 6 of the National Security Agency Act over the same information, which concerns the intelligence functions of the NSA. The exceptional compilation of information that the Government Defendants, after extraordinary efforts, have prepared in response to Plaintiffs' discovery requests, and the Court's May 22, 2017, Order, must be protected from disclosure and excluded from this case to avoid exceptionally grave damage to the national security of the United States.

[4] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

IV. (U) BACKGROUND

A. (U) The National Security Agency

23. **(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.[5]

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

---

[5] **(U)** Executive Order 12333, reprinted as amended in 50 U.S.C § 3001 note, generally describes the NSA's authority to collect foreign intelligence that is not subject to the FISA 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."

25. **(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. 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.

26. **(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; cyber-security; arms proliferation; international terrorism; counter-intelligence; and foreign aspects of international narcotics trafficking.

27. **(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 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."

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

28. **(U)** The external threat to the national security of the United States that gave rise to the NSA intelligence activities challenged in this lawsuit was, of course, the threat of international terrorism. On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the east coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Those operatives targeted the Nation's financial center in New York with two of the jetliners, which they deliberately flew into the Twin Towers of the World Trade Center. Al Qaeda targeted the headquarters of the Nation's Armed Forces, the Pentagon, with the third jetliner. Al Qaeda operatives were apparently headed toward Washington, D.C. with the fourth jetliner when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was most likely the White House or the Capitol, strongly suggesting that al Qaeda's intended mission was to strike a decapitating blow to

the Government of the United States—to kill the President, the Vice President, or Members of Congress. The attacks of September 11 resulted in approximately 3,000 deaths—the highest single-day death toll from hostile foreign attacks in the Nation's history. In addition, these attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars of damage to the economy.

29. **(U)** On September 14, 2001, then-President Bush declared a national emergency "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." Presidential Proclamation No. 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001). On September 14, 2001, both Houses of Congress passed a Joint Resolution authorizing the President of the United States "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11. Authorization for Use of Military Force, Pub. L. No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept. 18, 2001) ("Cong. Auth."). Congress also expressly acknowledged that the attacks rendered it "necessary and appropriate" for the United States to exercise its right "to protect United States citizens both at home and abroad," and acknowledged in particular that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." *Id.* pmbl.[6]

[6] **(U)** Following the 9/11 attacks, the United States also immediately began plans for a military response directed at al Qaeda's training grounds and havens in Afghanistan. A Military Order was issued stating that the attacks of September 11 "created a state of armed conflict," *see* Military Order by the President § 1(a), 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001), and that al Qaeda terrorists "possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the United States Government," and concluding that "an extraordinary emergency exists for national defense purposes." Military Order, § 1(c), (g), 66 Fed. Reg. at 57833-34. Indeed, shortly after the attacks, NATO took the unprecedented step of invoking Article 5 of the North Atlantic Treaty, which provides that an "armed attack against one or more of [the parties]

30. **(U)** 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, a set of groups that possesses the evolving capability and intention of inflicting further attacks on the United States. The conflict with al Qaeda and other terrorist groups continues today, at home as well as abroad. Moreover, the conflict against al Qaeda and other terrorist groups is a very different kind of conflict, against a very different enemy, than any other conflict or enemy the Nation has previously faced. Terrorist groups operate not as a traditional nation-state but as a diffuse, decentralized network of individuals, cells, and loosely associated, often disparate groups, that act sometimes in concert, sometimes independently, and sometimes in the United States, but always in secret—and their mission is to destroy lives and to disrupt a way of life through terrorist acts. Terrorists work in the shadows; secrecy is essential to terrorists' success in plotting and executing attacks.

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

---

shall be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246.

Classified *Ex Parte, In Camera* Declaration of Adm. Michael S. Rogers, National Security Agency
Jewel v. Nat'l Security Agency, No. 4:08-cv-4373-JSW
17

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

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

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

[redacted]

34. **(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 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.

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

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

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

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

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

[redacted]

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

39. **(U)** It is against this backdrop that the risks of disclosing the information presented in this declaration in response to Plaintiffs' discovery requests, and contained in the documents responsive to Plaintiffs' requests for production being made available for the Court's *ex parte, in camera* review, should be assessed.

C. (U) The President's Surveillance Program and Its Transition to FISA-Based Authorization

40. **(U)** Starting on October 4, 2001, in response to the terrorist attacks of September 11, 2001, President Bush authorized the Secretary of Defense to employ the capabilities of the Department of Defense, including the NSA, to undertake three inter-related intelligence-gathering activities to enhance the United States' ability to detect and prevent acts of terrorism within the United States. This became known as the President's Surveillance Program ("PSP").

President Bush authorized the NSA to collect: (1) the contents[8] of certain international communications, a program that was later referred to as the Terrorist Surveillance Program, or "TSP"; (2) non-content telephony metadata in bulk, and (3) non-content Internet metadata in bulk, all subject to various conditions. Authorization of the PSP was intended to address an important gap in NSA's intelligence collection activities. Communications technology had undergone significant changes since the enactment of the Foreign Intelligence Surveillance Act ("FISA") in 1978, as a result of which by 2001 international communications to and from the United States were primarily carried by wire rather than radio transmission. Obtaining authority under FISA to conduct foreign-intelligence surveillance of wire-based communications in the United States presented great practical difficulties for the NSA. The President's authorization of the PSP resolved these difficulties and facilitated NSA surveillance directed at identifying foreign terrorist operatives who were communicating with individuals in the United States. President Bush re-authorized the PSP approximately every 30-60 days until its termination in January 2007.[9]

---

[8] **(U)** The term "content" is used herein to refer to the substance, meaning, or purport of a communication, as defined in 18 U.S.C. § 2510(8), as distinguished from the type of addressing or routing information referred to herein as "metadata."

[9] ~~**(TS//STLW//SI//OC/NF)**~~ [redacted]

Pages 23-25 – Redacted in their Entireties

[redacted][11]

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

47. **(U)** This state of affairs prompted the NSA to seek additional statutory authority under the FISA to intercept the content of international communications that transited facilities inside the United States. In August 2007, Congress enacted temporary legislation, the Protect America Act ("PAA"), Pub. L. 110-55, 121 Stat. 552 (previously codified at 50 U.S.C. §§ 1805A-1805C), which granted NSA additional flexibility under the FISA to target international communications carried in the United States without obtaining an individual court order for each selector, so long as the target was located outside the United States. This restored some of the operational flexibility needed to swiftly target rapidly changing selectors on multiple terrorist targets that existed under the PSP.

48. **(U)** In July 2008, following the expiration of the PAA, Congress enacted in its place 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

[11] ~~(TS//SI//OC/NF)~~ [redacted]

702"), which created new statutory authority permitting the electronic surveillance of non-United States persons reasonably believed to be outside of the United States without individual FISC orders. 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), (g).[12] The statute does not specify the technological means by which the acquisition is to be accomplished, except to specify that it may direct "the assistance of an electronic communication service provider." *Id.* § 1881a(g)(2)(A)(vi).

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

[12] **(U)** Four requirements 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. 50 U.S.C. § 1881a(g)(2)(A)(iv), (i)(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(i)(2)(B). Third, the FISC must find that the Government's minimization procedures meet FISA's requirements. *Id.* §§ 1801(h), 1821(4), 1881a(i)(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).

[redacted]

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

[redacted]

51. **(U)** The NSA used the telephony metadata produced under this program to create a historical repository of information, which was used to ascertain whether international terrorist organizations were communicating with operatives in the United States. Under the FISC's orders governing the program, upon a determination of reasonable, articulable suspicion that a selector, typically a telephone number, was associated with an international terrorist organization under investigation by the Federal Bureau of Investigation ("FBI"), NSA analysts were permitted

[13] **(U)** The Court's orders generally defined call detail records to include comprehensive communications routing information, including but not limited to session-identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity ("IMSI") number, International Mobile station Equipment Identity ("IMEI") number, etc.), trunk identifier, telephone calling card number, and time and duration of a call.

to use that selector to conduct queries (electronic searches) of the database to identify telephone numbers that had been in contact with the suspected-terrorist selector, as well as the wider circle of numbers in contact with those that had communicated directly with the selector. Although the NSA collected and maintained a large volume of call-detail records under the program, the requirement of reasonable, articulable suspicion barred indiscriminate querying of the data, and as a result the vast majority of the data obtained under the program were never reviewed by any person. Additionally, in accordance with minimization procedures[14] imposed by the FISC's orders, the NSA stored, analyzed, and disseminated foreign intelligence information gleaned from this data under carefully controlled circumstances, and under stringent supervision and oversight by the FISC as well as by Executive Branch authorities including the Department of Justice.

52. **(U)** The FISC re-authorized the program approximately every 90 days, on 43 separate occasions, until the passage of the USA FREEDOM Act of 2015, Pub. L. 114-23, 129 Stat. 268. Effective November 29, 2015, the USA FREEDOM Act explicitly prohibits the United States Government from collecting telephony metadata records in bulk under FISA. In accordance with the statutory ban the NSA discontinued its collection, querying, and analysis of bulk telephony metadata pursuant to Section 215. In lieu of bulk collection, the USA FREEDOM Act authorizes a new mechanism for targeted production by service providers of call-detail records associated with specific selectors, such as telephone numbers, approved by the FISC on the basis of a reasonable, articulable, suspicion that the selectors are associated with foreign powers (or agents of foreign powers) engaged in international terrorist activities. (The Government may also collect records associated with the numbers that have been in contact with

[14] **(U)** Minimization procedures, within the meaning of the FISA business records provision, are "specific procedures [adopted by the Attorney General] that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign-intelligence information." 50 U.S.C. § 181(g).

a suspected-terrorist selector.) The NSA may process, analyze, disseminate and retain telephony metadata records only in the manner permitted by minimization procedures adopted by the Attorney General in accordance with the USA FREEDOM Act and approved by the FISC.

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

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

[redacted]

D. (U) Plaintiffs' Allegations and the Government's Prior Assertions of Privilege

55. (U) In the course of my official duties, I have been advised of the *Jewel* litigation, and I have reviewed the allegations raised in this litigation, including the Complaint filed in the *Jewel* action on September 18, 2008. In sum, Plaintiffs allege that, after the 9/11 attacks, the NSA received presidential authorization to engage in "dragnet" communications surveillance in concert with major telecommunications companies. *See, e.g., Jewel* Compl. ¶¶ 2-3. Plaintiffs allege that, pursuant to presidential authorization and with the assistance of telecommunication companies (including AT&T and Verizon), the NSA indiscriminately intercepted the content and obtained the communications records of millions of ordinary Americans. I am aware the Plaintiffs also contend that their allegations encompass such collection activities even as they were later transitioned to FISC-authorized programs. Plaintiffs have stated that they no longer seek injunctive relief for alleged violations of their rights under the Constitution, but continue to

seek monetary relief for alleged violations of their rights under the Wiretap Act, 18 U.S.C. § 2510, *et seq.*, and the Stored Communications Act, 18 U.S.C. § 2701, *et seq.*

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

E. (U) Officially Disclosed Information Concerning the Challenged Programs

57. **(U)** In December 2005, then-President Bush publicly acknowledged the existence of the TSP, presidentially-authorized activity in which the NSA intercepted the content of international communications involving persons reasonably believed to be associated with al Qaeda and affiliated terrorist organizations. In the wake of unauthorized disclosures, beginning in June 2013, about other intelligence-gathering activities conducted by the NSA, the DNI, at the direction of then-President Obama, and in keeping with President Obama's transparency initiative, declassified and made public certain information about a number of sensitive programs undertaken by the NSA under the authority of the FISA. Certain of the information that the DNI has declassified concerns the allegations raised in this litigation, as discussed in great detail in the classified declarations referenced above. In addition, in December 2013 then-President Obama declassified the existence of the two metadata-collection programs conducted under the PSP. I summarize these various official disclosures below.

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

58. **(U)** The Government has publicly revealed certain information about its use of Section 702 of FISA to target certain non-U.S. persons reasonably believed to be located outside of the United States for the purpose of acquiring foreign intelligence information. As noted above, the Government's use of the authority provided by Section 702 is subject to FISC oversight. Section 702 may not be used to target U.S. persons or persons located inside the United States, and the Government may not use the statute to intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located inside the United States. Electronic communication service providers

may be compelled to supply all information, facilities, or assistance necessary to accomplish acquisitions conducted pursuant to Section 702.

59. **(U)** The Government has explained that 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 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 information to be collected, which must meet the statutory definition of foreign intelligence information, but do not identify the particular non-U.S. persons who will be targeted for collection. Instead, the certifications include targeting procedures approved by the Attorney General that 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 must determine 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. Once targeted surveillance under Section 702 has been authorized, the NSA takes the lead in designating relevant communications selectors, such as e-mail addresses, with which to target specific non-U.S. persons reasonably believed to be located outside the United States. The NSA's targeting procedures require that there be an appropriate, documented foreign intelligence purpose for the acquisition and that the selector be used by a non-U.S. person reasonably believed to be located outside the United States.

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

[redacted]

61. (U) Since June 2013, the Government has declassified and publicly released thousands of pages of materials pertaining to its Section 702 collection activities. Categories of documents that have been subject to public release (in redacted form) include, among other things, certain memorandum opinions and orders issued by the FISC authorizing or reauthorizing Section 702, and certain of the NSA's Section 702 targeting and minimization procedures.

62. (U) The Government has also publicly disclosed FISC orders and opinions concerning various failures to fully implement and comply with FISC-ordered procedures for the Section 702 program. Inquiries conducted by the NSA and the Department of Justice indicated that these compliance incidents occurred due to human error and technological issues. These releases, many of which contained important national security redactions, were intended to add to the public's understanding of changes made to Section 702 collection to ensure compliance

[15] ~~(S//NF)~~ [redacted]

[16] (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.

with FISC orders, statutory requirements, and to protect important privacy interests. For example, the Government has publicly released, in redacted form, successive copies of joint Attorney General-DNI semi-annual assessments of compliance with procedures and guidelines issued pursuant to Section 702 of the FISA. In July 2014, the Privacy and Civil Liberties Oversight Board, an independent Executive Branch agency established pursuant to statute, 42 U.S.C. § 2000ee, issued its report on the Government's implementation of Section 702.

63. **(U)** Most recently, in an opinion issued on April 26, 2017, the FISC approved amended certifications and NSA targeting and minimization procedures designed to restrict certain aspects of its Upstream Internet collection following the identification of issues of non-compliance with certain provisions of the NSA's Section 702 minimization procedures. Historically, the NSA had been authorized through its Upstream Internet collection to acquire not only communications "to" or "from" a targeted selector, but also communications "about" a Section 702 selector. An example of an "about" communication is an e-mail that includes a targeted e-mail address in the text or body of the e-mail, even though the e-mail is between two persons who are not themselves targets. In October 2016, the NSA notified the FISC of several inadvertent compliance incidents related to queries involving U.S. person information in 702 Upstream Internet collection. Internal NSA review indicated that human error was the primary cause of the compliance incidents; NSA systems design was also found to be a contributing factor. After a considerable evaluation of its Upstream program and available technology undertaken in response to these incidents, the NSA decided that its Upstream Internet surveillance activities would no longer collect any communications that are solely "about" a foreign intelligence target. Instead, this surveillance would now be limited to only those communications that are directly "to" or "from" a foreign intelligence target.

2. (U) Bulk Collection of Telephony Metadata Under FISA

64. **(U)** Shortly after the unauthorized disclosures that began in June 2013, the Government acknowledged the existence of the NSA's Section 215 bulk telephony metadata

program, which was still in operation at that time. The Government disclosed that, pursuant to dozens of FISC orders issued by multiple FISC judges, the NSA had been collecting and analyzing bulk telephony metadata from certain telecommunication service providers, to assist the Government in detecting communications of known or suspected terrorists operating outside of the United States who may have been communicating with others inside the U.S., as well as communications between operatives located within the U.S. It was explained that the NSA did not, under this program, collect, listen to, or record the content of any call, nor did it intentionally collect the name, address, or financial information of any subscriber, customer, or party to a call, or cell site locational information. The Government also explained that although the program was broad in scope and involved the collection and aggregation of a large volume of data from multiple telecommunications service providers, it never captured information on all (or virtually all) calls made and/or received in the U.S.

65. **(U)** The Government also revealed certain details about the process through which it obtained FISC orders, approximately every 90 days, re-authorizing this program. The Government submitted detailed applications from the FBI, explaining that the records were sought for investigations to protect against international terrorism that concerned specified foreign terrorist organizations identified in the application. As Section 215 required at that time, each application contained a statement of facts showing that there were reasonable grounds to believe that the metadata as a whole were relevant to the investigations of these organizations.

66. **(U)** The Government acknowledged that the NSA stored and analyzed this information, although under carefully controlled circumstances and under stringent supervision and oversight by all three branches of Government. It explained further that, due to the prohibition on queries of the data except those based on selectors reasonably suspected of association with foreign terrorist operatives, the vast majority of the accumulated metadata were never seen by any person. It was also made public that from May 2006 until February 2014, the determinations of reasonable, articulable suspicion were made by certain NSA officials, and

thereafter were made (until the program's termination) by the FISC. (Where the identifier was reasonably believed to be used by a U.S. person, determinations of reasonable, articulable suspicion could not be made based solely on activities protected by the First Amendment.)

67. **(U)** The Government also explained that the data made accessible to NSA analysts, even on the basis of authorized queries, were limited to communications records within three "hops" from the seed identifier (and, after February 2014, limited to just two "hops"). The query results could include only identifiers that had been in direct contact with the seed (the first "hop"), identifiers in direct contact with the first "hop" identifiers (the second "hop"), and identifiers in direct contact with second "hop" identifiers (the third "hop"). By querying the metadata in this fashion, NSA intelligence analysts were able to: (1) detect domestic identifiers calling foreign identifiers associated with a foreign terrorist organization and discover additional identifiers with which the foreign identifiers were in contact; (2) detect foreign identifiers associated with a foreign terrorist organizations calling into the U.S., and discover the domestic identifiers with which they were in contact; and (3) detect possible terrorist-related communications occurring between communicants located inside the United States. The Government has also publicly acknowledged, that in accordance with the mandate of the USA FREEDOM Act, the Section 215 bulk telephony metadata program was terminated in November 2015.

68. **(U)** Soon after it acknowledged the existence of the Section 215 telephony metadata program, the Government declassified and publicly disclosed a number of FISC "primary" orders and opinions authorizing the Government to carry out the program.[17] The Government did not disclose any of the so-called "secondary" orders issued by the FISC to individual telecommunications service providers directing them to produce call-detail records to the NSA in bulk. The Government, however, acknowledged the authenticity of the improperly and

[17] **(U)** Following the Government's declassification of the Section 215 bulk telephony metadata program in June 2013, the Government continued to process and release documents relating to this program.

unlawfully disclosed FISC secondary order issued on April 25, 2013, to Verizon Business Network Services, Inc. ("VBNS"). The VBNS order, which expired by its terms after approximately 90 days, on July 19, 2013, was (and remains) the only declassified FISC order identifying any particular provider that participated in the Section 215 telephony metadata program. Since the disclosure of this order in June 2013, the United States has continued to protect against any further disclosures of FISC orders directed at any provider under the program. While the authentication of that order means that the identity of one participating provider was officially acknowledged for the time period covered by that order, the order was limited to VBNS, did not identify any other provider, and did not relate to any other corporate component of Verizon Communications other than VBNS. The Government has neither confirmed nor denied whether VBNS participated in the Section 215 telephony metadata program either before or after the period covered by the April 2013 order, or whether VBNS participates in any other NSA intelligence program. The identities of the providers that furnished assistance to the NSA under the Section 215 bulk telephony metadata program, including VBNS, as to any time period other than the approximately 90-day duration of that order, have not been disclosed and remain currently and properly classified.

69. **(U)** The Government has also disclosed compliance incidents involving the bulk telephony metadata collection program. As with the Section 702 program, these compliance incidents were the product of human error and technological issues. In 2009, the Government reported these problems to the FISC (and Congress) and remedied them, and the FISC (after temporarily suspending the Government's authority to query the database without the court's approval) continued to authorize the program.

3. (U) Bulk Collection of Internet Metadata Under FISA

70. **(U)** In November 2013, the Government also declassified and acknowledged the existence of FISC-authorized bulk collection of Internet metadata, carried out under FISA's PR/TT provision, for the purpose of obtaining foreign-intelligence information.[18] The Government explained that certain (unidentified) telecommunications service providers were compelled by FISC order to provide this information, that the data collected included certain dialing, routing, addressing, and signaling information such as the "to" and "from" lines of an e-mail and the date and time the e-mail was sent, but not the content of an e-mail or the subject line. The Government also disclosed that the NSA acquired, stored, accessed, and analyzed the accumulated bulk Internet metadata (in similar fashion to the bulk telephony metadata collected under Section 215), subject to FISC orders requiring compliance with minimization procedures limiting access to, retention, and dissemination of the metadata. The Government also acknowledged that the program operated on a large scale (but without specifying its scope or the identities of any participating providers); that the program had been terminated in December 2011; and that bulk Internet metadata collected under the program had been destroyed.

71. **(U)** As it did with the Section 702 and Section 215 programs, the Government also publicly disclosed FISC orders and opinions concerning various unintended failures to fully implement and comply with FISC-ordered minimization procedures applicable to the bulk Internet metadata collection program. In 2004 and 2009, the Government reported these problems to the FISC (and Congress) and remedied them, after which the FISC continued to re-authorize the program until the Government decided to terminate it.

---

[18] **(U)** Following the November 2013 declassification decision, the U.S. Government on several occasions publicly released additional documents relating to the bulk PR/TT program.

4. (U) Presidentially Authorized NSA Activities After 9/11

72. **(U)** In light of former-President Bush's December 2005 acknowledgment concerning the existence of the TSP, and the declassification decisions discussed above concerning the NSA's targeted content collection under Section 702 and its bulk collection of telephony and Internet metadata under FISA, former-President Obama in December 2013 publicly disclosed the existence of the metadata-collection activities previously conducted pursuant to presidential authorization. Accordingly, certain limited information concerning these activities has now been declassified. In furtherance of this declassification, and in response to requests made under the Freedom of Information Act, the U.S. Government released several partially redacted Inspectors General reports, originally completed in 2009, detailing the PSP.

73. **(U)** The publicly available documents reveal that starting on October 4, 2001, former-President Bush, in order to detect and prevent further acts of international terrorism within the United States, authorized the NSA to collect the contents of international communications reasonably believed to involve agents of al Qaeda or its affiliates, to collect telephony metadata in bulk, and to collect Internet metadata in bulk, as discussed above. It has been made public that former-President Bush re-authorized these activities every 30-60 days (until transitioned to FISC authorization under FISA), and that each presidential authorization required the minimization of information concerning American citizens to the extent consistent with the effective accomplishment of the mission of detection and prevention of acts of terrorism within the United States. The public record also reflects that the NSA applied additional internal constraints on the presidentially-authorized activities, to protect the privacy interests of U.S. persons. It is also now a matter of public record that the collection of communications content pursuant to presidential authorization ended in January 2007, when the Government transitioned authorization of this activity to FISA; that presidentially authorized bulk collection of telephony metadata transitioned to FISC authorization under Section 215 in May 2006; and that

presidentially authorized bulk collection of Internet metadata transitioned to FISC authorization under FISA's PR/TT provision in July 2004.

74. **(U)** Notwithstanding the Government's extensive public disclosures of the NSA's intelligence-gathering activities conducted under the PSP and pursuant to FISA, the Government has continued to withhold information about the specific sources and methods and operational details related to these programs, including the identities of targets and subjects of surveillance, the identities of persons about whose communications the NSA has obtained metadata, and the identities of telecommunications service providers that have assisted the NSA in Upstream collection. These sources and methods and operational details remain properly classified, and are the subject of the PDDNI's privilege assertions, in her capacity as Acting DNI, and my own assertion of NSA's statutory privilege.

V. (U) INFORMATION REGARDING PLAINTIFFS' STANDING

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

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

[redacted]

76. **(U)** Each of these categories of information is addressed in the subsections below, with cross-references, for the Court's convenience, to the specific Interrogatories and Requests for Admission to which the information provided pertains. These responses are based on the results of queries of communications data using identifiers provided by the Plaintiffs. These queries were conducted on available documentation concerning the challenged NSA intelligence-gathering activities, which were located after an extensive search, and on the current recollection of individuals involved in the operation of these programs at various times since 2001 who remain employed by the NSA. Thus, although the following description of the NSA's programs is as complete and accurate as possible under the circumstances, it is based on non-comprehensive records and imperfect human memories. Consequently, as will be seen below, the level of detail available about the scope and operation of these programs varies over time and from program to program. In each case, however, the Government Defendants have responded to Plaintiffs' requests to the best of their ability, with the information that can be gleaned from the available sources.

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

[redacted]

A. (U) Whether the Content of Plaintiffs' Communications Has Been Collected Under the PSP or Upstream

[Request for Admission Nos. 1-5, 23-27; Interrogatory Nos. 1-3, 18-20]

78. **(U)** In brief, Plaintiffs' Request for Admission Nos. 1-5 and 23-27, and Interrogatory Nos. 1-3 and 18-20, ask the Government Defendants to state whether communications of Plaintiffs have been "interacted with," "copied," "filtered," or "scanned" in connection with PSP content or Upstream collection.

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

[redacted]

83. ~~(U//FOUO)~~ Fourth, with regard to the NSA's PSP content collection, the Court is already aware, from the declarations of Dr. Mark C[redacted] (the Chief of the Office of Compliance for Capabilities within the NSA's Engagement and Policy Directorate) and Elizabeth B[redacted] (Deputy Director of Capabilities), that the NSA discovered a few months ago that PSP Internet content data that had been stored for purposes of this litigation on magnetic tapes were deleted in whole or in part at one or more points of time prior to 2017. The NSA thereafter began a significant technical effort to recover as much of the lost data as possible so that it could be searched. That effort is ongoing, and the NSA will update the Court regarding this project periodically.

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

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

[19] ~~(S//NF)~~ [redacted]

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

[20] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

[redacted]

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

88. **(U)** In accordance with the terms of the President's authorization under which the PSP operated, the content collection process was designed to facilitate the interception of one-end-foreign communications to or from persons known or reasonably believed by the U.S. intelligence community (based on a range of information, including sensitive foreign intelligence derived from a variety of sources) to be members or agents of al Qaeda or affiliated foreign terrorist organizations.

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

Pages 49-67 – Redacted in their Entireties

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

[redacted]

131. **(U)** Last year, after a comprehensive review of NSA's mission needs, its current technological constraints, U.S. person privacy interests, and certain difficulties in implementation, the NSA decided to cease certain activities conducted as part of its Upstream Internet acquisition process. Specifically, after considerable evaluation of the program and available technology, the NSA decided that its Upstream surveillance activities would no longer include any Internet communications that are solely "about" a foreign-intelligence target, and instead would be limited to surveillance of communications that are directly to or from a target. These changes, which were approved by the FISC and implemented in April 2017, were designed to retain the elements of Upstream collection that currently provide the greatest value to national security while reducing the likelihood that the NSA will acquire communications of U.S. persons or others who are not in direct contact with one of the NSA's foreign-intelligence targets.

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

[redacted]

133. **(U)** In 2011, the FISC expressed concern that the NSA's acquisition of MCTs resulted in the collection of a substantial number of wholly domestic communications of U.S. persons (and other persons located in the United States) having no relationship to a foreign-intelligence target. For example, if an MCT contained only a single e-mail containing a reference to a targeted selector, the NSA's acquisition devices would collect all of the e-mails contained in the transaction, regardless of the fact that none of the other e-mails contained in the transaction concerned the target of the NSA's surveillance. To address the FISC's concerns the Government prepared a revised set of NSA minimization procedures that included special segregation, marking, and handling requirements for MCTs, a reduced default retention period for Upstream communications, and a categorical prohibition on the use of known U.S.-person identifiers to query the result of Upstream Internet collection. The FISC concluded that these amended minimization procedures substantially reduced the risk that U.S.-person information unrelated to the NSA's foreign-intelligence targets would be used or disseminated by the Agency, and accordingly permitted Upstream collection to continue under the revised procedures.

134. **(U)** In late 2016, however, the NSA notified the FISC, that as a result of human error and in part because of NSA systems design, NSA analysts had since 2011 conducted U.S.-person queries of repositories containing Upstream Internet communications, notwithstanding the prohibition against doing so contained in the Agency's Section 702 minimization procedures. To resolve these compliance problems, in March 2017 the Government submitted to the FISC a set of amended Section 702 certifications and revised NSA targeting and minimization procedures that substantially change how the NSA conducts certain aspects of its Upstream Internet acquisition. In particular, the revised procedures, approved by the FISC on April 26,

2017, prohibited the acquisition of about communications altogether, and limited Upstream Internet collection only to Internet communications that are to or from Section 702 targets, in order to avoid the acquisition of potentially problematic MCTs.

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

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

Pages 71-73 – Redacted in their Entireties

[redacted]

142. **(U)** To the extent the Plaintiffs believed that the NSA's purpose in conducting surveillance on the Internet backbone is to acquire an ability to conduct the kind of dragnet surveillance of all or substantially all of Americans' online communications alleged in their Complaint, that was not the NSA's objective, nor has it ever achieved or attempted to achieve that level of surveillance, or anything approaching it, under the PSP or Section 702.

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

143. **(U)** In a series of related inquiries, Plaintiffs ask the Government Defendants to describe the extent to which communications scanned for selectors during the PSP content or Upstream collection process has "encompassed the totality of the international e-mails sent or received in the United States," Interrogatory Nos. 16, 33, and to admit to a series of propositions regarding interactions with "all" communications in transmission over "selected Internet facilities" where PSP content and Upstream collection have occurred. Request for Admission Nos. 6-9, 28-31.

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

Pages 75-104 – Redacted in their Entireties

[redacted]

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

[redacted]

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

[redacted]

[redacted]

219. **(U)** Plaintiffs ask the Government Defendants to state whether the NSA obtained bulk telephony or Internet metadata associated with Plaintiffs' communications under the PSP, or authority of FISA. In response to these requests—as in response to Plaintiffs' similar requests regarding alleged "interaction" with their communications under PSP content and Upstream collection, *see* Section V.A, above—the NSA has conducted, or will conduct, appropriate searches of relevant data, as set forth below. The

results of such searches are the most direct evidence available of whether metadata associated with Plaintiffs' communications were collected.

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

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

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

Pages 107-108 – Redacted in their Entireties

[redacted]

227. **(U)** Finally, the NSA cannot perform searches of metadata collected under the NSA's bulk Internet metadata program, as authorized by the FISC pursuant to the FISA's pen register and trap and trace authority (the PR/TT program). This is so because, as the NSA has previously explained, *see* § IV.D, above, those data were destroyed in December 2011 upon termination of the PR/TT program.

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

228. **(U)** This section of the declaration responds to Plaintiffs' discovery requests concerning the scope, sources and methods, and operational details of the NSA's bulk collection of telephony and Internet metadata, as authorized under the PSP and, thereafter, FISC orders issued pursuant to FISA.

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

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

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

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

[redacted]

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

[redacted]

[redacted][35]

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

[redacted]

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

[redacted]

[34] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

[35] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

Pages 111-147 – Redacted in their Entireties

[redacted]

293. **(U)** [redacted].

H. (U) Requests To Admit Authenticity of Certain Documents

[Request for Admission Nos. 50-63]

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

295. **(U) The Alleged OIG Working Draft.** Plaintiffs' Request for Admission Nos. 50-52 all concern a document entitled "ST-09-0002 Working Draft" and dated March 24, 2009. As stated in Plaintiffs' Request for Admission No. 50, the document is attached as Exhibit A to the Declaration of Richard R. Wiebe, ECF No. 147, filed in this case on July 2, 2013. Plaintiffs request that the Government Defendants admit that this document is "genuine," that it was written by NSA "employees on matters within the scope of their employment during the course of their employment," and that the NSA employees making the statements in the report were authorized by the NSA to do so.

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

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

298. **(U) Alleged AT&T Documents**. Plaintiffs' Request for Admission Nos. 53-60 ask similar questions about three purported AT&T documents attached as exhibits to the Declaration of Mark Klein, ECF No. 84, filed in this case on July 2, 2012. Namely, Plaintiffs ask the Government Defendants to admit that all three documents are "genuine," that they were made by AT&T employees on matters within the scope of their employment during that employment, and

that they were made by AT&T representatives while those representatives were serving as agents for the Government Defendants.

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

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

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

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

[redacted]

303. **(U) Alleged "Fairview" Documents.** Finally, Plaintiffs' Request for Admission Nos. 62-63 concern two documents entitled "Fairview Dataflow Diagrams" and "Fairview at a Glance," attached as Exhibits A and B to their requests. Plaintiffs ask the Government Defendants to admit that these document are "genuine," and that they "accurately depict[] surveillance configurations used to conduct Internet surveillance at AT&T Internet facilities within the United States."

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

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

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

[redacted][90]

I. (U) Classified Response to Plaintiffs' Requests for Production

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

(U) Request Nos. 1-5, 25-29: Evidence of "Interaction" with Plaintiffs' Communications

308. (U) Plaintiffs' Request for Production Nos. 1-5 and 25-29 respectively seek documents showing that Plaintiffs' communications were "interacted with" as part of PSP content or Upstream collection. Request Nos. 1 and 25 seek any Internet communications of Plaintiffs that the NSA collected under the PSP or Upstream. Request No. 2-5 and 26-29 seek

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

any documents "evidencing or relating to" any "interaction," "copying," "filtering," or "scanning" of the content of Plaintiffs' Internet communications under PSP or Upstream.

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

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

(U) Request Nos. 6-10, 30-34: PSP Content and Upstream Collection Processes

311. **(U)** Plaintiffs' Request Nos. 6-10 and 30-34 respectively seek documents "sufficient to show" the process by which the NSA has collected communications content under the PSP and Upstream. Operational details about PSP and Upstream content collection are described above in section V.B. Additionally, documents sufficient to show the nature of the collection process are included in the materials being made available to the Court for *in camera*, *ex parte* review.

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

Pages 154-155 – Redacted in their Entireties

[redacted]

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

[redacted]

(U) Request Nos. 49-50, 52: Evidence of Metadata Collection from Plaintiffs' Communications

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

[redacted]

319. **(U)** As discussed above, the NSA is currently in the process of conducting searches of bulk telephony metadata obtained pursuant to Section 215 of the USA Patriot Act. The

Government will report the results of these searches to the Court on or before April 1, 2018, and provide any responsive "hits" generated by these searches for the Court's *ex parte, in camera* review on that date.

~~(TS//STLW//SI//OC/NF)~~ [redacted]

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

[redacted]

(U) Request Nos. 53-56: Extent of Metadata Collection from "Copied" and "Scanned" Communications

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

[redacted]

[redacted]

(U) Request No. 57: Graphics Depicting PSP, Upstream, or Bulk Metadata Collection

322. (U) Finally, Plaintiffs' Request for Production No. 57 seeks "[a]ny graphics depicting the PSP, Upstream surveillance, bulk collection of Internet metadata, or bulk collection of telephone records." The Government Defendants have identified a number of documents responsive to this request, but many are duplicative and to produce them all would be cumulative. Therefore, the Government Defendants propose to make available to the Court a representative subset of the responsive documents sufficient to depict the content and bulk metadata collection processes at issue.

VI. (U) INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE

323. (U) As discussed above, the Government has officially declassified and disclosed certain information about the existence and nature of the NSA intelligence programs that Plaintiffs seek to contest. However, the information set forth in this declaration in response to Plaintiffs' discovery requests; contained in the documents responsive to Plaintiffs' requests for production being made available for the Court's *ex parte, in camera,* review; and that may later be provided to the Court in response to Plaintiffs' requests, remains properly classified and is subject to the PDDNI's state secrets privilege assertion, in her capacity as Acting DNI, and my own assertion of NSA's statutory privilege in this declaration. This information includes the identities of persons whose communications were subject to the challenged intelligence activities, specific operational details concerning the programs' scope and operation, the sources

and methods they utilized, and the identities of the U.S. telecommunications service providers that assisted the NSA in carrying out these programs. In general and unclassified terms, the PDDNI's assertion of the state secrets privilege, as Acting DNI, and my statutory privilege assertion encompasses the following categories of still-classified information and properly protected national security information concerning NSA activities:

A. **(U) Persons Subject to Intelligence Activities**: information contained in this classified declaration in response to Plaintiffs' discovery requests, in the additional documents responsive to Plaintiffs' requests for production being made available for the Court's *ex parte, in camera* review, and that may later be provided to the Court in response to Plaintiffs' requests, that would tend to confirm or deny whether particular individuals, including the named Plaintiffs, have been subject to any NSA intelligence activities;

B. **(U) Operational Information Concerning NSA Intelligence Activities**: information contained in this classified declaration in response to Plaintiffs' discovery requests, in the additional documents responsive to Plaintiffs' requests for production being made available for the Court's *ex parte, in camera* review, and that may later be provided to the Court in response to Plaintiffs' requests, concerning the scope and operational details of NSA intelligence activities, including:

(1) **(U)** *Communications Content Collection:* information concerning the scope or operational details of NSA intelligence activities related to the collection of Internet communications content under the PSP, transitional FISA authority, or FISA Section 702;

(2) **(U)** *Communications Metadata Collection:* information concerning the scope or operational details of NSA intelligence activities relating to the bulk collection of telephone and Internet non-content communications metadata under the PSP, or authority of FISA;

and

C. **(U) Telecommunication Provider Identities**: information contained in this classified declaration in response to Plaintiffs' discovery requests, in the additional documents responsive to Plaintiffs' requests for production being made available for the Court's *ex parte, in camera* review, and that may later be provided to the Court in response to Plaintiffs' requests, that would tend to confirm or deny whether AT&T, Verizon, Sprint, or any other telecommunications carrier has provided assistance to the NSA in connection with any intelligence activity, including the activities at issue in this litigation.

VII. (U) HARM OF DISCLOSURE OF PRIVILEGED INFORMATION

A. **(U) Information Concerning Whether Plaintiffs Have Been Subject to the**

Alleged NSA Activities

324. **(U)** The first major category of information as to which I am supporting the PDDNI's assertion of privilege, as Acting DNI, and asserting the NSA's own statutory privilege, concerns information contained in section V of this declaration, in the additional documents being made available to this Court for its *ex parte, in camera* review, and that may later be provided to the Court in response to Plaintiffs' discovery requests, indicating whether the named Plaintiffs have been subject to the NSA intelligence activities at issue in this lawsuit. The Plaintiffs allege that the contents of their own Internet communications have been and continue to be subject to the processes involved in the NSA's backbone collection of Internet content under the PSP, and Section 702. Further, Plaintiffs allege that the NSA has collected telephony and Internet metadata about their communications, under the PSP and FISA authorization, in connection with the NSA bulk collection programs. As set forth below, confirmation or denial of such information by the NSA reasonably could be expected to cause exceptionally grave damage to the national security.

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

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

[redacted]

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

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

[redacted]

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

[redacted]

[redacted]

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

[redacted]

3. (U) Harm of Disclosing Whether Plaintiffs Were Subject to NSA Activities

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

[redacted]

[redacted]

330. **(U)** As a matter of course, the NSA cannot publicly confirm or deny whether any individual is or has 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 who are the actual targets or subjects of foreign-intelligence gathering is relatively straightforward. If an individual knows or suspects he is a target or subject of U.S. intelligence activities, he would naturally tend to alter his behavior to take new precautions against such scrutiny. In addition, revealing who is not a target or the subject of intelligence gathering would indicate who has avoided surveillance or collection, and which channels of communication may be secure. Such information could allow an actual or potential adversary, secure in the knowledge that he is 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 a person may be unwittingly utilized or even forced by foreign adversaries to convey information through a secure channel. 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.

331. **(U)** Similar harms would result from confirming or denying whether particular persons' communications 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 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 a situation involving an actual target or subject, an actual or potential adversary of the United States could then easily deduce that the person in the latter instance is or has been a target of or subject to surveillance or other intelligence-gathering activity. In addition, disclosure of whether a person's communications have or have not been

targeted, or intercepted through the targeting of a third party, would reveal whether a particular channel of communication is secure, and also reveal to third-party targets whether their own communications may be secure. Moreover, each occasion that the Government confirms (even if compelled to confirm) that a person has or has not been a subject of surveillance makes it more difficult in the future to withhold information about the surveillance status of other individuals. This could potentially result in a cascading effect of uncontrolled disclosures.

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

333. **(U)** For all of these reasons, the NSA cannot disclose whether the Plaintiffs' communications have been subject to NSA intelligence collection activities without causing exceptionally grave damage to national security.

B. (U) Operational Information Concerning NSA Intelligence Activities

334. **(U)** I am also supporting the PDDNI's assertion of privilege, as Acting DNI, and asserting the NSA's statutory privilege over still-classified facts concerning NSA intelligence activities, sources, or methods that are discussed in section V of this declaration, in documents being made available to the Court for its *ex parte, in camera* review, and that may later be provided to the Court in response to Plaintiffs' discovery requests. This includes extraordinarily detailed information concerning the technical operations, locations, scope and targeting of the

challenged communications content and bulk metadata collection activities, as well as the identities of the providers who have assisted the NSA in conducting those activities, some of which are currently conducted under FISA Section 702 and other authorities. As set forth below, the disclosure of such information would cause exceptionally grave harm to national security.

1. (U) Information Concerning NSA Content Collection Activities

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

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

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

Pages 166-170 – Redacted in their Entireties

[redacted]

2. (U) Information Concerning NSA Bulk Collection of Metadata

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

a. (U) Bulk Collection of Internet Metadata

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

Pages 172-176 – Redacted in their Entireties

b. (U) Bulk Collection of Telephony Metadata

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

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

[redacted]

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

[redacted]

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

[redacted]

[redacted]

C. (U) Harm from Revealing Whether Specific Carriers Have Provided Assistance

361. ~~(TS//STLW//SI-[redacted]//OC/NF)~~ [redacted]

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

Pages 180-188 – Redacted in their Entireties

[redacted]

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

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

380. **(U)** As set forth above, in June 2013 the media reported the unauthorized disclosure of an April 25, 2013, FISC order, issued under the Section 215 bulk telephony metadata program, directing a particular Verizon Communications subsidiary, Verizon Business Network Services ("VBNS"), to provide call-detail records to the NSA, in bulk, for a period of approximately 90 days. Shortly thereafter the DNI officially declassified and acknowledged the authenticity of this order to address significant public interest—and correct public misimpressions—concerning this U.S. intelligence activity. As also noted above, this is the only FISC order identifying any participating provider in an NSA intelligence activity that has been declassified, and, since its disclosure in June 2013, the U.S. Government has not confirmed or

denied the past or current participation of any specific provider in any NSA intelligence program, apart from the participation of VBNS in the telephony metadata program for the 90-day duration of the now-expired April 25, 2013, FISC Order. Whether or not, or to what extent, a particular telecommunications provider has assisted the NSA in conducting its foreign-intelligence mission remains an extraordinarily sensitive and significant matter that the Government continues to protect, to avoid even greater harm to national security than has already occurred since June 2013.

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

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

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

[redacted]

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

[redacted]

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

[redacted]

~~TOP SECRET//STLW//SI-[redacted]//ORCON/NOFORN~~

[redacted]

VIII. (U) CONCLUSION

385. **(U)** Set forth in this declaration are the Government Defendants' responses to Plaintiffs' interrogatories and requests for admission on the issue of standing. Additional documents responsive to Plaintiffs' requests for production on the standing issue are also being made available for the Court's *ex parte, in camera* review. The Government Defendants have responded to the best of their ability to Plaintiffs' requests, and to the Court's order to "marshal all evidence" on the standing issue, based on currently available documents and data, and the recollections of current NSA employees involved in the challenged intelligence-gathering programs. The information contained in this declaration, in the accompanying documents, in the forthcoming results of ongoing database searches, and that might later be provided to the Court in response to Plaintiffs' discovery requests, is classified, and extraordinarily sensitive. Its disclosure would cause exceptionally grave damage to the national security of the United States. For the reasons explained above, I support the assertion by the PDDNI, in her capacity as Acting DNI, of the state secrets privilege over this information, and of the statutory privilege under 50 U.S.C. § 3024(i)(1), and I assert the NSA's privilege under section 6 of the National Security Agency Act, 50 U.S.C. § 3605(a).

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

Executed on February 16, 2018

ADM. MICHAEL S. ROGERS, DIRECTOR,
NATIONAL SECURITY AGENCY

CERTIFICATE OF SERVICE

I hereby certify that on December 6, 2019, I electronically filed the foregoing Supplemental Excerpt of Record with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. Participants in the case are registered CM/ECF users, and service will be accomplished by the appellate CM/ECF system.

JOSEPH H. HUNT
Assistant Attorney General
DAVID L. ANDERSON
United States Attorney
H. THOMAS BYRON III
s/ Joseph F. Busa
JOSEPH F. BUSA
Attorneys, Appellate Staff
Civil Division, Room 7537
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 305-1754
Joseph.F.Busa@usdoj.gov