~~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

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.

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

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

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

[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]

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]