STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
BRYAN DEARINGER
RODNEY PATTON
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-2205
Fax: (202) 616-8470
Attorneys for the United States and Government Defendants Sued in their Official Capacities

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CAROLYN JEWEL, *et al.* Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.* Defendants.	Case No. 08-cv-4373-JSW
VIRGINIA SHUBERT, *et al.* Plaintiffs, v. BARACK OBAMA, *et al.* Defendants.	Case No. 07-cv-693-JSW **CLASSIFIED DECLARATION OF FRANCES J. FLEISCH, NATIONAL SECURITY AGENCY EX PARTE, IN CAMERA SUBMISSION** No Hearing Scheduled Courtroom 11, 19th Floor Judge Jeffrey S. White

(U) Table of Contents

		Page
I.	(U) INTRODUCTION	4
II.	(U) CLASSIFICATION OF DECLARATION	5
III.	(U) SUMMARY	8
IV.	(U) BACKGROUND	12
	A. (U) The National Security Agency	12
	B. (U) September 11, 2001, and the al Qaeda Threat	15
	C. (U) Plaintiffs' Allegations and the Government's Prior Assertions of Privilege	19
	D. (U) Official Disclosures Since September 2012	20
	1. (U) Collection of Bulk Telephony Metadata Under Section 215 of the FISA	21
	2. (U) Bulk Collection of Internet Metadata	24
	3. (U) Collection of Communications Content Pursuant to Section 702 of FISA	24
	4. (U) Presidentially Authorized NSA Activities After 9/11	26
V.	(U) INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE	28
VI.	(U) HARM OF DISCLOSURE OF PRIVILEGED INFORMATION	29
	A. (U) Information Concerning Whether Plaintiffs Have Been Subject to the Alleged NSA Activities	29
	1. ~~(TS//SI//NF)~~ [redacted]	30
	2. ~~(TS//SI//NF)~~ [redacted]	31
	3. (U) Harm of Disclosing Whether Plaintiffs Were Subject to NSA Activities	32
	B. (U) Operational Information Concerning NSA Intelligence Activities	35
	1. (U) Information Concerning Plaintiffs' Content Surveillance Allegations	36

2. **(U)** Information Concerning Plaintiffs' Communications Records Collection Allegations 47

(a) **(U)** Collection of Bulk Telephony Metadata 47

(b) **(U)** Internet Metadata Collection 53

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

1. ~~(TS//SI//NF)~~ [redacted] 64

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

(a) ~~(TS//SI [redacted] OC/NF)~~ [redacted] 69

(b) ~~(TS//SI [redacted] OC/NF)~~ [redacted] 74

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

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

VII. **(U)** CONCLUSION 84

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

CLASSIFIED DECLARATION OF FRANCES J. FLEISCH
NATIONAL SECURITY AGENCY

(U) I, Frances J. Fleisch, do hereby state and declare as follows:

I. (U) INTRODUCTION

1. **(U)** I am the Acting Deputy Director for the National Security Agency ("NSA" or "Agency"), an intelligence agency within the Department of Defense. I have held this position since December 9, 2013. Prior to holding the position of Acting Deputy Director, I was the Agency's Executive Director from June 2010 to December 8, 2013. Before moving into the Executive Director position, I served in a number of leadership and management positions since joining the agency in 1980. As Acting Deputy Director, I serve as the senior civilian leader of the NSA and act as the Agency's chief operating officer, responsible for guiding and directing strategies, operations, and policy. Under our internal regulations, and in the absence of the Director of the NSA, I am responsible for directing the NSA, overseeing the operations undertaken to carry out its mission and, by specific charge of the President and the Director of National Intelligence, protecting NSA activities and intelligence sources and methods. I have been designated an original TOP SECRET classification authority under Executive Order ("EO") No. 13526, 75 Fed. Reg. 707 (2009), and Department of Defense Manual No. 5200.1, Vol. 1, Information and Security Program (Feb. 24, 2012).

2. **(U)** The purpose of this declaration is to support an assertion of the military and state secrets privilege (hereafter, "state secrets privilege") by the Director of National Intelligence ("DNI") as the head of the Intelligence Community, as well as the DNI's assertion of a statutory privilege under the National Security Act, to protect information related to the NSA activities described herein below. 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.*) ("NSA Act"), to protect the information related to the NSA activities described herein below. General Keith B. Alexander, the Director of the NSA, has been sued in his official and individual capacities in the above-captioned litigation and has recused himself from the decision on whether to assert privilege in his official capacity. As the Acting Deputy Director, and by specific delegation of the Director, I am authorized to review the materials associated with this litigation, prepare whatever declarations I determine are appropriate, and determine whether to assert the NSA's statutory privilege. The statements made herein are based on my personal knowledge of NSA activities and operations, and on information made available to me as the Acting Deputy Director of the NSA.

II. (U) CLASSIFICATION OF DECLARATION

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

this purpose, the letters "U," "C," "S," and "TS" indicate respectively that the information is either UNCLASSIFIED, or is classified CONFIDENTIAL, SECRET, or TOP SECRET.[1]

4. **(U)** Additionally, this declaration contains Sensitive Compartmented Information ("SCI"), which is "information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods." 28 C.F.R. § 17.18(a). Because of the exceptional sensitivity and vulnerability of such information, these safeguards and access requirements exceed the access standards that are normally required for information of the same classification level. Specifically, this declaration references communications intelligence ("COMINT"), also referred to as special intelligence ("SI"), which is a subcategory of SCI. COMINT or SI identifies SCI that was derived from exploiting cryptographic systems or other protected sources by applying methods or techniques, or from foreign communications.

5. ~~**(TS//SI//OC/NF)**~~ This declaration also contains information related to or derived from the STELLARWIND program, a controlled access signals intelligence program under Presidential authorization created in response to the attacks of September 11, 2001. In this declaration, information pertaining to the STELLARWIND program is denoted with the special marking "STLW" and requires more restrictive handling. Despite the December 2005 public

[1] ~~**(TS//SI//OC/NF)**~~ In prior declarations and briefing materials, the NSA has used the "TSP" designation to refer to the portion of the program that was publicly disclosed by then-President Bush in December 2005. [redacted]

acknowledgement of the Terrorist Surveillance Program ("TSP"), and the recent public acknowledgment by the U.S. Government of NSA telephony and Internet metadata collection activities that were also part of the STELLARWIND program, certain details about the STELLARWIND program (including the TSP) remain highly classified and strictly compartmented. [redacted][2]

6. **(U//~~FOUO~~)** Finally, the "ORCON" designator means that the originator of the information controls to whom it is released. In addition to the fact that classified information contained herein may not be revealed to any person without authorization pursuant to Executive Order 13526, this declaration contains 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."

[2] **(U)** [redacted]

III. (U) SUMMARY

7. (U) Plaintiffs in this litigation allege that, following the terrorist attacks of September 11, 2001, the NSA, pursuant to presidential authorization and with the assistance of plaintiffs' telecommunications companies (namely, AT&T and Verizon), indiscriminately intercepted the content and obtained the communications records of millions of ordinary Americans as part of an alleged "dragnet" communications surveillance. The Government has previously asserted the state secrets privilege in these cases, most recently in September 2012, to protect from disclosure highly sensitive intelligence-gathering information relevant to confirming or negating plaintiffs' allegations. This declaration responds to the Court's order that the Government explain the impact of recent official disclosures about NSA intelligence-gathering activities on the national security issues in the litigation, as reflected in its state secrets privilege assertion. July 23, 2013 Amended Order (ECF No. 153 at 25); Sept. 27, 2013 Transcript of Proceedings at 7.[3]

8. (U) The Government's recent official disclosures follow a series of unprecedented, unauthorized, and unlawful disclosures, by a former NSA contractor, of Top Secret documents concerning certain classified NSA surveillance programs. The media revealed those unauthorized disclosures beginning in June 2013. These disclosures are now risking, and in some cases causing, the exceptionally grave damage to national security that the Government has previously identified to the Court, including the loss of valuable intelligence and,

[3] (U) This declaration supplants all prior privilege assertions. In order to focus on the information which remains subject to this privilege assertion, this declaration does not repeat or address all topics that were addressed in prior declarations. The Court is respectfully referred to prior declarations for additional background.

specifically, information that may assist in detecting or preventing a future mass casualty terrorist attack.

9. **(U)** The Government responded to the recent unlawful disclosures by officially acknowledging the existence of certain programs because of the importance of correcting inaccurate information to the public about those programs, despite the harm to national security that such an official acknowledgement would cause. In sum, the Government confirmed the existence and some information concerning (1) the telephony metadata program, in which the NSA obtains, pursuant to orders issued by the Foreign Intelligence Surveillance Court ("FISC"), telephone company business records in bulk containing certain non-content information about phone calls made, such as the phone numbers dialed, and the date, time, and duration of the calls, and uses that information to identify unknown terrorist operatives; (2) a previous program of bulk collection of certain Internet metadata, such as the "to" and "from" lines of an email and the date and time the email was sent, also authorized by the FISC and also for counter-terrorism purposes; and (3) certain information about the Government's use of authority conferred by Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), to collect, for foreign intelligence purposes, certain communications of non-U.S. persons located outside the United States, pursuant to approval of the FISC.

10. **(U)** In addition, the Government has now declassified the existence of the two metadata collection activities that were conducted prior to FISC authorization, under presidential authorizations issued by President Bush in the wake of the September 11 attacks. But for many reasons vital to national security, the classified sources and methods (many of which the NSA continues to utilize today), intelligence gathered, and operational details of what has been called the President's Surveillance Program ("PSP") must remain protected from public disclosure to

avoid even greater damage to national security than is already occurring as a result of the unlawful disclosures. To the extent this information is at risk of disclosure in litigating plaintiffs' claims, the Government continues to assert the state secrets privilege and applicable statutory privileges over that information. In particular, and in unclassified terms, the privilege applies to information about whether plaintiffs themselves have been subject to any of the surveillance activities they complain about; classified intelligence sources and methods of the NSA programs at issue, such as the identities of any telecommunications carriers and facilities that provided assistance to the NSA; and intelligence collected under the programs.

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

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

[redacted]

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

[redacted]

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

15. **(U)** For all of these reasons, as further detailed below, the Government continues to assert the state secrets privilege in these cases, as described in my declaration, notwithstanding the Government's recent official disclosures.

IV. (U) BACKGROUND

A. (U) The National Security Agency

16. **(U)** The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. The NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate signals intelligence ("SIGINT") information, of which COMINT is a significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations. *See* Executive Order 12333, § 1.7(c), as amended.[4]

[4] **(U)** Executive Order 12333, reprinted as amended in 50 U.S.C § 3001 note, generally

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

18. **(U)** The NSA's SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities set forth in EO 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

---

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 "Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information for foreign intelligence and counterintelligence purposes to support national and departmental missions."

develop at a cost of billions of dollars and untold human effort. It relies on sophisticated collection and processing technology.

19. **(U)** There are two primary reasons for gathering and analyzing foreign intelligence information. The first, and most important, is to gain information required to direct U.S. resources as necessary to counter external threats and in support of military operations. The second reason is to obtain information necessary to the formulation 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; arms proliferation; international terrorism; counter-intelligence; and foreign aspects of international narcotics trafficking.

20. **(U)** The NSA's ability to produce foreign intelligence information depends on its access to foreign and international electronic communications. Foreign intelligence produced by COMINT activities 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) September 11, 2001, and the al Qaeda Threat

21. (U) 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.

22. (U) On September 14, 2001, a national emergency was declared "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.[5]

23. **(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. That conflict is continuing today, at home as well as abroad. Moreover, the conflict against al Qaeda and its allies is a very different kind of conflict, against a very different enemy, than any other conflict or enemy the Nation has previously faced. Al Qaeda and its affiliates operate not as a traditional nation-state but as a diffuse, decentralized network of

[5] **(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] 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.

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. Al Qaeda works in the shadows; secrecy is essential to al Qaeda's success in plotting and executing its terrorist attacks.

24. ~~(TS//SI//NF)~~ The 9/11 attacks posed significant challenges for the NSA's signals intelligence mission because of [redacted] Global telecommunications networks, especially the Internet, have developed in recent years into a loosely interconnected system—a network of networks—that is ideally suited for the secret communications needs of loosely affiliated terrorist cells. Hundreds of Internet service providers, or "ISPs," and other providers of communications services offer a wide variety of global communications options, often free of charge. [redacted]

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

[redacted]

26. **(U)** Our efforts against al Qaeda and its affiliates therefore present critical challenges for the Nation's communications intelligence capabilities. First, in this type of conflict, more so than in any other we have ever faced, communications intelligence is essential to our ability to identify the enemy and to detect and disrupt its plans for further attacks on the United States. Communications intelligence often is the only means we have to learn the identities of particular individuals who are involved in terrorist activities and the existence of particular terrorist threats. Second, at the same time that communications intelligence is more important than ever, the decentralized, non-hierarchical nature of the enemy and their sophistication in exploiting the agility of modern telecommunications make successful communications intelligence more difficult than ever. It is against this backdrop that the risks

presented by this litigation should be assessed, in particular the risks of disclosing NSA sources and methods implicated by the claims being raised.

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

27. **(U)** In the course of my official duties, I have been advised of the *Jewel* and *Shubert* cases, and I have reviewed the allegations raised in this litigation, including the Complaint filed in the *Jewel* action on September 18, 2008, and the Second Amended Complaint ("SAC") filed in the *Shubert* action on May 8, 2012. 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, *Shubert* SAC ¶¶ 1-7. 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. Plaintiffs seek relief in this litigation that would prohibit such collection activities, even though they were later transitioned to FISC-authorized programs and remain so to the extent the programs continue.

28. **(U)** In addition, I am familiar with the previous classified declarations filed in these cases in September and November 2012. In those declarations, the DNI and the NSA asserted the state secrets privilege over the following broad categories of information: (1) any information that may tend to confirm or deny whether particular individuals, including plaintiffs, have been subject to the alleged NSA intelligence activities; and (2) any information concerning NSA intelligence activities, sources, or methods that may relate to or be necessary to adjudicate plaintiffs' allegations, including allegations that the NSA, with the assistance of telecommunications carriers such as AT&T and Verizon, indiscriminately intercepts the content

of communications and collects the communication records of millions of Americans as part of an alleged program authorized by the President after 9/11. This latter category included (i) information concerning the scope and operation of the now inoperative TSP regarding the interception of the content of certain international communications reasonably believed to involve a member or agent of al Qaeda or an affiliated terrorist organization,[6] and any other information related to demonstrating that the NSA does not otherwise engage in the content surveillance "dragnet" alleged by plaintiffs; (ii) information concerning whether or not the NSA obtained from telecommunications companies such as AT&T and Verizon communication transactional records as alleged in the complaints; and (iii) information that may tend to confirm or deny whether AT&T, Verizon, or other telecommunications carriers have provided assistance to the NSA in connection with any of the alleged activities.

D. (U) Official Disclosures Since September 2012

29. **(U)** In the wake of unauthorized disclosures, beginning in June 2013, about intelligence-gathering activities conducted by the NSA, the DNI, at the direction of the President and in light of the President's transparency initiative, has declassified and made public certain information about a number of sensitive programs undertaken under the authority of the FISA. Certain of the information that the DNI has declassified concerns the allegations raised in this litigation, and this information has been described in great detail in the classified declarations

[6] **(U)** In December 2005, then-President Bush publicly acknowledged the existence of a presidentially-authorized NSA activity that later came to be called the "Terrorist Surveillance Program" under which the NSA was authorized to intercept the content of specific international communications (*i.e.*, to or from the United States) involving persons reasonably believed to be associated with al Qaeda and affiliated terrorist organizations. 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."

referenced above. In addition, the President has declassified the fact of the existence of two portions of the discontinued President's Surveillance Program, which also concern the allegations at issue in this litigation. I summarize these various official disclosures below.

1. (U) Collection of Bulk Telephony Metadata Under Section 215 of the FISA

30. **(U)** First, since May 2006, under a provision of the FISA known as Section 215 and codified at 50 U.S.C. § 1861, the NSA obtains, pursuant to orders of the FISC, bulk telephony metadata – business records created by telecommunications service providers that include such information as the telephone numbers placing and receiving calls, and the time and duration of those calls.[7] The Government has declassified and publicly disclosed a number of "primary" orders of the FISC to the Government authorizing it to carry out the bulk telephony metadata program. The Government has acknowledged only one "secondary" FISC order, however, to one telecommunications service provider (Verizon Business Network Services, Inc. ("VBNS")), and for only one approximately 90-day period of time (from April 25, 2013 to July 19, 2013). The Government acknowledged this secondary order only after the order was disclosed unlawfully and without authorization. This is the only FISC order identifying any particular provider that has been declassified and, 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 telephony metadata program. While the authentication of that order means that the identity of one participating provider has been officially acknowledged for the

[7] **(U)** Under the terms of the FISC's orders, the NSA is authorized to collect information including, as to each call, the telephone numbers that placed and received the call, other session-identifying information (e.g., International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card number, and the date, time, and duration of a call.

particular time period of that order, the order was limited to VBNS, did not identify any other provider, did not relate to any other corporate component of Verizon other than VBNS, and was of limited duration (expiring on July 19, 2013). There has been no official acknowledgement of whether or not VBNS assisted the NSA with the FISC telephony metadata program either before or after the period covered by the April 2013 order, or whether VBNS continues to participate in the program. The identities of the providers that furnish assistance to the NSA under the telephony metadata program, including VBNS, as to any other time period other than the approximately 90-day duration of that order, have not been declassified and remain currently and properly classified.

31. **(U)** The Government also disclosed that it does not collect, listen to, or record the content of any call under this program, nor does it collect the name, address, or financial information of any subscriber, customer, or party to a call, or cell site locational information. The Government obtains FISC orders under this program by submitting detailed applications from the Federal Bureau of Investigation ("FBI") explaining that the records are sought for investigations to protect against international terrorism that concern specified foreign terrorist organizations identified in the application. As required by Section 215, each application contains a statement of facts showing that there are reasonable grounds to believe that the metadata as a whole are relevant to the investigations of these organizations.

32. **(U)** The NSA stores and analyzes this information under carefully controlled circumstances and under stringent supervision and oversight by all three branches of Government. The vast majority of the metadata are never seen by any person. Rather, the NSA has been authorized to query the archived data solely with identifiers, typically telephone numbers, for which there are facts giving rise to a reasonable, articulable suspicion ("RAS") that

the number is associated with one or more of the foreign terrorist organizations that are the subject of FBI investigations previously identified to the FISC. Where the identifier is reasonably believed to be used by a U.S. person, the NSA may not make the RAS determination solely based on activities protected by the First Amendment.

33. **(U)** The accessible results of an approved query are limited to records of communications within three "hops" from the seed identifier.[8] That is, the query results may only include identifiers having a direct contact with the seed (the first "hop"), identifiers having a direct contact with the first "hop" identifiers (the second "hop"), and identifiers having a direct contact with second "hop" identifiers (the third "hop"). By querying the metadata using the RAS standard, NSA intelligence analysts are able to: (1) detect domestic identifiers calling foreign identifiers associated with one of the foreign terrorist organizations and discover identifiers that the foreign identifiers are in contact with; (2) detect foreign identifiers associated with a foreign terrorist organization calling into the U.S. and discover which domestic identifiers are in contact with the foreign identifiers; and (3) detect possible terrorist-related communications occurring between communicants located inside the U.S.

34. **(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 telephony metadata collection program. These compliance incidents were due to 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

[8] **(U)** A "seed" is an initial identifier used to generate a query.

authority to query the database without the court's approval) reauthorized the program in its current form.

2. (U) Bulk Collection of Internet Metadata

35. **(U)** Second, the Government has recently declassified and acknowledged the existence of FISC-authorized bulk collection of Internet metadata carried out under the "pen register, trap and trace" ("PRTT") provision of the FISA. The data collected included certain routing, addressing, and signaling information such as the "to" and "from" lines of an email and the date and time the email was sent, but not the content of an email or the subject line. Certain telecommunications service providers were compelled to provide this transactional information, which the NSA analyzed to obtain foreign intelligence information. The FISC's orders authorizing this collection required the Government to comply with minimization procedures limiting the retention and dissemination of the metadata, including a requirement of a reasonable, articulable suspicion that selection terms used to query the bulk data were associated with foreign terrorist organizations.[9] This program of bulk Internet metadata collection was terminated in 2011, because it did not meet the operational expectations the NSA had for it.

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

36. **(U)** Third, the Government has publicly revealed certain information about its use of authority conferred by Section 702 of the FISA to collect, for foreign intelligence purposes, certain communications of non-U.S. persons located outside the United States, pursuant to

[9] **(U)** Similar to the telephony metadata program (*see* ¶ 34 *supra*), the Government has also publicly disclosed FISC orders and opinions concerning various failures to fully implement and comply with FISC-ordered procedures for the Internet metadata collection program. These compliance incidents were due to human error and technological issues. In 2009, the Government reported these problems to the FISC (and Congress) and remedied them.

approval of the FISC. Section 702 facilitates the targeted acquisition of foreign intelligence information concerning foreign targets located outside the United States under court oversight. Electronic communication service providers are compelled to supply information to the Government pursuant to authorized directives issued by the Attorney General and the DNI.

37. **(U)** Once targeted surveillance under Section 702 has been authorized, the NSA takes the lead in tasking relevant telephone and electronic communications selectors to target specific non-U.S. persons reasonably believed to be located outside the United States. Consistent with the statute, 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.

38. **(U)** Once a target has been approved, the NSA uses two means to acquire the target's electronic communications. First, it acquires such communications directly from compelled U.S.-based providers. This has been publicly referred to as the NSA's PRISM collection. Second, in addition to collection directly from providers, the NSA collects electronic communications with the compelled assistance of electronic communication service providers as they transit Internet "backbone" facilities within the United States.[10] The NSA has strict minimization and dissemination procedures, and as is the case with the telephony metadata program, the NSA's Section 702 collection activities are subject to extensive oversight by all three branches of the Government.

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

39. **(U)** As with the telephony metadata program, the Government has also disclosed compliance incidents involving its Section 702 collection activities. In an opinion issued on October 3, 2011, the FISC found the NSA's proposed minimization procedures as applied to the NSA's upstream collection of Internet transactions containing multiple communications, or "MCTs," deficient. Oct. 3, 2011 FISC Op., 2011 WL 10945618. In response, the NSA modified its proposed procedures and the FISC subsequently determined that the NSA adequately remedied the deficiencies such that the procedures met the applicable statutory and constitutional requirements, and allowed the collection to continue. Aug. 24, 2012 FISC Op., 2012 WL 9189263, at *2-3; Nov. 30, 2011 FISC Op., 2011 WL 10947772.

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

40. **(U)** In December 2005 then-President Bush acknowledged the existence of a presidentially-authorized NSA activity called the TSP under which NSA was authorized to intercept the content of specific international communications (*i.e.*, to or from the United States) involving persons reasonably believed to be associated with al Qaeda and affiliated terrorist organizations. Other intelligence activities were authorized by the President after the 9/11 attacks in a single authorization and were subsequently authorized under orders issued by the FISC. In light of the declassification decisions described above concerning the NSA's collection of telephony and Internet metadata and targeted content collection under FISC orders, the President has determined to publicly disclose the fact of the existence of those activities prior to the FISC orders, pursuant to presidential authorization. Accordingly, certain limited information concerning these activities has now been declassified:

41. **(U)** Starting on October 4, 2001, 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. President Bush authorized the NSA to collect: (1) the contents of certain international communications, a program that was later referred to as the TSP; and (2) telephony and Internet non-content metadata in bulk, subject to various conditions.

42. **(U)** President Bush issued authorizations 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 applied additional internal constraints on the presidentially-authorized activities.

43. **(U)** 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 Government transitioned the TSP to the authority of the FISA and under the orders of the FISC. In August 2007, Congress enacted the Protect America Act ("PAA") as a temporary measure. The PAA, which expired in February 2008, was replaced by the FISA Amendments Act of 2008 ("FAA"), which was enacted in July 2008 and remains in effect today. Today, content collection is conducted pursuant to section 702 of the FISA. The metadata activities also were transitioned to orders of the FISC. The bulk collection of telephony metadata transitioned to the authority of the FISA in May 2006 and is collected pursuant to Section 215 of FISA. The bulk collection of Internet metadata was transitioned to the authority of the FISA in July 2004 and was collected pursuant to Section 402 of FISA. In December 2011, the Government decided not to seek reauthorization of the bulk collection of Internet metadata.

V. (U) INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE

44. (U) While information about the existence of the components of the PSP has now been declassified, specific operational details concerning the program's scope, operation, the sources and methods it utilized, and intelligence it produced remain properly classified and are subject to the DNI's state secrets privilege assertion and my own assertion of NSA's statutory privilege in this declaration. In general and unclassified terms, the DNI's assertion of the state secrets privilege 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 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 concerning the scope and operational details of NSA intelligence activities that may relate to or be necessary to adjudicate plaintiffs' allegations, including:

(1) **(U)** *Communications Content Collection:* information concerning the scope or operational details of NSA intelligence activities that may relate to or be necessary to adjudicate plaintiffs' claims that the NSA indiscriminately intercepts the content of communications, *see, e.g., Jewel* Complaint ¶¶ 9, 10, 73-77; *Shubert* SAC ¶¶ 1,2, 7, 64-70, including:

(a) **(U)** *TSP Information:* information concerning the scope and operation of the now inoperative TSP regarding the interception of the content of certain international communications reasonably believed to involve a member or agent of al Qaeda or an affiliated terrorist organization;

(b) **(U)** *FISA Section 702:* information concerning operational details related to the collection of communications under FISA section 702; and

(c) **(U)** Any other information related to demonstrating that the NSA has not otherwise engaged in the content-surveillance dragnet that the plaintiffs allege.

(2) **(U)** *Communications Records Collection:* information concerning the scope or operational details of NSA intelligence activities that may relate to or be necessary to adjudicate plaintiffs' claims regarding the NSA's bulk collection of telephone and Internet non-content communications records ("metadata"), *see, e.g.*, *Jewel* Complaint ¶¶ 10, 11, 13, 73-77, 82-97; *Shubert* SAC ¶¶ 102;

C. (U) Telecommunication Provider Identities: information that may tend to confirm or deny whether AT&T or Verizon (and to the extent relevant or necessary, any other telecommunications carrier) has provided assistance to the NSA in connection with any intelligence activity, including the collection of communications content or non-content transactional records alleged to be at issue in this litigation.

VI. (U) HARM OF DISCLOSURE OF PRIVILEGED INFORMATION

A. (U) Information Concerning Whether Plaintiffs Have Been Subject to the Alleged NSA Activities

45. **(U)** The first major category of information as to which I am supporting the DNI's assertion of privilege, and asserting the NSA's own statutory privilege, concerns information as to whether particular individuals, including the named plaintiffs in this lawsuit, have been subject to alleged NSA intelligence activities. 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. The named plaintiffs in the *Jewel* and *Shubert* cases allege that the content of their own telephone and Internet communications has been and continues to be subject to unlawful search and seizure by the NSA, along with the content of communications of millions of ordinary Americans.[11] Further, the named plaintiffs allege that the NSA has been and is

[11] **(U)** Specifically, the *Jewel* plaintiffs allege that pursuant to a presidentially authorized program after the 9/11 attacks, the NSA, with the assistance of AT&T, acquired and continues to

continuing to collect and analyze the private telephone and Internet transaction records of millions of Americans, with the assistance of telecommunication carriers, again including information concerning the plaintiffs' telephone and Internet communications.[12]

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

46. ~~(TS//STLW//SI//OC/NF)~~ As described herein, the NSA does not engage in "dragnet" surveillance of the content of communications as plaintiffs allege. [redacted]

acquire the content of phone calls, emails, instant messages, text messaged, web and other communications, both international and domestic, of millions of ordinary Americans – "practically every American who uses the phone system or the Internet" – including the plaintiffs. *See Jewel* Compl.¶¶ 7, 9, 10; *see also id.* at ¶¶ 39-97. The *Shubert* plaintiffs allege that the contents of "virtually every telephone, Internet and email communication sent from or received within the United States since shortly after September 11, 2001," including plaintiffs' communications, are being "searched, seized, intercepted, and subject to surveillance without a warrant, court order or any other lawful authorization in violation of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1810." *See Shubert* SAC ¶ 1; *see also id.* ¶¶ 5, 7.

[12] **(U)** Specifically, the *Jewel* plaintiffs allege that the NSA has "unlawfully solicited and obtained from telecommunications companies the complete and ongoing disclosure of the private telephone and internet transactional records" of millions of ordinary Americans, including plaintiffs. *See Jewel* Compl. ¶¶ 7, 10, 11, 13, 82-97. They further claim the NSA analyzes this information. *Id.* ¶ 11. The *Shubert* plaintiffs allege that "NSA now monitors huge volumes of records of domestic emails and Internet searches…[and] receives this so-called 'transactional' data from…private companies…" *See Shubert* SAC ¶ 102.

[redacted][13] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted][14]

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

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

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

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

[redacted]

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

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

[redacted]

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

[16] (~~TS//STLW/SI//OC/NF~~) During the time period covered by the Presidential Authorizations, the NSA estimated that it collected Internet metadata associated with approximately [redacted] At the time the bulk collection of Internet metadata pursuant to orders of the FISC (the PRTT Order) expired in December 2011, the NSA estimates that the percentage of Internet metadata that it collected had been reduced to approximately [redacted] Furthermore, the NSA has previously estimated that, prior to the 2006 FISC Order, about [redacted] telephony metadata records was presented to an analyst for review.

[redacted]

disclosure of information concerning whether plaintiffs have been personally subject to these NSA activities reasonably could be expected to cause exceptionally grave damage to national security because it would reveal information concerning whether particular individuals have been subject to surveillance and the nature, scope, and extent of NSA surveillance activities.

49. **(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 subject of intelligence gathering would indicate who has avoided surveillance or collection and what may be a secure channel for communication. Such information could lead an actual or potential adversary, secure in the knowledge that he is not under government scrutiny, to help a hostile foreign adversary convey information; alternatively, such a person may be unwittingly utilized or even forced to convey information through a secure

channel to a foreign adversary. Revealing which channels are free from surveillance and which are not would also reveal sensitive intelligence methods and thereby could help any adversary evade detection and capitalize on limitations in NSA's capabilities. Similar harms would result from confirming or denying whether a person's communications have been subject to collection even where it may be assumed a person is law-abiding and not likely to be an actual target or subject of such activity. For example, if the NSA were to confirm that specific individuals have not been targets of or subject to collection (*i.e.*, whether their communications have 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 likewise seek such confirmation or denial and then easily deduce by comparing such responses 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.

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

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

[redacted]

52. **(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 the national security.

B. (U) Operational Information Concerning NSA Intelligence Activities

53. **(U)** I am also supporting the DNI's assertion of privilege and asserting the NSA's statutory privilege over any other still-classified facts concerning NSA intelligence activities, sources, or methods that may relate to or be necessary to litigate the plaintiffs' claims and allegations, including that: (1) the NSA is indiscriminately intercepting the content of communications of millions of ordinary Americans, *see e.g., Jewel* Complaint ¶¶ 7, 9, 10; *Shubert* SAC ¶¶ 1, 5, 7; and (2) the NSA is collecting the private telephone and Internet transactional records of Americans with the assistance of telecommunications carriers, again including information concerning the plaintiffs' telephone and Internet communications. *See Jewel* Complaint ¶¶ 7, 10, 11, 13, 82-97; *see Shubert* SAC ¶ 102. As described above, the scope

of the Government's privilege assertion includes but is not limited to still-classified information concerning (1) the collection of communication content under the now inoperative TSP as well as pursuant to authority of FISA Section 702, and any other NSA activities that would be at risk of disclosure or required in demonstrating that the NSA has not engaged in content "dragnet" surveillance activities that plaintiffs allege; and (2) information that may relate to or be necessary to adjudicate plaintiffs' claims regarding the NSA's bulk collection of telephony and Internet communication records. As set forth below, the disclosure of such information would cause exceptionally grave harm to national security.

1. (U) Information Concerning Plaintiffs' Content Surveillance Allegations

54. **(U)** After the existence of the TSP was officially acknowledged in December 2005, the Government stated that this activity was limited to the interception of the content of certain communications for which there were reasonable grounds to believe that: (1) such communication originated or terminated outside the United States; and (2) a party to such communication is a member or agent of al Qaeda or an affiliated terrorist organization. Nonetheless, plaintiffs' allege that the NSA indiscriminately intercepts the content of communications of millions of ordinary Americans. *See e.g., Jewel* Complaint ¶¶ 7, 9, 10; *see Shubert* SAC ¶¶ 1, 5, 7. As the Government has also previously stated,[17] plaintiffs' allegation

[17] **(U)** *See* Public Declaration of Dennis Blair, Director of National Intelligence, ¶ 15 (April 3, 2009) (Dkt. 18-3 in *Jewel* action (08-cv-4373); Public Declaration of Deborah A. Bonanni, National Security Agency ¶ 14 (Dkt. 18-4 in *Jewel* action (08-cv-4373); Public Declaration of Dennis Blair, Director of National Intelligence, ¶ 15 (October 30, 2009) (Dkt. 680-1 in *Shubert* action (MDL 06-cv-1791); Public Declaration of Lt. Gen. Keith B. Alexander, National Security Agency ¶ 19 (Dkt. 680-1 in *Shubert* action (MDL 06-cv-1791).

that the NSA has undertaken indiscriminate surveillance of the content[18] of millions of communications sent or received by people inside the United States after 9/11 under the TSP is false. But in order to disprove plaintiffs' claim that the NSA indiscriminately collected the content of the communications of millions of Americans, the NSA would have to disclose the specifics of its content collection activities. Under the TSP, the NSA was directed pursuant to presidential authorization[19] to intercept the content of only those international telephone and Internet communications for which there were reasonable grounds to believe that such communications involved a member or agent of al Qaeda or an affiliated terrorist organization. To the extent the NSA must demonstrate that content surveillance under the TSP was so limited, and was not plaintiffs' alleged content "dragnet," or demonstrate that the NSA has not otherwise engaged in the alleged content "dragnet," highly classified NSA intelligence sources and

---

[18] **(U)** Again, 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).

[19] ~~**(TS//STLW//SI//OC/NF)**~~ The specific wording of the presidential authorizations evolved over time and during certain periods authorized other activities. [redacted]

methods about the operation of the TSP and current NSA intelligence activities (including under FISA Section 702) would be subject to disclosure or the risk of disclosure. The disclosure of whether and to what extent the NSA utilizes certain intelligence sources and methods would reveal to foreign adversaries the NSA's capabilities, or lack thereof, enabling them to either evade particular channels of communications that are being monitored, or exploit channels of communication that are not subject to NSA activities, in either case risking exceptionally grave damage to national security. As set forth below, a range of operational details concerning the TSP, as well as other NSA sources and methods, remains properly classified and privileged from disclosure, and could not be revealed to address plaintiffs' content "dragnet" allegations.

55. **(U)** Authorization of the TSP was intended to address an important gap in NSA's intelligence collection activities---namely, that significant changes in communications technology since the enactment of the FISA in 1978 meant that the NSA faced great difficulties in identifying foreign terrorist operatives who were communicating with individuals within the United States. FISA established the framework for court approval of the U.S. Government's efforts to conduct foreign intelligence surveillance of individuals in the United States. When FISA was enacted in 1978, most international communications to or from the United States were transmitted via satellite or radio technology. Congress intentionally excluded the vast majority of satellite or radio communications from the definition of "electronic surveillance" in the FISA. *See* 50 U.S.C. §1801(f).

56. ~~**(TS// SI//OC/NF)**~~ The interception of domestic communications within the United States, which were carried nearly exclusively on a wire, for foreign intelligence purposes, generally required a court order. As a result, [redacted]

[redacted]

[redacted] the FISA did limit the NSA's ability to collect "one-end" telephone or Internet communications to or from the United States on a wire inside the United States.

57. **(U)** Since the time FISA was enacted, sweeping advances in modern telecommunications technology upset the balance struck by Congress in 1978. By 2001, most international communications to or from the United States were carried on a wire and many domestic communications had increasingly become wireless. As a result of this change in communications technology, the NSA's collection from inside the United States of international communications (previously carried primarily via radio transmission) had shrunk considerably and the Government was forced to prepare FISA applications if it wished to collect the communications of non-U.S. persons located overseas.

58. ~~**(TS//STLW/SI//OC/NF)**~~ These circumstances presented a significant concern in the exceptional circumstances after 9/11. The NSA confronted the urgent need to identify further plots to attack U.S. interests both domestically and abroad. To do so, it needed to intercept the communications of terrorist operatives who, as described above, [redacted] Further, as the [redacted] the United States was faced with the prospect of losing vital intelligence---and failing to detect another feared imminent attack---while the Government prepared thousands of individual applications for FISA Court authorization on a large number of rapidly changing telephone numbers and email addresses.

59. ~~**(TS//STLW/SI//OC/NF)**~~ Under the TSP, the NSA collected the content of certain international telephone communications [redacted]

[redacted]

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

[redacted]

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

[redacted][21]

[redacted][22]

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

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

61. ~~(TS//STLW/SI//OC/NF)~~ In addition, the NSA took specific steps in the actual TSP content interception process to minimize the risk that the communications of non-targets were intercepted. With respect to telephone communications, [redacted] the only communications intercepted were those to or from the targeted number of an individual who was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization. For the interception of the content of Internet communications under the TSP, the NSA used identifying information obtained through its analysis of the target, such as email addresses [redacted] to target for collection the communications of individuals reasonably believed to be members or agents of al Qaeda or an affiliated terrorist organization. [redacted] The NSA did not search the content of the communications [redacted] with "key words" (such as "wedding" or "jihad") other than the targeted selectors themselves. *See Jewel* Complaint ¶11; *Shubert* SAC ¶¶ 70, 72 (alleging key word searches on communications content). Rather, the NSA targeted for collection Internet addresses [redacted] associated with suspected members or agents of al Qaeda or affiliated terrorist organizations, or communications in which such [redacted] were mentioned. In addition, due to technical limitations of the hardware and software, incidental collection of non-target communications occurred, and in such circumstances the NSA applied its

[redacted]

minimization procedures to ensure that communications of non-targets were not disseminated. To the extent such facts would be necessary to dispel plaintiffs' erroneous content "dragnet" allegations, they could not be disclosed without revealing highly sensitive intelligence methods.[23]

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

[redacted]

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

[redacted]

63. ~~(TS//STLW/SI//OC/NF)~~ In order to disprove plaintiffs' claims of "dragnet" content surveillance, the NSA would need to reveal the more limited nature of the content collection under the TSP. [redacted]

[redacted][24]

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

[redacted]

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

[redacted] For example, under the NSA's current "upstream" collection program under Section 702 of the FISA, the NSA seeks to collect communications to, from, or about a tasked selector (*e.g.*, an email address) associated with a target reasonably believed to be located outside the United States. [redacted]

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

[redacted]

66. ~~(TS//SI//NF)~~ The public disclosure of the above information about the specifics of the NSA's content collection activities would greatly benefit NSA's adversaries. Foreign adversaries, to include foreign governments and terrorist organizations, would be provided with a detailed roadmap [redacted]

2. (U) Information Concerning Plaintiffs' Communications Records Collection Allegations

67. **(U)** Plaintiffs also allege that the NSA is collecting the private telephone and Internet transaction records of millions of Americans, again including information concerning plaintiffs' telephone and Internet communications. *See, e.g., Jewel* Complaint ¶¶ 7, 10, 11, 13, 8, 13, 82-97; *see Shubert* SAC ¶ 102. To address these allegations would risk or require disclosure of NSA sources and methods and reasonably could be expected to cause exceptionally grave damage to national security. While the Government has declassified the existence of the telephony and Internet metadata collections, and some information concerning those programs as authorized by the FISC, significant operational details concerning these activities remain properly classified, including the identity of communication providers who may have assisted in this collection, and other sources and method of collection and analysis. As set forth below, disclosure of this information reasonably could be expected to cause grave damage to national security.

(a) (U) Collection of Bulk Telephony Metadata

68. **(U)** As with the operational details concerning the NSA's collection of communications content, I am supporting the DNI's state secrets privilege assertion, and asserting NSA's statutory privilege, over still-classified information that may relate to or be necessary to litigate plaintiffs' claims as they relate to the alleged collection of telephony metadata.

69. **(U)** The still classified operational details concerning the collection of telephony metadata include, but are not necessarily limited to, whether metadata of plaintiffs' telephone communications were actually collected by the NSA from plaintiffs' particular communications

providers; whether any metadata of plaintiffs' telephone communications, if collected, were viewed or analyzed by anyone at the NSA; information demonstrating the scope of the telephony metadata collection program; and information demonstrating the need for and effectiveness of the program

70. ~~(TS//STLW/SI//OC/NF)~~ First and foremost, I support the DNI's privilege assertion, and assert the NSA's statutory privilege, [redacted][25] [redacted][26] [redacted]

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

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

[redacted]

71. **(U)** As set forth in this declaration, following the unauthorized disclosure in June 2013 of one FISC Order issued as part of the telephony metadata program, the Government confirmed the authenticity of one order, issued on April 25, 2013, by the FISC to a particular Verizon Communications subsidiary, Verizon Business Network Services (VBNS), thereby confirming the participation of VBNS in the program for the duration of that order (approximately 90 days). This is the only FISC order identifying any particular provider under this program that has been declassified, and since the disclosure of this order in June 2013, the United States has not confirmed or denied the past or current participation of any specific provider in the telephony metadata program apart from the participation of VBNS for the approximately 90 day duration of the now-expired April 25, 2013, FISC Order. As explained further below, the continued protection of whether or not, or to what extent, a particular telecommunications provider assisted the NSA under FISC Order or otherwise 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.

72. ~~(TS//SI//NF)~~ In addition, still-classified details of the NSA's process for querying the telephony metadata, [redacted] must not be disclosed to prevent risking exceptionally grave damage to national security. [redacted]

[redacted]

[27] [redacted]

[28] [redacted]

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

[28] ~~(TS//SI//NF)~~ As noted above, *see* ¶ 31 *supra*, the NSA does not collect cell site location information ("CSLI") pursuant to Section 215 of the FISA. [redacted] the FISC orders did not authorize the NSA to collect CSLI. [redacted]

[redacted]

73. ~~(TS//SI//NF)~~ Additionally, while the NSA has publicly disclosed that it is authorized to query the telephony metadata collected under FISC orders either by manual analyst queries or through an automated query process, other specific details concerning how the NSA's automated query process works remain currently and properly classified. [redacted]

[redacted][29]

[redacted]

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

[redacted]

74. ~~(TS//SI//NF)~~ Finally, to the extent that facts related to how the NSA analyzes telephony metadata are required to litigate plaintiffs' claims [redacted], the disclosure of still classified sources and methods related to the analysis of the metadata reasonably could be expected to cause grave damage to national security. [redacted]

[redacted][30] [redacted]

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

[redacted][31]

(b) (U) Internet Metadata Collection

75. **(U)** I am also supporting the DNI's privilege assertion, and asserting the NSA's statutory privilege, over still-classified operational details concerning the NSA's bulk collection of Internet metadata under presidential authorization.

76. **(~~TS//STLW/SI//OC/NF~~)** [redacted] Although the program is no longer operative,[32] [redacted][33] [redacted]

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

[32] **(~~TS//SI//NF~~)** On December 7, 2011, the NSA completed the destruction of all PRTT metadata collected under the authorization of the FISC from the Agency's repositories.

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

[redacted]

Disclosure of this information would provide a roadmap to our adversaries of the scope and methodologies of this intelligence-gathering activity and thus reasonably could be expected to cause grave damage to national security.

77. (~~TS//STLW/SI//OC/NF~~) [redacted] After proceeding for nearly three years under Presidential authorization, the bulk collection of Internet metadata under PRTT provision was first authorized by the FISC in July 2004, and was reauthorized approximately every 90 days thereafter until December 2011.[34] [redacted] This information remains properly classified and subject to the DNI's privilege assertion, as well as my own NSA statutory privilege assertion and, as detailed further below, [redacted] in this collection activity reasonably could be expected to cause grave damage to national security.

[redacted]

[34] (~~TS//SI//NF~~) In accord with FISC oversight of NSA activities subject to the FISA, starting in [redacted] authorization for the PRTT Order was discontinued while the NSA resolved certain compliance issues with the FISC. The PRTT Order was reauthorized in [redacted] until its last authorization expired in December 2011.

78. ~~(TS//STLW/SI//OC/NF)~~ Second, the method by which the NSA collected Internet metadata under presidential authorization and subsequent FISC orders also remains classified and properly protected from disclosure under the DNI's and my own privilege assertions. Specifically, [redacted][35]

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

[redacted] Revelations as to the NSA's capabilities, and the potential disclosure of intelligence gather from these techniques, reasonably could be expected to cause grave damage to national security.

79. ~~(TS//SI//NF)~~ Third, disclosure of the nature of the Internet metadata collected by the NSA under presidential authorization, and as that collection activity was transitioned to FISA, would reveal other highly sensitive and still classified sources and methods. [redacted][36] [redacted]

[36] ~~(TS//SI//NF)~~ Under the FISC's PRTT Orders, the NSA queried the archived metadata only using Internet selectors for which there were facts giving rise to a reasonable, articulable suspicion that the email address was associated with [redacted]

[redacted]

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

[redacted]

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

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

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

[redacted] Accordingly, to the extent necessary to address whether [redacted] plaintiffs' metadata was actually collected, revealing the foregoing details concerning the categories of metadata the NSA collected would reveal highly sophisticated operational details of NSA's current SIGINT operations and reasonably could be expected to cause grave damage to national security by alerting adversaries as to the NSA's specific collection capabilities.

81. ~~(TS//SI//NF)~~ Finally, it bears emphasis that the continuing importance of the sources and methods by which bulk Internet metadata was collected and analyzed underscores the need to protect operational details of this activity. [redacted]

[redacted]

82. ~~(TS//SI//NF)~~ As with telephony metadata, the collection of this information allowed the NSA to use sophisticated and unique analytical capabilities to track the contacts (even retrospectively) [redacted] of known terrorists. The techniques that the NSA developed pursuant to presidential authorization have been refined over time and continue today to derive sensitive intelligence that is vital to protecting the national security of the United States. [redacted]

[redacted] Revealing these capabilities would cause exceptionally grave damage to national security.

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

84. (~~TS//SI//OC/NF~~) [redacted] Thus, if necessary to litigate plaintiffs' claims, the disclosure of details about the scope and operation of the now-discontinued bulk Internet metadata collection program, beyond the facts that have been officially confirmed by the Government, can be expected to compromise the NSA's current collection activities and analytical capabilities, and thus cause exceptionally grave damage to the national security of the United States.

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

85. **(~~TS//STLW/SI [redacted] //OC/NF~~)** I am also supporting the DNI's state secrets privilege assertion, and asserting NSA's statutory privilege, over information relating to [redacted] The *Jewel* plaintiffs and three of the *Shubert* plaintiffs allege that they are customers of AT&T, and that AT&T participated in the alleged intelligence-gathering activities that the plaintiffs seek to challenge. Additionally, at least one *Shubert* plaintiff also claims to be a customer of Verizon, and that Verizon similarly participated in the alleged intelligence-gathering activities that the plaintiffs seek to challenge. The harm from officially acknowledging whether or not any specific carrier has assisted the NSA is significant, as noted above, and continues to exist notwithstanding the recent official disclosures. While the Government has declassified some information concerning the nature and scope of the programs described above -- including that it collects telephony and Internet metadata in bulk, from multiple telecommunication providers -- and has also confirmed the authenticity of a single now-expired FISC Order issued to a single carrier that had been unlawfully disclosed, it has not otherwise declassified information concerning the identities of companies that are or were subject to FISC orders under NSA intelligence-gathering programs [redacted]

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

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

[redacted]

[redacted][40]

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

[redacted]

[redacted][41]

88. (~~TS//SI [redacted] //OC/NF~~) Confirmation or denial of a relationship between the NSA and AT&T, Verizon, or any other telecommunications carrier relating to intelligence activities would cause exceptionally grave damage to the national security in multiple ways, notwithstanding the Government's recent disclosures.[42] [redacted]

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

[42] **(U)** Congress recognized the need to protect the identities of telecommunications carriers alleged to have assisted the NSA when it enacted provisions of the FISA Amendments Act of 2008 that barred lawsuits against telecommunications carriers alleged to have assisted the NSA after the 9/11 attacks. In enacting this legislation, the Senate Select Committee on Intelligence ("SSCI") found notwithstanding the fact that the existence of the TSP had been officially acknowledged, that "electronic surveillance for law enforcement and intelligence purposes depends in great part on the cooperation of private companies that operate the nation's telecommunications system." S. Rep. 110-209 (2007) at 9 (accompanying S. 2248, Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008). Notably, the SSCI expressly stated that, in connection with alleged post-9/11 assistance, "it would be inappropriate to disclose the names of the electronic communication service providers from which assistance was sought, the activities in which the Government was engaged or in which the providers assisted, or the details regarding any such assistance." *Id.* The Committee added that the "identities of persons or entities who provide assistance to the intelligence community are properly protected as sources and methods of intelligence." *Id.*

[redacted]

[redacted] Finally, the harms to national security that would result from public disclosure of a provider's assistance are still likely to occur notwithstanding the recent declassification of some aspects of the NSA's intelligence gathering activities, including the official confirmation that telephony metadata are collected in bulk from more than one provider.

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

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

[redacted]

[redacted]

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

[redacted]

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

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

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

[redacted]

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

[redacted]

[redacted]

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

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

[redacted]

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

[redacted]

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

[redacted]

[redacted][43]

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

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

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

[redacted] [44]

[redacted] [45] [redacted] [46] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

---

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

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

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

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

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

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

[redacted]

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

[redacted]

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

[redacted]

[redacted]

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

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

[redacted]

[redacted][47]

[redacted]

[redacted][48]

---

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

[48] ~~(TS//TSP/SI [redacted] //OC/NF)~~ [redacted]

[redacted]

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

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

[49] [redacted]

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

[redacted]

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

[redacted]

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

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

[redacted]

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

[redacted]

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

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

[redacted]

[51] [redacted]

[redacted]

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

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

111. (~~TS//SI [redacted] //OC/NF~~) I have determined that [redacted] must remain classified to avoid the risk of exceptionally grave damage to the national security, notwithstanding the Government's recent official disclosures about the NSA's collection of bulk telephony and Internet metadata and communications content under presidential authority and under the FISA. While the Government has declassified some information concerning the nature and scope of these programs—including that the telephony metadata program is a bulk collection activity from multiple telecommunication providers—and has also confirmed the authenticity of a single FISC Order directed to VBNS that had been unlawfully disclosed to the news media, it has not otherwise declassified information concerning the identities of companies that are or were subject to FISC orders [redacted]

112. (~~TS//SI//OC//NF~~) Shortly after the unauthorized disclosure and publication of the FISC Order, issued on April 25, 2013, to VBNS, requiring that provider to furnish to the NSA all telephony metadata for communications (i) between the United States and abroad; or (ii) wholly within the United States, the DNI authenticated and declassified this order to address significant public interest—and correct public misimpressions—concerning this U.S. intelligence activity. As noted above, this is the only FISC Order identifying any particular provider that has been declassified and, since its disclosure in June 2013, the United States has continued to protect against any further disclosures of FISC orders [redacted] While the authentication of that order means that the identity of one participating provider has been officially acknowledged during the particular time period of that

order, the order was limited to VBNS, did not identify any other provider, [redacted] and was of limited duration (expiring on July 19, 2013). [redacted]

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

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

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

[redacted]

116. ~~(TS//SI//NF)~~ Determinations about where to draw the line regarding information that can be made public and information that must remain classified are necessarily predictive judgments made in light of important and competing considerations, including the need to protect the Nation and the need for Government accountability to the public. The fact that the U.S. Government has officially acknowledged that the collection of telephony metadata occurs in bulk and involves the participation of more than one provider, [redacted] does not in itself reveal which particular companies are now providing records to the NSA or for how long they have been doing so, or which companies are not providing records. And, as outlined above, significant national security reasons remain for protecting that information. [redacted]

VII. (U) CONCLUSION

117. ~~(TS//STLW/SI//OC/NF)~~ Upon examination of the allegations, claims, facts, and issues raised by these cases, it is my judgment that issues that are central to the litigation implicate sensitive state secrets and that disclosure of these secrets could cause exceptionally grave harm to the national security of the United States. Although plaintiffs' alleged content surveillance dragnet does not (and did not) occur, proving why that is so, [redacted] would directly implicate highly classified intelligence sources and methods still relevant to NSA activities today. Similarly, attempting to address plaintiffs' allegations with respect to the bulk collection of non-content metadata would also compromise currently operative NSA sources and methods that are essential to protecting national security, including for detecting and preventing a terrorist attack.

118. (~~TS//STLW/SI [redacted] //OC/NF~~) [redacted] In the NSA's judgment, any effort to probe the outer-bounds of such privileged information would pose inherent and significant risks of disclosure of that information, including critically sensitive information about NSA sources, methods, operations, targets, and relationships. Providing access to records and data associated with the programs at issue in these cases would tend to reveal, particularly to sophisticated foreign adversaries, the full picture of U.S. intelligence gathering sources and methods.

119. **(U)** The United States has an overwhelming interest in detecting and thwarting further plots to perpetrate mass-casualty attacks by al Qaeda and other terrorist organizations. The United States has already suffered one massive attack that killed thousands, disrupted the Nation's financial center for days, and successfully struck at the command and control center for the Nation's military. It remains a key objective of al Qaeda and other terrorist groups to carry out a massive attack in the United States that could result in a significant loss of life, as well as have a devastating impact on the U.S. economy.

120. **(U)** As set forth above, terrorist organizations around the world seek to use our own communications infrastructure against us as they secretly attempt to infiltrate agents into the United States, waiting to attack at a time of their choosing. One of the greatest challenges the United States confronts in the ongoing effort to prevent another catastrophic terrorist attack against the U.S. Homeland is the critical need to gather intelligence quickly and effectively. Time is of the essence in preventing terrorist attacks, and the Government faces significant obstacles in finding and tracking terrorist operatives as they manipulate modern technology in an attempt to communicate while remaining undetected. The NSA sources, methods, and activities described herein are vital tools in this effort.

121. (U) For the foregoing reasons, I support the DNI's assertion of the state secrets privilege and statutory privilege to prevent the disclosure of the information described herein and detailed herein. I also assert a statutory privilege under Section 6 of the National Security Act with respect to the information described herein which concerns the functions of the NSA. I respectfully request that the Court protect that information from disclosure to prevent exceptionally grave damage to the national security of the United States.

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

DATE: 12.20.13

Frances J. Fleisch
National Security Agency