STUART F. DELERY
Acting Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
VINCENT M. GARVEY
Deputy Branch Director
ANTHONY J. COPPOLINO
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782/Fax: (202) 616-8460
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.	**No. 08-cv-4873-JSW** **CLASSIFIED DECLARATION OF FRANCES J. FLEISCH, NATIONAL SECURITY AGENCY** **EX PARTE, IN CAMERA SUBMISSION** Date: November 2, 2012 Time: 9:00 a.m. Courtroom 11, 19th Floor Judge Jeffrey S. White

(U) Table of Contents

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 Executive Director for the National Security Agency (NSA), an intelligence agency within the Department of Defense. I have held this position since June 2010. As the Executive Director, I serve as an adjunct to the Deputy Director for all NSA matters. Under our internal regulations, and in the absence of the Director and Deputy Director, 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 No. 13526, 75 Fed. Reg. 707 (2009) and Department of Defense Directive No. 5200.1-R, Information and Security Program Regulation, 32 C.F.R. § 159a.12 (2000).

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 NSA activities described herein below. General Keith B. Alexander, the Director of the National Security Agency, has been sued in his official and individual capacity in the above captioned litigation and has recused himself from the decision on whether to assert privilege in his official capacity. As the Executive 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. Through this

declaration, I 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 as a note to 50 U.S.C. § 402) ("NSA Act"), to protect the information related to NSA activities described herein below. The statements made herein are based on my personal knowledge of NSA activities and operations, and on information made available to me as the Executive Director of the NSA.[1]

II. (U) Summary

3. (U) In the course of my official duties, I have been advised of the above-captioned *Jewel*, *Shubert*, and *In re NSA Telecommunications Records Litigation*, 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 above-referenced *Shubert* action on May 8, 2012.[2] 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 the presidentially-authorized activities at issue in this litigation went beyond the "Terrorist Surveillance Program" ("TSP"), which was publicly acknowledged by the President

---

[1] (U) This declaration addresses and asserts privilege with respect to allegations raised in the above-captioned *Jewel action* as well as a separate action---*Shubert v. Obama* (07-cv-00693). In addition, the harm to national security that would result from the disclosure of NSA sources and methods described herein is applicable to similar allegations concerning NSA activities raised in other lawsuits in *In re NSA Telecommunications Records Litigation* (M:06-cv-1791)

[2] ~~(TS//SI//OC/NF)~~ Starting in 2006, the Director of National Intelligence, supported by declarations from the NSA like this one, has asserted the state secrets privilege and related statutory privileges concerning NSA intelligence sources and methods in several other cases that have been before this court, including in a 2006 lawsuit brought by the plaintiffs in *Jewel* against AT&T (*Hepting v. AT&T*) (06-cv-00672), as well as in 2007 with respect to lawsuits brought against *Verizon Communications*, and again in 2007 and 2009 in the *Shubert* action, and also in 2009 in the *Jewel* action. This declaration concerns the same sources and methods that were at issue in those prior declarations, and sets forth substantially the same facts and harms to national security previously described to the court. In light of the passage of time, this submission updates, expands upon, and supplants prior privilege assertions in this litigation.

in December 2005 and was limited to the interception of specific international communications involving persons reasonably believed to be associated with al Qaeda and affiliated terrorist organizations. Rather, plaintiffs allege that other intelligence activities were also authorized by the President after 9/11, and that, with the assistance of telecommunication companies, including AT&T and Verizon, the NSA has indiscriminately intercepted the content and obtained the communications records of millions of ordinary Americans as part of an alleged presidentially-authorized "Program" after 9/11. *See Jewel* Compl. ¶¶ 2-13; 39-97; *Shubert* SAC ¶¶ 1-7; 57-58; 60-91.

4. **(U)** I cannot disclose on the public record the specific nature of NSA information or activities implicated by the plaintiffs' allegations. As described further below, the disclosure of information related to the NSA's activities, sources, and methods implicated by the plaintiffs' allegations reasonably could be expected to cause exceptionally grave damage to the national security of the United States. In addition, it is my judgment that sensitive state secrets are so central to the subject matter of the litigation that any attempt to proceed in the case risks disclosure of the classified privileged national security information described herein and exceptionally grave damage to the national security of the United States.

5. ~~(TS//TSP//SI-[redacted]//OC/NF)~~ The allegations in this lawsuit put at issue the disclosure of information concerning several highly classified and critically important NSA intelligence activities, sources and methods that commenced under presidential authorization after the 9/11 terrorist attacks, but which were later transitioned to the authority of the Foreign Intelligence Surveillance Act ("FISA"), including ongoing activities conducted under orders approved by the Foreign Intelligence Surveillance Court ("FISC").[3] As described in more detail

[3] ~~(TS//SI-[redacted]//OC/NF)~~ As described further below, pursuant to the FISA and specific orders of the FISC, the intelligence activities that NSA carries out under the authority of the FISA and authorization of the FISC are classified. NSA's FISC-approved activities that are at issue here are classified at the TOP SECRET//COMINT level as their unauthorized disclosure

below, starting in October 2001, then-President Bush issued a presidential authorization that directed the NSA to undertake three discrete activities after the 9/11 attacks that were designed to enhance NSA's capability to detect and prevent further attacks. (Collectively these activities were designated by the NSA code-name "STELLARWIND".)

A. ~~(TS//TSP//SI//OC/NF)~~ *Basket 1 – Content Collection*: The first presidentially-authorized activity after the 9/11 attacks was the collection of the content[4] of certain international communications (telephone and Internet) reasonably believed to involve a member of a terrorist organization. From the outset this activity was limited by the NSA to "one-end international" communications – that is, to or from the United States. This content collection activity was directed at groups engaged in international terrorism and, starting March 2004, was limited to international communications reasonably believed to involve an individual associated specifically with al Qaeda or its affiliated organizations. When publicly acknowledged in December 2005, this content collection activity was referred to as the "Terrorist Surveillance Program." The TSP authorization ended in February 2007 and was initially replaced by orders of the FISC, which were later supplanted by Congressional amendments to the FISA that authorized the NSA to collect certain communications of non-U.S. persons located overseas.

B. ~~(TS//TSP//SI-[redacted]//OC/NF)~~ *Basket 2 – Telephony Meta Data*: The second activity undertaken by the NSA after the 9/11 attacks, pursuant to the same presidential authorization, entailed the bulk collection of telephony "meta data" -- which is information derived from call detail records that reflects, but is not limited to, the date, time, and duration of telephone calls, as well as the phone numbers used to place and receive the calls. As described below, this activity was transitioned to an order of the FISC starting in May 2006 and, while subject to subsequent modification by the FISC, remains in place today.

C. ~~(TS//TSP//SI-[redacted]//OC/NF)~~ *Basket 3 – Internet Meta Data*: The third activity undertaken by the NSA after the 9/11 attacks, again pursuant to the same presidential authorization, was the bulk collection of Internet meta data, which is header/router/addressing information, such as the "to," "from," "cc," and "bcc" lines on an email, as opposed to the content or subject lines of a standard email. As described below, this activity was transitioned to an order of the FISC starting in July 2004 until December 2011, when NSA decided not to seek reauthorization of this activity.[5]

---

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

[4] ~~(TS//SI//OC/NF)~~ 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 opposed to the type of addressing or routing information referred throughout this declaration as "meta data."

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

6. ~~(TS//TSP//SI//OC/NF)~~ Plaintiffs' allegations put at issue all three NSA activities originally authorized by the President after the 9/11 attacks and later transitioned to FISA authority. For example, plaintiffs in both the *Jewel* and *Shubert* actions allege that the NSA was authorized by the President to engage in a communications "dragnet" after 9/11 that included the indiscriminate collection of the content of millions of telephony and Internet communications. *See Jewel* Compl. ¶¶ 7, 9, 73, 74, 81; *Shubert* SAC ¶¶ 7, 70, 84. This allegation of a *content* "dragnet" is false, however. The NSA's collection of the content of communications (*i.e.*, the substance, meaning or purport of the communication) under the post 9/11 presidential authorization was directed at one-end international communications in which a participant was reasonably believed to be associated with a group engaged in international terrorism (later limited to al Qaeda and its affiliates), and was focused on specific "selectors" (such as phone numbers and Internet addresses) believed to be associated with such individuals. The content surveillance authorized therefore did not constitute the kind of "dragnet" collection of the content of millions of Americans' telephone or Internet communications that the plaintiffs allege. Indeed, as set forth below [redacted] However, the operational details of the TSP and other NSA content collection activities could not be disclosed to address, disprove, or otherwise litigate the plaintiffs' allegation of a content "dragnet" without causing exceptional harm to NSA's sources and methods of gathering intelligence---including methods currently used to detect and prevent further terrorist attacks under the authority of the FISA.

7. ~~(TS//TSP//SI//OC/NF)~~ Similarly, plaintiffs' allegations that the NSA has collected certain non-content information (*i.e.*, meta data) about telephone and Internet

[redacted]

communications cannot be addressed without risking or requiring disclosure of highly sensitive sources and methods that continue to be utilized today and causing exceptionally grave damage to national security. As explained below, the bulk collection of meta data enables highly sophisticated analytical tools that can uncover the contacts [redacted] of members or agents of [redacted].[6]

8. ~~(TS//TSP//SI [redacted]//OC/NF)~~ In addition, plaintiffs' allegation that telecommunications carriers, including AT&T (at issue in *Jewel*) and Verizon (at issue in *Shubert*), and other carriers at issue in other lawsuits in *In re NSA Telecommunications Record Litigation*, assisted the NSA in alleged intelligence activities cannot be confirmed or denied without risking exceptionally grave damage to national security. Because the NSA has not undertaken the alleged "dragnet" collection of communications content, no carrier has assisted in that alleged activity. [redacted]

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

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

[redacted]

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

[redacted]

11. ~~(TS//TSP//SI-[redacted]//OC/NF)~~ For the foregoing reasons, detailed further

below, the DNI's state secrets and statutory privilege assertions, and my own statutory privilege assertion on behalf of the NSA, seek to protect against the disclosure of the highly classified intelligence sources and methods put at issue in this case, including: (1) any information that would tend to confirm or deny whether particular individuals, including the named plaintiffs, have been subject to the alleged NSA intelligence activities; (2) information concerning NSA intelligence sources and methods, including facts demonstrating that the content collection under the TSP was limited to terrorist-related international communications, and that NSA did not and does not otherwise engage in plaintiffs' alleged content surveillance "dragnet"; (3) facts that would tend to confirm or deny the other intelligence activities authorized by the President after 9/11 and later transitioned to the authority of the FISA – that is, existence of the NSA's bulk meta data collection, and any information about those activities; and (4) the fact that [redacted] In particular, the fact that there has been public speculation about alleged NSA activities, including in media reports, books, or plaintiffs' declarations, does not diminish the need to protect intelligence sources and methods from further exposure. The process of sorting out what is true, partly true, or wholly false in public reports or in plaintiffs' allegations and declarations, would necessarily risk or require disclosure of what in fact the NSA has undertaken, when, how, and under what authority. As set forth herein, such official confirmation and disclosure of classified privileged national security information by the Government would remove any doubt as to NSA's actual sources and methods, confirm to our adversaries what channels of communication to avoid, and cause exceptionally grave damage to the national security. For these reasons, as set forth further below, I request that the Court uphold the DNI's state secrets and statutory privilege assertions, as well as the NSA statutory privilege assertion that I now raise, and protect the information described in this declaration from disclosure.

III. (U) Classification of Declaration

12. ~~(S//SI//NF)~~ This declaration is classified TOP SECRET//TSP//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 Sates; "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 degree 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.[7]

13. (~~U//FOUO~~) Additionally, this declaration also 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

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

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.

14. ~~(TS//TSP//SI [redacted]//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 9/11. In this declaration, information pertaining to the STELLARWIND program is denoted with the special marking "TSP" and requires more restrictive handling.[8] Despite the December 2005 public acknowledgment of the TSP, details about the TSP program as well as the STELLARWIND program in its entirety, remain highly classified and strictly compartmented. [redacted]

[redacted]

[8] ~~(TS//TSP//SI [redacted]//OC/NF)~~ Information pertaining to the STELLARWIND program can also be denoted with the special marking "STLW." In prior declarations and briefing materials, 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]

[9] (U) [redacted]

15. **(U)** 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." The "ORCON" designator means that the originator of the information controls to whom it is released.

IV. (U) Background Information

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 communications intelligence ("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.[10]

17. ~~(TS//SI//NF)~~ Signals intelligence (SIGINT) consists of three subcategories: (1) communications intelligence (COMINT); (2) electronic intelligence (ELINT); and (3) foreign instrumentation signals intelligence (FISINT). Communications intelligence (COMINT) is defined as "all procedures and methods used in the interception of communications and the

[redacted]

[10] **(U)** Executive Order 12333, reprinted as amended in 50 U.S.C § 401 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 "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."

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] Electronic intelligence (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). Foreign instrumentation signals intelligence (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 Executive Order No. 12333, § 1.7(c)(2), as amended. In performing its SIGINT mission, 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 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) <u>September 11, 2001 and the al Qaeda Threat</u>

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 evidently the White House or the Capitol, strongly suggesting that al Qaeda's intended mission was to strike a decapitation 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). The United States also immediately began plans for a military response directed at al Qaeda's training grounds and havens in Afghanistan. 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.[11]

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 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

[11] (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.

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]

[redacted]

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

[redacted]

[redacted]

26. ~~(TS//SI//NF)~~ 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. ~~(TS//TSP//SI//OC/NF)~~ Presidentially-Authorized NSA Activities After 9/11

27. ~~(TS//TSP//SI//OC/NF)~~ As indicated above, in December 2005 then-President Bush acknowledged the existence of a presidentially-authorized NSA activity called the "Terrorist Surveillance Program" under which NSA was authorized to intercept the content of specific international communications involving persons reasonably believed to be associated with al Qaeda and affiliated terrorist organizations. As also noted, 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 Foreign Intelligence Surveillance Court ("FISC"). As described below, disclosure of the intelligence sources and methods involved in the TSP and other classified activities reasonably can be expected to cause exceptionally grave

damage to national security.

28. ~~(TS//TSP//SI//OC/NF)~~ In the extraordinary circumstances after the 9/11 attacks ---when the Intelligence Community believed further catastrophic attacks may be imminent--- the President directed the NSA to address important gaps in its intelligence collection activities, and to undertake further measures to detect and prevent future attacks. Starting in October 2001 and continuing with modifications, the President authorized NSA to undertake three activities.[12] While these activities were distinct in nature, they were designed to work in tandem to meet the threat of another mass casualty terrorist attack by enabling NSA to not only intercept the content of particular terrorist communications, but to identify other phone numbers and email addresses with which a terrorist had been in contact – and thus, potentially, to identify other individuals who may be involved in plotting terrorist attacks.[13]

1. ~~(TS//TSP//SI//OC/NF)~~ Basket 1 – Telephony and Email Content Collection

29. ~~(TS//TSP//SI//OC/NF)~~ First, the NSA was authorized by the President to intercept the content[14] of certain telephone and Internet communications for which there were reasonable grounds to believe that such communications originated or terminated outside the United States. [redacted]

[12] ~~(TS//SI//OC/NF)~~ In other lawsuits in *In re NSA Telecommunications Records Litigation*, some plaintiffs allege that NSA commenced the particular presidentially-authorized intelligence activities put at issue in the allegations *prior* to the 9/11 attacks. The activities described herein were authorized by the President *after* the 9/11 attacks.

[13] ~~(S//NF)~~ Each Presidential authorization (with the exception of the first such authorization) was supported by a threat assessment memorandum signed by the Director of Central Intelligence until 2005 and thereafter by the Director of National Intelligence, which documented the current threat to the U.S. homeland and to U.S. interests abroad from al Qaeda and affiliated terrorist organizations. The DNI has separately asserted privilege in order to prevent the disclosure of classified al Qaeda threat information.

[14] ~~(TS//SI//OC/NF)~~ 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), as distinguished from the type of addressing or routing information referred throughout this declaration as "meta data."

[redacted] Thus, the initial scope of the authorization permitted NSA to intercept communications where a communicant was not only reasonably believed to be a member or agent of al Qaeda and affiliated organizations, but of other international terrorist organizations as well [redacted] Starting in March 2004, the presidential authorization for content collection was limited to the collection of international communications where a party to such communication was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization. The existence of this activity was disclosed by then-President Bush in December 2005 and subsequently referred to as the "Terrorist Surveillance Program" ("TSP"). The first presidential authorization of the TSP was on October 4, 2001, and the TSP was reauthorized approximately every 30-60 days throughout the existence of the program.[15]

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

[15] ~~(TS//TSP//SI//OC/NF)~~ The specific wording of the presidential authorizations evolved over time and during certain periods authorized other activities (this declaration is not intended to and does not fully describe the authorizations and the differences in those authorizations over time). For example, as already noted, the documents authorizing the TSP also contained the authorizations for the meta data activities described herein [redacted]

[redacted]

31. ~~(TS//TSP//SI//OC/NF)~~ 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 Foreign Intelligence Surveillance Act in 1978 meant that 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). 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] the FISA did limit NSA's ability to collect "one-end" telephone or Internet international communications *to or from* the United States on a wire inside the United States.

[redacted]

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

32. ~~(TS//TSP//SI//OC/NF)~~ 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 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. 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 [redacted] individual applications for FISA Court authorization on a large number of rapidly changing selectors.[17]

33. ~~(TS//TSP//SI//OC/NF)~~ Accordingly, after the 9/11 attacks, the President directed the NSA immediately to correct the gap in collecting the content of international communications from known or suspected foreign terrorists to or from the United States. As described below, Congress subsequently agreed to certain amendments to the FISA to address this collection gap and grant NSA flexibility to collect quickly on overseas, non-U.S. person

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

targets without individual FISC orders. Thus, sources and methods by which the NSA intercepted the content of information under the TSP are still utilized today under similar FISA authority and remain highly sensitive and classified information concerning the means by which the NSA may obtain significant foreign intelligence information, including, but not limited, to terrorist threats.

2. ~~(TS//TSP//SI//OC/NF)~~ Basket 2 – Bulk Telephony Meta Data Collection

34. ~~(TS//TSP//SI [redacted] //OC/NF)~~ The second discrete NSA activity authorized by the President, again pursuant to the same presidential authorization, was the bulk collection of meta data related to *telephony* communications. As noted, telephony meta data is information derived from call detail records that reflect non-content information such as, but not limited to, the date, time, and duration of telephone calls, as well as the phone numbers used to place and receive the calls.[18] The purpose of collecting telephony meta data in bulk is to query this information with particular "selectors" (*i.e.* phone numbers) reasonably believed to be associated with a member or agent of al Qaeda or affiliated terrorist organization in order to ascertain other contacts and patterns of communications for that selector. Thus, while the amount of telephony meta data obtained through the bulk collection under presidential authorization was significant,

[redacted]

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

only a tiny fraction of telephony meta data records collected by the NSA has actually been presented to a trained professional for analysis.[19] However, the collection of meta data in bulk is necessary to utilize sophisticated and vital analytical tools for tracking the contacts [redacted] of al Qaeda and its affiliates. Again, the particular sources and methods by which the NSA collects and analyzes telephony meta data remain in use today pursuant to authority of the FISA and Executive Order 12333, and constitute highly significant tools for detecting and preventing terrorist attacks and thus for protecting national security.

3. ~~(TS//TSP//SI//OC/NF)~~ Basket 3 – Bulk Internet Meta Data Collection

35. ~~(TS//TSP//SI [redacted]//OC/NF)~~ The third discrete NSA activity authorized by the President, again pursuant to the same presidential authorization, was the NSA collected bulk meta data related to Internet communications--- header/router addressing information, such as the "to," "from," "cc," and "bcc" lines, as opposed to the content or subject lines, of a standard email.[20] In addition to collecting the content of particular communications [redacted], NSA also obtained in bulk Internet meta data [redacted].[21] As with telephony meta

[19] ~~(TS//TSP//SI//OC/NF)~~ NSA estimates that by the end of 2006, only [redacted] of the telephony meta data collected had actually been retrieved for analysis.

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

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

data. NSA would then query the bulk Internet meta data with particular "selectors" (*e.g.* email address) reasonably believed to be associated with a member or agent of al Qaeda or affiliated terrorist organization in order to ascertain other contacts [redacted] of Internet communications for that selector (and thus, again, only a tiny fraction of Internet meta data collected was viewed by an analyst). [redacted]

[redacted]

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

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

[redacted]

D. ~~(TS//SI//OC/NF)~~ Current NSA Activities Transitioned from Presidential Authority

37. ~~(TS//TSP//SI//OC/NF)~~ The three sources and methods of intelligence collection initially authorized by the President immediately following 9/11 have evolved over the last eleven years and continue to be utilized today. Thus, disclosure of the particular sources and methods described herein as they were utilized under presidential authorization would compromise the use of those sources and methods under other authority and thereby risk exceptionally grave damage to national security.

1. ~~(TS//SI//OC/NF)~~ Collection of Communication Content

38. ~~(TS//TSP//SI//OC/NF)~~ First, in January of 2007, the content interception activities that had been occurring under the TSP were transitioned to authority of the FISA.[22] Specifically, on January 10, 2007, the FISC issued orders authorizing the Government to conduct certain electronic surveillance that had been occurring under the TSP. Those orders included: [redacted] the "Foreign Telephone and Email Order," which authorized electronic surveillance of telephone and Internet communications [redacted] where the Government determined that there was probable cause to believe that (i) one of the communicants is a member or agent of [redacted]

[22] ~~(TS//SI//OC/NF)~~ This declaration generally describes the transition of all three Presidentially-authorized activities to FISA authority, but does not describe in detail the FISC Orders themselves, the details of their periodic renewal, specific legal issues that arose, the process involved in obtaining FISC approval, continual briefings to the various congressional oversight committees, or any subsequent compliance issues and corrective action taken as a result of those incidents. The FISC undertakes close oversight of NSA activities that are subject to the FISA, and NSA has worked extensively to ensure compliance with FISC orders, including those described herein.

[redacted]; and (ii) the communication is to or from a foreign country (*i.e.*, a one-end foreign communication to or from the United States). Thereafter, any electronic surveillance, as that term is defined in the FISA (*see* 50 U.S.C. § 1801(f)), that was occurring as part of the TSP became subject to the approval of the FISA Court and the TSP was not reauthorized.[23]

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

[redacted]

[23] (U) On January 17, 2007, the Attorney General made public the general facts that new orders of the Foreign Intelligence Surveillance Court had been issued that authorized the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization; that, as a result of these orders, any electronic surveillance that had been occurring as part of the TSP was then being conducted subject to the approval of the FISA Court; and that, under these circumstances, the TSP was not reauthorized.

[24] ~~(TS//SI//OC/NF)~~ [redacted] the January 2007 FISC Foreign Telephone and Email Order authorized NSA to intercept the content of communications of [redacted]

[redacted]

40. ~~(TS//SI//OC/NF)~~ The process of seeking renewal of the January 2007 FISC Foreign Telephone and Email Order after its original 90 day authorization ultimately led the Executive Branch to press for and Congress to enact amendments to the FISA that granted NSA greater flexibility to collect the content of international communications without the need for individual FISC orders for each selector targeted. [redacted]

[redacted]

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

[redacted] As discussed next, this prompted NSA to seek additional statutory authority under the FISA to intercept the content of international communications [redacted] inside the United States.

41. ~~(TS//TSP//SI//OC/NF)~~ In August 2007, Congress enacted the Protect America Act ("PAA"), which granted NSA additional flexibility under the FISA to target international communications without an individual court order for each selector. Under the PAA, the FISA's definition of "electronic surveillance" was clarified to *exclude* "surveillance directed at a person reasonably believed to be located outside the United States" 50 U.S.C. § 1805A. This change in the definition of electronic surveillance under the FISA permitted the NSA to intercept communications off of a wire inside the United States without an individual court order 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 TSP. The PAA eliminated the need for the Foreign Telephone and Email Order, and that Order expired after the PAA was enacted.

42. ~~(TS//SI//OC/NF)~~ The PAA authorized the DNI and the Attorney General to jointly "authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States" for up to one year. *id.* § 1805B(a), and to issue directives to communications service providers requiring them to "immediately provide the

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

Government with all information, facilities, and assistance necessary to accomplish the acquisition" of necessary intelligence information. *id.* § 1805B(e). Such directives were issued to a number of telecommunication and internet service providers, and the NSA conducted content surveillance of overseas targets under the PAA with the assistance of those telecommunication carriers. More specifically, in August 2007, the Attorney General and DNI issued the requisite certifications, and, among other things, content collection under the PAA continued as to persons reasonably believed to be outside the United States involving communications of . Under the PAA, approximately foreign selectors that had been authorized under the Foreign Telephone and Email Order were transitioned to collection by NSA under authority of the PAA.

43. ~~(TS//SI//OC/NF)~~ The PAA was enacted as a temporary measure set to expire in 180 days, and it ultimately did expire on February 16, 2008 (although directives issued under the PAA continued in effect until their stated expiration dates). On July 11, 2008, the Foreign Intelligence Surveillance Act Amendments Act of 2008 (FAA) was signed into law. Section 702 of the FAA created new statutory authority and procedures that permitted the targeting of non-United States persons reasonably believe to be outside of the United States without individual FISC orders but subject to directives issued to telecommunications carriers by the Director of National Intelligence and the Attorney General under Section 702(h) of the FISA for the continuation of overseas surveillance under this new authority. *See* 50 U.S.C. § 1881a(h) (as added by the FISA Act of 2008, P.L. 110-261). Directives that had been issued under the PAA for content surveillance of overseas targets (including surveillance of specific targets overseas) were thus replaced by new directives for such surveillance issued pursuant to the FAA. While the existence of prior PAA authority and current FAA authority are set forth in public

statutory provisions, the operational details of the sources and methods used by NSA to carry out that authority remain highly classified.

44. ~~(TS//TSP//SI//OC/NF)~~ As with the TSP, the purpose of the new authority in Section 702 of the FAA was to account for changes in communications technology since 1978 whereby international communications were increasingly transmitted to the United States via fiber optic cable and, consequently, increasingly subject to FISA's definition of electronic surveillance and requirements. By granting NSA the authority to conduct acquisitions inside the United States by targeting non-United States persons located outside the United States in order to acquire foreign intelligence information without the need for individualized FISC orders approving surveillance for each individual target, Section 702 permitted the NSA to continue to undertake content surveillance for overseas targets in a manner similar to that permitted under the TSP. As of August 2012, NSA presently has a total of approximately [redacted] individual foreign selectors under coverage pursuant to Section 702 of the FAA. Section 702 has proven to be a critical tool in the Government's efforts to acquire significant foreign intelligence necessary to protect the Nation's security and has quickly become one of the most important legal authorities available to the Intelligence Community.

45. ~~(TS//TSP//SI//OC/NF)~~ In sum, the post 9/11 content surveillance activities undertaken by the NSA evolved from the presidentially authorized TSP to the FISC Foreign Telephone and Email Order, to the directives issued under the PAA and, ultimately, to the directives that are now being issued pursuant to the FISA Amendments Act of 2008. Each authorization sought to enable the NSA to undertake content surveillance on numerous multiple targets overseas without the need to obtain advance court approval for each target. But, as explained further below, none of these content surveillance activities has entailed the kind of indiscriminate "dragnet" content surveillance of domestic or international telephony or Internet

communications that the plaintiffs allege. Rather, from the outset, content collection by the NSA has focused on international communications reasonably believed to involve terrorist organizations [redacted].

2. ~~(TS//SI//OC/NF)~~ Collection of Bulk Telephony Meta data (Business Records)

46. ~~(TS//TSP//SI-[redacted]//OC/NF)~~ As set forth above, the second activity authorized by then-President Bush after the 9/11 attacks was the bulk collection of meta data related to telephony communications --- again, information derived from call detail records that reflect non-content information such as, but not limited to, the date, time and duration of telephone calls, as well as the phone numbers used to place and received the calls. That activity, which began pursuant to Presidential authorization in October 2001, continues today under the authority of the FISA.

47. ~~(TS//TSP//SI//OC/NF)~~ Beginning in May 2006, the bulk collection of non-content telephony meta data, previously subject to Presidential authorization, was authorized by the FISC pursuant to what is known as the Telephone Business Records Order. The FISC found that, in order to protect against international terrorism, reasonable grounds existed to order certain telecommunication carriers to produce to the NSA in bulk "call detail records" or "telephony meta data," pursuant to 50 U.S.C. § 1861(c) (authorizing the production of business records for, inter alia, an investigation to protect against international terrorism). While this bulk collection is again very broad in scope, the NSA has been authorized by the FISC to query the archived telephony data solely with identified telephone numbers for which there are facts giving rise to a reasonable, articulable suspicion that that the number is associated with (among other foreign targets) [redacted] (referred to as a "RAS" determination). Bulk telephony meta data collection, as continued to be authorized under FISA authority, remains a vital source and method needed to utilize sophisticated analytical tools for

tracking [redacted] contacts of [redacted].

3. ~~(TS//SI//OC/NF)~~ Collection of Bulk Internet Meta data

48. ~~(TS//TSP//SI//OC/NF)~~ As also described above, the third activity authorized by then-President Bush after the 9/11 attacks was the bulk collection of meta data related to Internet communications. NSA carried out this bulk collection activity under presidential authorization [redacted] During the period from [redacted] 2004, an application was prepared and submitted to the FISC to continue the bulk collection of Internet meta data. In July 2004, the FISC authorized the bulk collection of Internet meta data through the use of a pen register and trap and trace device ("FISC Pen Register Order" or "PRTT Order"). *See* 50 U.S.C. § 1841, *et seq.* (defining "pen register" and "trap and trace device").

49. ~~(TS//SI//OC/NF)~~ Initially, under the PRTT Order, NSA was authorized to collect, in bulk, meta data associated with electronic communications [redacted] in a manner similar to that which NSA had utilized under presidential authorization. Specifically, the collection of Internet meta data [redacted] had been authorized because [redacted] In addition, while NSA was authorized to collect Internet meta data in bulk [redacted], it was permitted to query the archived meta data only using Internet selectors for which there were facts giving rise to a reasonable, articulable suspicion that the email address was associated with [redacted]. As with bulk collection of telephony meta data collection, the bulk collection of Internet meta data allowed the NSA to use critical and unique analytical capabilities to track the contacts (even retrospectively) [redacted] of

known terrorists.

50. ~~(TS//SI//OC/NF)~~ The FISC Pen Register Order was reauthorized approximately every 90 days from July 2004 until December 2011.[27] In December 2011, NSA did not seek reauthorization of the PRTT Order after concluding that this activity was too limited in scope to justify further resources. [redacted] Thus, the disclosure of this source and method would compromise NSA's current collection activities and analytical capabilities and cause

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

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

exceptionally grave damage to the national security of the United States.

51. ~~(TS//TSP//SI//OC/NF)~~ The *Jewel* and *Shubert* plaintiffs allege that, in March 2004, the Acting Attorney General of the Department of Justice refused to reauthorize certain aspects of the activities authorized by the President after the 9/11 attacks. *See Jewel* Compl. ¶¶ 45-49; *Shubert* SAC ¶ 97-99. I was not the Executive Director of NSA in March 2004, nor was I personally involved in the matter at issue, and this declaration does not describe the full details of this dispute [redacted]

[redacted]

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

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

[redacted]

V. (U) Information Subject to DNI and NSA Privilege Assertions

52. ~~(TS//TSP//SI//OC/NF)~~ As the foregoing discussion indicates, a wide range of intelligence sources and methods, used over the past decade and still in use today, are at risk of disclosure in this lawsuit. While the plaintiffs' allegations are focused on the period immediately following 9/11, and seek to challenge alleged activities undertaken pursuant to presidential authorization, the sources and methods used by NSA at that time continue to be used under subsequent authorizations. To expose a source and method, based on its use during one period of time, under one authority, would compromise, if not destroy, NSA's ability to use that method today. All of the presidentially authorized activities being challenged in this lawsuit (starting in July 2004) were placed under other FISA authority and have been subject to Congressional oversight. The need to protect these sources and methods continues to exist notwithstanding plaintiffs' challenge to the lawfulness of their use under presidential authorization.

53. ~~(TS//TSP//SI//OC/NF)~~ Accordingly, the NSA seeks to protect from disclosure in this case the sources and methods its has utilized to undertake (i) content surveillance under the TSP, including information needed to demonstrate that the TSP was not the content "dragnet" plaintiffs allege; (ii) bulk collection of telephony meta data; (iii) bulk collection of Internet meta data, including the analytical tools for querying such data to detect terrorist contacts; (iv) facts concerning whether any NSA surveillance activities have been directed at or collected any

[redacted]

information concerning the plaintiffs (which would risk disclosure of the existence and scope of the source and methods at issue); and (v) [redacted]

54. **(U)** In general and unclassified terms, the following categories of information are subject to the DNI's assertion of the state secrets privilege and statutory privilege under the National Security Act, as well as my assertion of the NSA statutory privilege:

A. **(U)** Information that may tend to confirm or deny whether the plaintiffs have been subject to any alleged NSA intelligence activity that may be at issue in this matter; and

B. **(U)** 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 also collects the communication records of millions of Americans as part of an alleged "Program" authorized by the President after 9/11. *See, e.g.*, *Jewel* Comp. ¶¶ 2-13; 39-97; *Shubert* SAC ¶¶ 1-9; 57-58; 62-91.

The scope of this assertion includes but is not limited to:

(i) **(U)** Information concerning the scope and operation of the now inoperative "Terrorist Surveillance Program" ("TSP") regarding the interception of the content of certain one-end international communications reasonably believed to involve a member or agent of al-Qaeda or an affiliated terrorist organization, and any other information related to demonstrating that the NSA does not otherwise engage in the content surveillance "dragnet" that the plaintiffs allege; and

(ii) **(U)** Information concerning whether or not the NSA obtained from telecommunications companies such as AT&T and Verizon communication transactional records as alleged in the Complaint; *see, e.g.*, *Jewel* Complaint ¶¶ 10; 82-97; *Shubert* SAC ¶ 102; and

(iii) **(U)** Information that may tend to confirm or deny whether AT&T, Verizon (and to the extent relevant or

necessary, any other telecommunications carrier), have provided assistance to the NSA in connection with any alleged activity; *see, e.g., Jewel* Complaint ¶¶ 2, 7-8, 10; 13 50-97; *Shubert* SAC ¶¶ 6, 10-13; 66-68.

VI. (U) Harm of Disclosure of Privileged Information

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

55. **(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, disclosure of such information would cause exceptionally grave damage to the national security.

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

56. ~~(TS//TSP//SI//OC/NF)~~ The named plaintiffs in the *Jewel*[31] and *Shubert*[32] cases allege that content of their own telephone and Internet communications have been and continue to be subject to unlawful search and seizure by the NSA, along with the content of communications of millions of ordinary Americans.[33] As set forth herein, the NSA does not

---

[31] (U) According to the Complaint, named plaintiffs in the *Jewel* case are Tash Hepting, Gregory Hicks, Carolyn Jewel, Erik Knutzen, and Joice Walton.

[32] (U) According to the Second Amended Complaint, the named plaintiffs in the *Shubert* case are Virginia Shubert, Noha Arafa, Sarah Dranoff, and Hilary Botein.

[33] (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 acquire the content of phone calls, emails, instant messages, text messages, 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* Complaint ¶¶ 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.

engage in "dragnet" surveillance of the content of communications as plaintiffs allege [redacted]

[redacted]

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

[redacted]

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

[redacted]

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

57. ~~(TS//TSP//SI//OC/NF)~~ Further, the named plaintiffs in *Jewel* and *Shubert* allege that the NSA has been and is continuing to collect 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.[36]

[redacted]

[36] (U) Specifically, the *Jewel* plaintiffs allege that 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* Complaint ¶¶ 7, 10, 11, 13, 82-97. 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.

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

[38] ~~(TS//TSP//SI//OC/NF)~~ During the time period covered by the Presidential Authorizations, NSA estimated that it collected Internet meta data associated with approximately [redacted]

[redacted]

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

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

[redacted]

59. (U) As a matter of course, the NSA cannot publicly confirm or deny whether any individual is subject to surveillance activities because to do so would tend to reveal actual targets. For example, if the NSA were to confirm in these two cases and others that specific individuals are not targets of surveillance, but later refuse to comment (as it would have to) in a case involving an actual target, an actual or potential adversary of the United States could easily deduce by comparing such responses that the person in the latter case is a target. The harm of revealing targets of foreign intelligence surveillance should be obvious. If an individual knows or suspects he is a target of U.S. intelligence activities, he would naturally tend to alter his behavior to take new precautions against surveillance. In addition, revealing who is not a target would indicate who has avoided surveillance and what may be a secure channel for communication. Such information could lead an actual or potential adversary, secure in the

[redacted] At the time the bulk collection of Internet meta data pursuant to orders of the FISC (the PRTT Order) expired in December 2011, NSA estimates that the percentage of Internet meta data that it collected had been reduced to approximately [redacted] With respect to telephony meta data, NSA has previously estimated that, prior to the 2006 FISC Order, about [redacted] telephony meta data records was presented to an analyst for review.

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

knowledge that he is not under surveillance, 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 hostile 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.[40]

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

[redacted]

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

[redacted]

B. (U) **Information Related to NSA Activities, Sources, or Methods Implicated by Plaintiffs' Allegations of a Communications "Dragnet"**

61. (U) I am also supporting the DNI's assertion of privilege and asserting the NSA's statutory privilege over any other 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) that 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: (1) information concerning the now inoperative "Terrorist Surveillance Program" 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 the plaintiffs allege; and (2) information concerning whether or not the NSA obtains transactional communications records from telecommunications companies. As set forth below, the disclosure of such information would cause exceptionally grave damage to national security.

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

62. (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,[41] plaintiffs' allegation that the NSA has undertaken indiscriminate surveillance of the content[42] of millions of communications sent or received by people inside the United States after 9/11 under the TSP is false. But 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 methods about the operation of the TSP and current NSA intelligence activities 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 communications that are not subject to NSA activities – in either case risking exceptionally grave damage to national security.

---

[41] (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).

[42] (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).

(a) (U) Information Related to the Terrorist Surveillance Program

63. **(U)** First, a range of operational details concerning the Terrorist Surveillance Program remains properly classified and privileged from disclosure, and could not be disclosed to address plaintiffs' content "dragnet" allegations including the following TSP-related information.

64. ~~(TS//TSP//SI//OC/NF)~~ First, interception of the content of communications under the TSP was triggered by a range of information, including sensitive foreign intelligence, obtained or derived from various sources, indicating that a particular phone number or email address was reasonably believed by the U.S. Intelligence Community to be associated with a member or agent of al Qaeda or an affiliated terrorist organization. Professional intelligence officers at the NSA undertook a careful but expeditious analysis of that information, and considered a number of possible factors, in determining whether it would be appropriate to target a telephone number or Internet selectors under the TSP. Those factors included whether the target phone number or email address was: (1) reasonably believed by the U.S. Intelligence Community, based on other authorized collection activities or other law enforcement or intelligence sources, to be used by a member or agent of al Qaeda or an affiliated terrorist organization: [redacted]

[redacted]

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

[redacted]

65. ~~(TS//TSP//SI//OC/NF)~~ Once the NSA determined that there were reasonable grounds to believe that the target was a member or agent of al Qaeda or an affiliated terrorist organization, the NSA took steps to focus the interception on the specific al Qaeda-related target and on communications of that target that were to or from a foreign country. In this respect, the NSA's collection efforts were [redacted] that the NSA had reasonable grounds to believe carry the "one-end foreign" communications of members or agents of al Qaeda or affiliated terrorist organizations.

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

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

[redacted]

[redacted]

68. ~~(TS//TSP//SI//OC/NF)~~ The NSA took specific steps in the actual TSP interception process to minimize the risk that the communications of non-targets were intercepted. With respect to telephone communications, specific telephone numbers identified through the analysis outlined above were [redacted] so that 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.

---

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

69. ~~(TS//TSP//SI//OC/NF)~~ 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 only 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 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.[45]

70. ~~(TS//TSP//SI//OC/NF)~~ In addition to procedures designed to ensure that the TSP was limited to the international communications of al Qaeda members and affiliates, the NSA

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

also took additional steps to ensure that the privacy rights of U.S. persons were protected. [redacted]

[redacted]

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

[redacted]

[46] ~~(TS//TSP//SI//OC/NF)~~ In addition, in implementing the TSP, the NSA was directed by the President to minimize the 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 President further directed that any failure to adhere to the provisions of the authorizations should be reported to the President. Accordingly, NSA applied its existing Legal Compliance and Minimization Procedures applicable to U.S. persons to the extent not inconsistent with the presidential authorization. *See* United States Signals Intelligence Directive (USSID) 18. These procedures require that the NSA refrain from intentionally acquiring the communications of U.S. persons who are not the targets of its surveillance activities, that it destroy upon recognition any communications solely between or among persons in the U.S. that it inadvertently acquires, and that it minimize all U.S. person identities in intelligence reporting unless a senior NSA official determines upon individual request that the recipient of the report requires such information in order to perform a lawful function assigned to it and the identity of the U.S. person is necessary to understand the foreign intelligence or to assess its significance.

[redacted]

[redacted] The foregoing information about the targeted scope of content collection under the TSP could not be disclosed, in order to address and rebut plaintiffs' allegation that the NSA, with the assistance of AT&T and Verizon, engaged in the alleged content "dragnet," without revealing specific NSA sources and methods and thereby causing exceptionally grave damage to the national security

(b) ~~(TS//SI//OC/NF)~~ Information Related to Content Surveillance Under Other Authority

72. ~~(TS//TSP//SI-[redacted]//OC/NF)~~ In addition to the foregoing facts about the TSP, information concerning other NSA intelligence activities, sources, and methods would be at risk of disclosure or required to address allegations or prove that there has been no "dragnet" program authorized by the President after 9/11 under which the NSA intercepts the content of virtually all domestic and international communications as the plaintiffs allege. [redacted]

[redacted]

[redacted]

73. ~~(TS//SI//OC/NF)~~ In addition, as outlined above, the content surveillance activities authorized under the TSP were transitioned in January 2007 to FISC-authorized electronic surveillance under Title I of the FISA and then, subsequently, to the Protect America Act of 2007, and then ultimately under Section 702 of the FISA Amendments Act of 2008.[47] Again, while the statutory authority is publicly known, the operational details of the surveillance activities remain highly classified. NSA continues to utilize sources and methods for content surveillance similar to that utilized under the TSP whereby the content of international telephone and Internet communications are captured at [redacted]

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

[redacted] by targeting [redacted] selectors reasonably believed to be associated with terrorist targets, including [redacted]. Disclosure of particular sources and methods utilized under the TSP, in order to litigate plaintiffs' "dragnet" allegations under presidential authorization, would compromise the use of similar sources and methods today. And disclosure of these sources and methods as currently utilized, in order to demonstrate there is no *ongoing* surveillance "dragnet," as alleged, would likewise compromise vital intelligence collection operations under FISA and other authority and, again, cause exceptionally grave damage to current efforts to detect and prevent terrorist attacks.[48]

2. (U) Plaintiffs' Allegations Concerning the Collection of Communication Records

74. (U) Plaintiffs also allege that the NSA is collecting the private telephone and Internet transaction records of millions of Americans, again including information concerning the plaintiffs' telephone and Internet communications. *See, e.g., Jewel* Complaint ¶¶ 7, 10, 11, 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.

75. ~~(TS//SI//OC/NF)~~ In addition to implicating the NSA's content collection activities authorized after the 9/11 attacks, the plaintiffs' allegations put directly at issue the

---

[48] ~~(TS//SI//OC/NF)~~ To the extent relevant to this case, additional facts about the operational details of the TSP and subsequent FISA authorized content surveillance activities could not be disclosed without causing exceptionally grave damage to national security, including for example information that would demonstrate the operational swiftness and effectiveness of utilizing content surveillance in conjunction with the bulk meta data collection activities. [redacted] the TSP, in conjunction with meta data collection and analysis described herein, allowed the NSA to obtain rapidly not only the content of a particular communication, but connections between that target and others who may form a web of al Qaeda conspirators.

NSA's bulk collection of non-content communication meta data. As explained above, the NSA has not engaged in the alleged "dragnet" of communication *content*, and to address plaintiffs' allegations concerning the bulk collection of *non-content* information would require disclosure of NSA sources and methods that would cause exceptionally grave damage to national security.

[redacted]

76. ~~(TS//SI//OC/NF)~~ The bulk meta data collection activities that have been undertaken by the NSA since 9/11 are vital tools for protecting the United States from another catastrophic terrorist attack. Disclosure of these meta data activities, sources, or methods would cause exceptionally grave damage to national security. It is not possible to target collection solely on known terrorist telephone identifiers and effectively discover the existence, location, and plans of terrorist adversaries. [redacted]

[redacted] Meta data collection and analysis provides a vital and effective capability to keep track of such operatives.

77. ~~(TS//SI//OC/NF)~~ In particular, the bulk collection of Internet and telephony meta data allows the NSA to use critical and unique analytical capabilities to track the contacts [redacted] of members or agents of [redacted] through the use of two highly sophisticated tools known as "contact-chaining" and [redacted] Contact-chaining allows the NSA to identify telephone numbers and email addresses that have been in contact with known [redacted] numbers and addresses; in turn, those contacts can be targeted for immediate query and analysis as new [redacted] numbers and addresses are identified. When the NSA performs a contact-chaining query on a terrorist-associated telephone identifier, [redacted]

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

[redacted]

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

[redacted]

80. ~~(TS//SI [redacted] //OC/NF)~~ Because it is impossible to determine in advance which particular piece of meta data will turn out to identify a terrorist, collecting meta data in *bulk* is vital for the success of contact-chaining [redacted]. NSA analysts know that the terrorists' telephone calls are located somewhere in the billions of data bits; what they cannot know ahead of time is exactly where. The ability to accumulate meta data substantially increases NSA's ability to detect and identify these targets. One particular advantage of bulk meta data collection is that it provides a historical perspective on past contact activity that cannot be captured in the present or prospectively. Such historical links may be vital to identifying new targets, because the meta data may contain links that are absolutely unique, pointing to potential

targets that otherwise would be missed. [redacted]

[redacted]

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

[redacted] These sources and methods enable the NSA to segregate some of that very small amount of otherwise undetectable but highly valuable information from the overwhelming amount of other information that has no intelligence value whatsoever—in colloquial terms, to find at least some of the needles hidden in the haystack. If employed on a sufficient volume of raw data, contact chaining [redacted] can expose [redacted] and contacts that were previously unknown. [redacted]

[redacted]

82. ~~(TS//TSP//SI//OC/NF)~~ As explained above, the bulk meta data collection activities that began under presidential authorization were transitioned to the authority of the FISA in July 2004 (PRTT Order for Internet meta data collection) and May 2006 (Business Records Order for telephony meta data collection). The PRTT Order was in effect until December 2011 and the Business Records Order remains in effect. Thus, long after the presidential authorization expired, NSA continued bulk meta data collection activities under FISA authority, [redacted]

[redacted]

[redacted]

83. ~~(TS//SI//OC/NF)~~ Accordingly, adjudication of plaintiffs' allegations concerning the collection of non-content meta data and records about communication transactions would risk or require disclosure of critical NSA sources and methods for tracking [redacted] contacts of terrorist communications as well as the existence of current NSA activities under FISA [redacted] Despite media speculation about these activities, official confirmation and disclosure of the NSA's bulk collection and targeted analysis of telephony meta data would confirm to all of our foreign adversaries [redacted] the existence of these critical intelligence capabilities and thereby severely undermine NSA's ability to gather information concerning terrorist connections and cause exceptional harm to national security.

3. ~~(TS//SI//OC/NF)~~ Information Concerning Current FISA Authorized Activities and Specific FISC Orders

84. ~~(TS//TSP//SI//OC/NF)~~ I am also supporting the DNI's state secrets privilege assertion, and asserting NSA's statutory privilege, over information concerning the various orders of the Foreign Intelligence Surveillance Court mentioned throughout this declaration that authorize NSA intelligence collection activities, as well as NSA surveillance activities conducted pursuant to the now lapsed Protect America Act ("PAA") and current activities authorized by the FISA Amendments Act of 2008. As explained herein, the three NSA intelligence activities initiated after the September 11 attacks to detect and prevent a further al Qaeda attack—(i) content collection of targeted al Qaeda and associated terrorist-related communications under what later was called the TSP; (ii) internet meta data bulk collection; and (iii) telephony meta data bulk collection—have, beginning in January 2007, July 2004, and May 2006 respectively, been conducted pursuant to FISA and are no longer being conducted under presidential authorization. FISC Orders authorizing the bulk collection of non-content transactional data for internet communications commenced in the July 2004 FISC Pen Register Order and expired in December 2011, and FISC Orders authorizing the bulk collection of non-content telephony meta data commenced in May 2006 and remain ongoing. The existence and operational details of these orders remain highly classified, and disclosure of information concerning the orders would cause exceptional harm to national security by revealing the existence and nature of still sensitive intelligence sources and methods.[49] In addition, while the Government has acknowledged the

[49] ~~(TS//SI//OC/NF)~~ For this reason, the FISC Telephone Business Records Order prohibits any person from disclosing to any other person that the NSA has sought or obtained the telephony meta data, other than to (a) those persons to whom disclosure is necessary to comply with the Order; (b) an attorney to obtain legal advice or assistance with respect to the production of meta data in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. They further provide that any person to whom disclosure is made pursuant to (a), (b), or (c) shall be subject to the nondisclosure requirements applicable to a person to whom the Order is directed in the same manner as such person. The bulk Pen Register orders say that the telecommunications companies who are served with them shall not "disclose

general existence of the January 10, 2007 FISC Orders authorizing electronic surveillance similar to that undertaken in the TSP, the content of those orders, and facts concerning the NSA sources and methods they authorize, cannot be disclosed without likewise causing exceptional harm to national security. Likewise, the particular content surveillance sources and methods utilized by the NSA pursuant to the PAA and, currently, under the FISA Amendments Act of 2008, likewise cannot be disclosed. For these reasons, the privilege assertion by the DNI, and my assertion of NSA's statutory privilege, encompass the FISC Orders and the sources and methods they concern.

4. (U) Information Concerning Plaintiffs' Allegations that Telecommunications Carriers Provided Assistance to the NSA

85. (U) The final major category of NSA intelligence sources and methods as to which I am supporting the DNI's assertion of privilege, and asserting the NSA's statutory privilege, concerns information that may tend to confirm or deny whether or not AT&T and Verizon (or to the extent necessary whether or not any other telecommunications provider) has assisted the NSA with alleged intelligence activities.[50] 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 surveillance 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

---

the existence of the NSA's investigation, or the pen registers and/or trap and trace devices unless and until ordered by the Court."

[50] ~~(TS//TSP//SI [redacted]//OC/NF)~~ On September 19, 2008, then-Attorney General Mukasey submitted a classified declaration and certification to this Court authorized by Section 802 of the Foreign Intelligence Surveillance Act Amendments Act of 2008, *see* 50 U.S.C. § 1885a, [redacted]

in the alleged surveillance activities that the plaintiffs seek to challenge. Confirmation or denial of a relationship between the NSA and AT&T, Verizon, or any other telecommunication carrier on alleged intelligence activities would cause exceptionally grave damage to national security. Confirming or denying such allegations of assistance would reveal to foreign adversaries whether or not NSA utilizes particular intelligence sources and methods and, thus, either compromise actual sources and methods or reveal that NSA does not utilize a particular source and method. Such facts would allow individuals, to include America's adversaries, to accumulate information and draw conclusions about how the U.S. Government collects communications, its technical capabilities, and its sources and methods. Any U.S. Government confirmation or denial would replace speculation with certainty for hostile foreign adversaries who are balancing the risk that a particular channel of communication may not be secure against the need to communicate efficiently. Such confirmation or denial would allow adversaries to focus with certainty on a particular channel that is secure.[51]

86. (U) Indeed, 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 telecommunication carriers alleged to have assisted the NSA after the 9/11 attacks. In enacting this legislation, the Senate Select Committee on Intelligence, after extensive oversight of the Terrorist Surveillance Program, found that "electronic surveillance for law enforcement and intelligence purposes depends in

---

[51] (U) For example, if NSA were to admit publicly in response to an information request that no relationship with telecommunications companies A, B, and C exists, but in response to a separate information request about company D state only that no response could be made, this would give rise to the inference that NSA has a relationship with company D. Over time, the accumulation of these inferences would disclose the capabilities (sources and methods) of NSA's intelligence activities and inform our adversaries of the degree to which NSA can successfully exploit particular communications. Our adversaries can then develop countermeasures to thwart NSA's abilities to collect their communications.

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.*

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

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

[redacted]

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

[redacted]

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

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

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

(a) (TS//TSP//SI-[redacted]//OC/NF) [redacted]

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

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

[redacted]

[54] (TS//TSP//SI-[redacted]//OC/NF) [redacted]

[redacted]

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

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

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

[redacted]

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

[redacted]

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

[redacted]

[redacted]

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

[redacted]

[redacted]

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

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

[redacted]

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

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

[redacted]

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

[redacted]

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

[redacted]

[redacted]

[redacted]

[58] ~~(TS//TSP//S[redacted]//OC//NF)~~ [redacted]

[redacted]

[59] ~~(TS//TSP//S[redacted]//OC/NF)~~ [redacted]

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

[redacted]

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

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

[redacted]

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

[redacted]

[redacted]

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

[redacted]

[redacted]

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

[redacted]

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

VII. (U) Risks of Allowing Litigation to Proceed

112. ~~(TS//TSP//SI [redacted] //OC/NF)~~ Upon examination of the allegations, claims, facts, and issues raised by these cases, it is my judgment that sensitive state secrets are so central to the subject matter of the litigation that any attempt to proceed will substantially risk the

disclosure of the privileged state secrets described above. Although plaintiffs' alleged content surveillance "dragnet" did not and does not occur, proving why that is so, [redacted] would directly implicate highly classified intelligence information and activities. Similarly, attempting to address plaintiffs' allegations with respect to the bulk collection of non-content information and records containing transactional meta data about communications would also compromise currently operative NSA sources and methods that are essential to protecting national security, including for detecting and preventing a terrorist attack. [redacted] In my judgment, any effort to probe the outer bounds of such classified information would pose inherent and significant risks of the disclosure of that information, including critically sensitive information about NSA sources, methods, operations, targets, and relationships. Indeed, any effort merely to allude to those facts in a non-classified fashion could be revealing of classified details that should not be disclosed. Even seemingly minor or innocuous facts, in the context of these cases or other non-classified information, can tend to reveal, particularly to sophisticated foreign adversaries, a much bigger picture of U.S. intelligence gathering sources and methods.

113. ~~(TS//SI//NF)~~ The United States has an overwhelming interest in detecting and thwarting further 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. Al Qaeda and other terrorist groups continue to pursue the ability and have clearly stated an intent 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.

114. ~~(TS//SI//NF)~~ As set forth above, terrorist organizations around the world seeks 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 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.

VIII. (U) Conclusion

115. **(U)** In sum, 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 Agency Act with respect to the information described herein which concerns the functions and activities of the NSA. Moreover, because proceedings in this case risk disclosure of privileged and classified intelligence-related information, I respectfully request that the Court not only protect that information from disclosure but also dismiss this case to prevent exceptional harm to the national security of the United States.

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

DATE: 9.11.12

Frances J. Fleisch
Executive Director
National Security Agency