BETH S. BRINKMANN
Deputy Assistant Attorney General
DOUGLAS N. LETTER
Terrorism Litigation Counsel
JOSEPH H. HUNT
Director, Federal Programs Branch
VINCENT M. GARVEY
Deputy Branch Director
ANTHONY J. COPPOLINO
Special Litigation Counsel
MARCIA BERMAN
Senior Litigation Counsel
PAUL E. AHERN
Trial Attorney
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 Government Defendants

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION	No. M:06-cv-01791-VRW **CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR NATIONAL SECURITY AGENCY**
This Document Relates Solely To: *Shubert, et al. v. United States of America, et al.* (Case No. 07-cv-00693-VRW)	***EX PARTE, IN CAMERA*** Date: December 15, 2009 Time: 10:00 a.m. Courtroom 6, 17th Floor Chief Judge Vaughn R. Walker

Derived From: NSA/CSSM 1-52
Dated: 20091030
Declassify On: 20341030

(U) **Table of Contents**

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER NATIONAL SECURITY AGENCY

(U) I, Lieutenant General Keith B. Alexander, do hereby state and declare as follows:

I. (U) Introduction

1. (U) I am the Director of the National Security Agency (NSA), an intelligence agency within the Department of Defense. 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. 12958, 60 Fed. Reg. 19825 (Apr. 17, 1995), as amended by Executive Order No. 13292, 68 Fed. Reg. 15315 (Mar. 25, 2003) (reprinted in 3 C.F.R. 2003 Comp. at 196 and at 50 U.S.C.A. § 435 (Supp. 2009)), and Department of Defense Directive No. 5200.1-R, Information 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. Specifically, in the course of my official duties, I have been advised of this litigation and the allegations in the plaintiffs' Amended Complaint. As described herein, various classified facts related to the plaintiffs' claims are subject to the DNI's state secrets privilege assertion. The disclosure of information discussed throughout this declaration, which relates to NSA intelligence information, activities, sources, methods, and relationships, 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 the disclosure of the secrets described herein and exceptionally grave damage to the national security of the United States. Through this declaration, I also hereby invoke and assert the NSA's statutory privilege set forth in section 6 of the National Security Agency Act of 1959, Public Law No. 86-36 (codified as a note to 50 U.S.C. § 402) ("NSA Act"), to protect the information related to NSA activities described below. The statements made herein are based on my personal knowledge of NSA activities and operations, and on information available to me as Director of the NSA.

II. (U) Summary

3. (U) I have reviewed the Amended Complaint in this case. Plaintiffs allege, in sum, that, after the 9/11 attacks, the NSA received presidential authorization to engage in surveillance activities far broader than the publicly acknowledged "Terrorist Surveillance Program" ("TSP"), which was limited to the interception of specific international communications involving persons reasonably believed to be associated with al Qaeda and affiliated terrorist organizations. Plaintiffs allege that the NSA, with the assistance of telecommunications companies, Amended Compl. ¶¶ 5-8, conducts a "dragnet" surveillance program involving the interception of "virtually every telephone, internet and/or email communication that has been sent from or received within the United States since 2001" as part of an alleged Presidentially-authorized "program" after 9/11, *id.* ¶¶ 1, 4. I cannot disclose on the public record the nature of any NSA information implicated by the plaintiffs' allegations. However, 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 and,

for this reason, are encompassed by the DNI's state secrets and statutory privilege assertions, as well as by my own statutory privilege assertion, and should be protected from disclosure in this case. 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 the disclosure of the classified privileged national security information described herein and exceptionally grave damage to the national security of the United States.

4. ~~(TS//TSP//SI//OC/NF)~~ The allegations in this lawsuit put at issue the disclosure of information concerning several highly classified and critically important NSA intelligence activities that commenced after the 9/11 terrorist attacks, but which are now being conducted pursuant to authority of the Foreign Intelligence Surveillance Act ("FISA"), including ongoing activities conducted under orders approved by the Foreign Intelligence Surveillance Court ("FISC"). Plaintiffs' allegation that the NSA undertakes indiscriminate surveillance of the *content*[1] of millions of communications sent or received by people inside the United States – under the now defunct-TSP or otherwise – is false, as discussed below. Likewise, the plaintiffs' allegations that telecommunications companies assisted with the alleged dragnet program are false, because the alleged dragnet does not exist. The NSA's collection of the content of communications under the TSP was directed at international communications in which a participant was reasonably believed to be associated with al Qaeda or an affiliated organization and did not constitute the kind of dragnet collection of the content of millions of Americans' telephone or Internet communications that the plaintiffs allege. Although the existence of the TSP has been acknowledged, the details of that program remain highly classified, along with

[1] ~~(TS//SI//NF)~~ The term "content" is used in this Declaration 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."

details of related content surveillance activities undertaken after the TSP ended pursuant to orders of the FISC. This information could not be disclosed to address or 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.

5. ~~(TS//TSP//SI//OC/NF)~~ In addition, as the Court is aware from prior classified declarations submitted by the NSA in this and related proceedings, the NSA has collected, pursuant to presidential authorization and currently under subsequent FISC orders, non-content information (*i.e.*, meta data) about telephone and Internet communications in order to enable highly sophisticated analytical tools that can uncover the contacts [redacted] of members or agents of [redacted] As noted above and detailed below, the content surveillance subject to presidential authorization after 9/11 was not the content dragnet surveillance that plaintiffs allege, and the collection of non-content information, while significant in scope, remains a highly classified matter currently under FISA authorization. For the NSA to attempt to explain, clarify, disprove, or otherwise litigate plaintiffs' allegations regarding a communications dragnet would require the NSA to confirm the existence of, or risk disclosure of facts concerning, intelligence sources and methods for the collection of non-content information related to communications, as well as current NSA operations under FISC Orders – disclosures that would cause exceptionally grave harm to national security.

---

[2] ~~(TS//SI//OC/NF)~~ Certain FISC Orders are also directed at [redacted]. Because the allegations in the complaint reference activities authorized after 9/11, which were directed at [redacted], any further references to the FISC Orders will focus solely on activities under the orders directed at [redacted].

6. ~~(TS//TSP//SI//~~[redacted]~~//OC/NF)~~ The plaintiffs' allegation that telecommunications carriers assisted the NSA in alleged intelligence activities also cannot be confirmed or denied without risking exceptionally grave harm 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] Disclosure of [redacted] would cause exceptionally grave damage to the national security.

7. ~~(TS//TSP//SI//~~[redacted]~~//OC/NF)~~ Accordingly, the DNI's state secrets and statutory privilege assertions, and my own statutory privilege assertion, seek to protect against the disclosure of the highly classified intelligence sources and methods put at issue in this case and vital to the national security of the United States, 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 specific al Qaeda and associated terrorist-related international communications and was not a content surveillance dragnet as plaintiffs allege; (3) facts that would tend to confirm or deny the existence of the NSA's bulk meta data collection and use, and any information about those activities; and (4) the fact that [redacted]

[redacted]. The fact that there has been public speculation about alleged NSA activities does not diminish the need to protect intelligence sources and methods from further exposure. Official confirmation and disclosure of the classified privileged national security information described herein would cause exceptionally grave damage to the national security. For these reasons, as set forth further below, I request that the Court uphold the state secrets and statutory privilege assertions that the DNI and I now make, and protect the information described in this declaration from disclosure.

III. (U) Classification of Declaration

8. ~~(S//SI//NF)~~ This declaration is classified TOP SECRET//TSP//SI-[redacted]//ORCON/NOFORN pursuant to the standards in Executive Order No. 12958, as amended by Executive Order No. 13292. Under Executive Order No. 12958, information is classified "TOP SECRET" if unauthorized disclosure of the information reasonably could be expected to cause exceptionally grave damage to the national security of the United States; "SECRET" if unauthorized disclosure of the information reasonably could be expected to cause serious damage to national security; and "CONFIDENTIAL" if unauthorized disclosure of the information reasonably could be expected to cause identifiable damage to national security. At the beginning of each paragraph of this declaration, the letter or letters in parentheses designate(s) the 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[3].

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

9. ~~(S//SI//NF)~~ 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 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 intercepted foreign communications.

10. ~~(TS//TSP//SI-[redacted]//OC/NF)~~ This declaration also contains information related to or derived from the TSP, a prior controlled access signals intelligence program that operated under presidential authorization in response to the attacks of September 11, 2001, until January 2007. Although the TSP was publicly acknowledged by then-President Bush in December 2005, details about the program remain highly classified and strictly compartmented. Information pertaining to this program is denoted with the special marking "TSP" and requires more restrictive handling. [redacted]

[redacted]

[redacted]

[redacted]

11. ~~(S//NF)~~ In addition to the fact that classified information contained herein may not be revealed to any person without authorization pursuant to Executive Order 12958, as amended, 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" (NF). The "ORCON" (OR) designator means that the originator of the information controls to whom it is released.

IV. (U) Background Information

A. (U) The National Security Agency

12. (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), 46 Fed. Reg. 59941 (Dec. 4, 1981), as amended.[5]

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

[5] (U) 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

13. ~~(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 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 non-U.S. aerospace surfaces and subsurface systems which may have either military or civilian applications.

14. (U) The NSA's SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities set forth in E.O. No. 12333, § 1.12(b), as amended. In performing its SIGINT mission, NSA has developed a sophisticated worldwide SIGINT collection network. 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.

---

signals intelligence information for foreign intelligence and counterintelligence purposes to support national and departmental missions."

15. (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.

16. (U) Foreign intelligence produced by COMINT activities is an extremely important part of the overall foreign intelligence information available to the United States and is often unobtainable by other means. Public disclosure of either the capability to collect specific communications or the substance of the information derived from such collection itself can easily alert targets to the vulnerability of their communications. Disclosure of even a single communication holds the potential of revealing intelligence collection techniques that are applied against targets around the world. Once alerted, targets can frustrate COMINT collection by using different or new encryption techniques, by disseminating disinformation, or by utilizing a different communications link. Such evasion techniques may inhibit access to the target's communications and therefore deny the United States access to information crucial to the defense of the United States both at home and abroad. COMINT is provided special statutory protection under 18 U.S.C. § 798, which makes it a crime to knowingly disclose to an unauthorized person classified information "concerning the communication intelligence activities of the United States or any foreign government."

B. **(U) September 11, 2001 and the al Qaeda Threat**

17. (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.

18. (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 § 2(a), 115 Stat. 224, 224 (Sept. 18, 2001). 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.

19. (U) Also after the 9/11 attacks, 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," *id.* § 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.

20. (U) As a result of the unprecedented attacks of September 11, 2001, the United States found itself immediately propelled into a worldwide war against a network of terrorist groups, centered on and affiliated with al Qaeda, that possesses the evolving capability and intention of inflicting further catastrophic attacks on the United States. That war is continuing today, at home as well as abroad. Moreover, the war against al Qaeda and its allies is a very

different kind of war, against a very different enemy, than any other war or enemy the Nation has previously faced. Al Qaeda and its supporters operate not as a traditional nation-state but as a diffuse, decentralized global 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.

21. ~~(TS//SI//NF)~~ The Classified *In Camera, Ex Parte* Declaration of Dennis C. Blair, Director of National Intelligence, details the particular facets of the continuing al Qaeda threat and, thus, the exigent need for the NSA intelligence activities described here. The NSA activities are directed at that threat, [redacted] Global telecommunications networks, especially the Internet, have developed in recent years into a loosely interconnected system – a network of networks – that is ideally suited for the secret communications needs of loosely affiliated terrorist cells. Hundreds of Internet service providers, or "ISPs," and other providers of communications services offer a wide variety of global communications options, often free of charge. [redacted][6]

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

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

23. ~~(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 new kind of war, more 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 particular NSA sources and methods implicated by the claims.

C. **(U) Summary of NSA Activities After 9/11 to Meet al Qaeda Threat**

24. (U) After the September 11 attacks, the NSA received presidential authorization and direction to detect and prevent further terrorist attacks within the United States by intercepting the content[7] of communications for which there were reasonable grounds to believe that (1) such communications originated or terminated outside the United States and (2) a party to such communication was 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" or "TSP").[8]

25. ~~(TS//TSP//SI//OC/NF)~~ In more specific and classified terms, the NSA has utilized a number of critically important intelligence sources and methods to meet the threat of another mass casualty terrorist attack on the United States – methods that were designed to work

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

[8] (U) On January 17, 2007, the Government 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.

in tandem and continue to this day under authority of the FISA. As noted above, one such method involved the program publicly acknowledged by then-President Bush as the TSP, in which the NSA intercepted the content of telephone and Internet communications pursuant to presidential authorization [9] As described further below, under the TSP, NSA did not engage in plaintiffs' alleged dragnet surveillance of communication content, but intercepted the content of particular communications where reasonable grounds existed to believe one party involved a member or agent of al Qaeda or affiliated terrorist organization based on particular "selectors" (phone numbers or Internet addresses) associated with that target. In addition to collecting the content of particular communications, the NSA has also collected *non-content* communication information known as "meta data." Specifically, after the 9/11 attacks, the NSA collected bulk meta data related to *telephony* communications for the purpose of conducting targeted analysis to track al Qaeda-related networks. 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

[9] ~~(TS//TSP//SI-[redacted]//OC/NF)~~ 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. The documents authorizing the TSP also contained the authorizations for the meta data activities described herein. The authorizations, moreover, 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). [redacted] *See* Classified *In Camera, Ex Parte* Declaration of LTG Keith B. Alexander ¶ 62, MDL No. 06-1791-VRW (N.D. Cal.) (submitted Apr. 20, 2007) (relating to all actions against the MCI and Verizon Defendants). [redacted]

duration of telephone calls, as well as the phone numbers used to place and receive the calls.[10] In addition, since the 9/11 attacks, the NSA has collected bulk meta data related to *Internet* communications. Internet meta data is header/router/addressing information, such as the "to," "from," "cc," and "bcc" lines, as opposed to the body or "re" lines, of a standard email.

26. ~~(TS//SI//OC/NF)~~ Each of the foregoing activities continues in some form under authority of the FISA and, thus, the NSA utilizes the same intelligence sources and methods today to detect and prevent further terrorist attacks that it did after the 9/11 attacks. First, as noted above, on January 10, 2007, the FISC issued two orders authorizing the Government to conduct certain electronic surveillance that had been occurring under the TSP. The FISC Orders were implemented on January 17, 2007, and, thereafter, any electronic surveillance that had been occurring as part of the TSP became subject to the approval of the FISC and the TSP was not reauthorized.[11]

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

[11] ~~(TS//SI//OC/NF)~~ As also described further, *see infra* ¶¶ 63-66, the FISC extended these orders with some modifications. What is described below as the Foreign Telephone and Email Order expired in August 2007 and was supplanted by authority enacted by Congress – first under the Protect America Act and then the FISA Amendments Act of 2008 – to authorize

27. ~~(TS//SI//OC/NF)~~ Second, with respect to the collection of telephony meta data, since May 2006 certain telecommunication providers have been required by an order of the FISC to produce to the NSA on a daily basis all telephony meta data that they create ("FISC Telephone Business Records Order"). The FISC Telephone Business Records Order has been reauthorized approximately every 90 days since it was first issued. Although this collection is broad in scope, the NSA was authorized by the FISC to query the archived telephony data with identified telephone numbers for which there are facts giving rise to a reasonable, articulable suspicion that the number is associated with [redacted] (hereafter referred to as a "RAS" determination).[12] Historically, only a tiny fraction of telephony meta data records collected by the NSA has actually been presented to a trained professional for analysis. As discussed further below, *see infra* ¶¶ 48-56, while the vast majority of records are thus never viewed by a human at the NSA, it is still necessary to collect the meta data in bulk in order to

---

foreign intelligence surveillance of targets located overseas without individual court orders.

[12] ~~(TS//SI//OC/NF)~~ As set forth further below, *see infra* ¶¶ 60-62, NSA's compliance with this limitation in the FISC Order has been subject to further proceedings in the FISC that commenced with a compliance report by the government on January 15, 2009, which indicated that the NSA had also been querying incoming telephony meta data with selectors for counterterrorism targets subject to NSA surveillance under Executive Order 12333, as to which the NSA had not made a "RAS" determination. On March 2, 2009, the FISC renewed the Order authorizing the bulk provision to NSA of business records containing telephony meta data from telecommunications carriers, but subjected that activity to new limitations, including that the NSA may query the meta data only after a motion is granted on a case-by-case basis (unless otherwise necessary to protect against imminent threat to human life). The FISC also required the Government to report to the FISC on its review of revisions to the meta data collection and analysis process and to include affidavits describing the value of the collection of telephony meta data authorized by the FISC Telephone Business Records Order. The Government submitted its report to the FISC as required on August 17, 2009. The FISC subsequently renewed the Telephone Business Records Order on September 3, 2009, and, in so doing, restored to NSA the authority to make RAS determinations for selectors that NSA counterterrorism personnel nominate for analysis through contact chaining [redacted] (these selectors are described as "seeds"). This renewed Order expires on October 30, 2009.

utilize sophisticated and vital analytical tools for tracking the contacts [redacted] for protecting the national security of the United States.

28. ~~(TS//SI//OC/NF)~~ Third, beginning in July 2004, the collection of Internet meta data in bulk has been conducted pursuant to an order of the FISC authorizing the use of a pen register and trap and trace device ("FISC Pen Register Order" or "PRTT Order"). *See* 18 U.S.C. § 3127 (defining "pen register" and "trap and trace device"). Pursuant to the FISC Pen Register Order, which has been reauthorized approximately every 90 days since it was first issued, the NSA is authorized to collect, in bulk, meta data associated with electronic communications [redacted] on the Internet.[13] [redacted] Although the NSA collects email meta data in bulk [redacted] it has been authorized by the FISC to query the archived meta data only using email addresses for which there are facts giving rise to a reasonable, articulable suspicion that the email address is associated with [redacted] As with bulk telephony meta data collection, bulk Internet meta data collection is necessary to allow the NSA to use critical and unique analytical capabilities to track the contacts (even retrospectively) [redacted] of known terrorists. Like telephony meta data activities, Internet meta

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

data collection and analysis are vital tools for protecting the United States from attack, and, accordingly, information pertaining to those activities is highly classified.[14]

V. (U) Information Protected by Privilege

29. (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 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, indiscriminately intercepts the content of communications and also, to the extent applicable to plaintiffs' claim, the communications records of millions of Americans as part of an alleged "Program" authorized by the President after 9/11. *See, e.g.*, Amended Compl. ¶¶ 1-8, 58.

(U) 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

---

[14] ~~(TS//TSP//SI//OC/NF)~~ As the NSA has previously advised the Court in related proceedings, [redacted] *See* Classified *In Camera, Ex Parte* Declaration of LTG Keith B. Alexander ¶ 31 n.8, MDL No. 06-1791-VRW (N.D. Cal.) (submitted Apr. 20, 2007) (relating to all actions against the MCI and Verizon Defendants).

(ii) (U) Any other information concerning NSA intelligence activities, sources, or methods that would be necessary to adjudicate the plaintiffs' claims, including, to the extent applicable, information that would tend to confirm or deny whether or not the NSA obtained from telecommunications companies communication transactional records; and

(iii) (U) Information that may tend to confirm or deny whether any telecommunications carrier has provided assistance to the NSA in connection with any alleged activity.

VI. (U) Description of Information Subject to Privilege and the Harm of Disclosure

A. (U) Information That May Tend to Confirm or Deny Whether the Plaintiffs Have Been Subject to Any Alleged NSA Activities

30. (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 harm to the national security.

31. ~~(TS//TSP//SI//OC/NF)~~ The named plaintiffs in this action – Virginia Shubert, Noha Arafa, Sarah Dranoff, and Hilary Botein – allege that the contents of their telephone and Internet communications were subject to "unlawful interception, search and seizure, and electronic surveillance," Amended Compl. ¶ 87, in connection with a program of "dragnet" surveillance that captures the contents of "virtually every telephone, internet and/or email communication that has been sent from or received within the United States since 2001," *id.* ¶¶ 1, 4. As set forth herein, the NSA does not engage in "dragnet" surveillance of the content of communications as plaintiffs allege. [redacted]

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

34. (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 this case 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, a person 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.

---

[16] ~~(TS//SI//OC/NF)~~ I previously noted that NSA has estimated that it collects Internet metadata associated with approximately [redacted] With respect to telephony meta data, I previously estimated that, prior to the 2006 FISC Order, about [redacted] telephony meta data records was presented to an analyst for review, *see* Classified *In Camera*, *Ex Parte* Declaration of LTG Keith B. Alexander ¶ 27 (submitted May 25, 2007), and the scope of that disparity remains generally the same.

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

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 a person, secure in the 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. 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.

35. ~~(TS//SI~~ [redacted] ~~//OC/NF)~~ [redacted], the underlying meta data collection could not be confirmed or denied without causing exceptionally grave damage to the national security. In particular, disclosure of whether the NSA currently receives plaintiffs' telephony or Internet meta data from any telecommunications companies would also violate specific provisions of the FISC Telephone Records and FISC Pen Register Orders. [redacted]

[redacted]

B. (U) Information Related to NSA Activities, Sources, or Methods Implicated by the Plaintiffs' Allegations and the Harm to National Security of Disclosure

1. (U) Plaintiffs' Allegations of a Communications Dragnet

36. (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 adjudicate the plaintiffs' claims and allegations, including that (i) the NSA is indiscriminately intercepting the content of communications of millions of ordinary Americans, *see, e.g.*, Amended Compl. ¶¶ 1-4, and (ii) to the extent relevant to this action, that the NSA is collecting the "call data" of people in the United States with the assistance of telecommunications carriers, presumably including information concerning the plaintiffs' communications. *See, e.g., id.* ¶¶ 5-8, 58. As described above, the scope of the government's privilege assertion includes but is not limited to: (1) facts concerning the operation of the now inoperative Terrorist Surveillance Program and any other NSA activities needed to demonstrate that the TSP was limited to the interception of the content of one-end foreign communications reasonably believed to involve a member or agent of al Qaeda or an affiliated terrorist organization and that the NSA does not otherwise conduct a dragnet of content surveillance as 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 harm to national security.

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

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

37. (U) After the existence of the TSP was officially acknowledged in December 2005, the Government stated that the NSA's collection of the content of communications under the TSP was directed at international communications in which a participant was reasonably believed to be associated with al Qaeda or an affiliated organization. Plaintiffs' allegation that the NSA has undertaken indiscriminate surveillance of the content of millions of communications sent or received by people inside the United States after 9/11 under the TSP is therefore false, again as the Government has previously stated.[19] But to the extent the NSA must demonstrate that content surveillance 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 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 harm to national security.

38. (U) The privileged information that must be protected from disclosure includes the following classified details concerning content surveillance under the now inoperative TSP.

39. ~~(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,

[19] (U) *See, e.g.*, Public Declaration of LTG Keith B. Alexander, Director, National Security Agency ¶ 16 (submitted May 25, 2007).

obtained or derived from various sources indicating that a particular phone number or email address is 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 email address 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]

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

[redacted]

40. ~~(TS//TSP//SI//OC/NF)~~ Once the NSA determined that there were reasonable grounds to believe that the target is 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.

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

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

[redacted][21]

43. ~~(TS//TSP//SI//[redacted]//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//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

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

affiliated terrorist organization. [redacted] The NSA did not search the content of the communications [redacted] with "key words" other than the targeted selectors themselves. Rather, the NSA targeted for collection only email 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 has occurred, and in such circumstances the NSA applies its minimization procedures to ensure that communications of non-targets are 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. ~~(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 also took additional steps to ensure that the privacy rights of U.S. persons were protected. [redacted]

[redacted]

[redacted][22]

46. ~~(TS//TSP//OC/NF)~~ [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'

[22] ~~(U//FOUO)~~ In addition, in implementing the TSP, the NSA applied the 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 United States that it inadvertently acquires, and that it refrain from identifying U.S. persons in its intelligence reports unless a senior NSA official determines 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.

allegation that the NSA engaged in the alleged content dragnet, without revealing specific NSA sources and methods, which would cause exceptionally grave damage to the national security.

47. ~~(TS//TSP//SI//OC/NF)~~ In addition to these facts about the TSP, facts about other NSA intelligence activities would be needed to address or prove that the NSA does not conduct the alleged content dragnet. [redacted] In short, there is no other "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. Again, however, information about NSA content surveillance activities beyond the TSP could not be disclosed in order to address and rebut plaintiffs' allegation without revealing specific NSA sources and methods and thereby causing exceptionally grave damage to national security.[23]

[23] ~~(TS//TSP//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 also could not be disclosed without exceptional harm to national security, including for example information that would demonstrate the operational swiftness and effectiveness of utilizing content surveillance in conjunction with the meta data activities. As noted, [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.

(b) (U) Other Classified Information Concerning NSA Activities

48. ~~(TS//TSP//SI//OC/NF)~~ To the extent that the plaintiffs' "dragnet" allegations also implicate other NSA activities, such as the bulk collection of *non-content* communication meta data or the collection of communications records, *see, e.g.*, Amended Compl. ¶ 58, addressing their assertions would require disclosure of NSA sources and methods that would cause exceptionally grave harm to national security. As also explained herein, these collection activities are now subject to the orders and supervision of the FISC.

49. ~~(TS//SI [redacted]//OC/NF)~~ As noted above, starting in October 2001, and since 2004 pursuant to the FISC Pen Register Order, the NSA collected bulk meta data associated with electronic communications [redacted] *See supra* ¶¶ 25, 28.[24] [redacted]

[redacted]

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

[redacted] pursuant to the FISC Telephone Records Order, certain telecommunication companies provide the NSA with bulk telephony meta data in the form of call detail records derived from information kept by those companies in the ordinary course of business. *See supra* ¶¶ 25, 27.

50. ~~(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 harm to national security. It is not possible to target collection solely on known terrorist telephone or Internet identifiers and effectively discover the existence, location, and plans of terrorist adversaries. [redacted]

[redacted]

[redacted]. The only effective means by which NSA analysts are able continuously to keep track of such operatives is through meta data collection and analysis.

~~(S//SI//NF)~~ Technical Details of Analytic Capabilities

51. ~~(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] 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]

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

[redacted]

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

[redacted]

54. ~~(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] 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]

55. ~~(TS//SI//OC/NF)~~ The foregoing discussion is not hypothetical. Since inception of the first FISC Telephone Business Records Order, NSA has provided 277 reports to the FBI. These reports have tipped a total of 2,900 telephone identifiers as being in contact with identifiers associated with [redacted]

[redacted]

56. ~~(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 [redacted] contacts of terrorist communications as well as the existence of current NSA activities under FISC Orders. 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 exceptionally grave harm to national security.[25]

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

57. ~~(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

[25] ~~(TS//TSP//SI//OC/NF)~~ In my prior classified declarations in this action, I set forth specific examples of how the intelligence sources and methods utilized by the NSA after the 9/11 attacks, including content surveillance under the TSP and pursuant to subsequent FISA authority, as well as non-content meta data collection and analysis, have led to the development by the NSA of actionable intelligence and important counter-terrorism efforts. *See, e.g.*, Classified *In Camera, Ex Parte* Declaration of LTG Keith B. Alexander ¶¶ 35-43, 58-61 (submitted May 25, 2007). To the extent that such information would be relevant to any litigation in this action, however, it could not be disclosed without revealing specific NSA intelligence information, sources, and methods, thereby causing exceptionally grave harm to national security, and that information remains subject to the government's privilege assertion.

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 noted 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 been subject to various orders of the FISC (as well as FISA statutory authority) and are no longer being conducted under presidential authorization. The bulk collection of non-content transactional data for Internet communications was first authorized by the FISC in the July 2004 FISC Pen Register Order, and the bulk collection of non-content telephony meta data was first authorized by the FISC in May 2006. The existence and operational details of these orders, and of subsequent FISC orders reauthorizing these activities, remain highly classified and disclosure of this information would cause exceptionally grave harm to national security.[26] In addition, while the Government has acknowledged the 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,

[26] ~~(TS//SI//OC/NF)~~ For this reason, the FISC Telephone Business Records Order and FISC Pen Register Orders prohibit 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. The FISC Orders 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.

cannot be disclosed without likewise causing exceptional harm to national security. Subsequent content surveillance sources and methods utilized by the NSA under the PAA and, currently, under the FISA Amendments Act of 2008 likewise cannot be disclosed. I summarize below the proceedings that have occurred under authority of the FISA or the FISC.

58. ~~(TS//SI//OC/NF)~~ (a) *Internet Meta Data*: Pursuant to the FISC Pen Register Order, which has been reauthorized approximately every 90 days after it was first issued, NSA is authorized to collect in bulk, from telecommunications carriers, meta data associated with electronic communications [redacted] The NSA is authorized to query the archived meta data collected pursuant to the FISC Pen Register Order using email addresses for which there were facts giving rise to a reasonable, articulable suspicion that the email address was associated with [redacted]. The FISC Pen Register Order was most recently reauthorized on [redacted], 2009, and requires continued assistance by the providers through [redacted] 2009.

59. ~~(TS//SI//OC/NF)~~ (b) *Telephony Meta Data*: Beginning in May 2006, the NSA's bulk collection of telephony meta data, previously subject to presidential authorization, was authorized by the FISC Telephone Business Records Order. Like the FISC Pen Register Order, the FISC Telephone Business Records Order was reauthorized approximately every 90 days. Based on the finding that reasonable grounds existed that the production was relevant to efforts to protect against international terrorism, the Order required telecommunications carriers to produce to the NSA "call detail records" or "telephony metadata" pursuant to 50 U.S.C.

§ 1861[c] (authorizing the production of business records for, *inter alia*, an investigation to protect against international terrorism). Telephony meta data was compiled from call detail data maintained by the providers in the ordinary course of business that reflected non-content information such as the date, time, and duration of telephone calls, as well as the phone numbers used to place and receive the calls. The NSA was authorized by the FISC to query the archived telephony meta data solely with identified telephone numbers for which there were facts giving rise to a reasonable, articulable suspicion that the number was associated with [redacted] (that is, a "RAS" determination). The FISC Telephone Business Records Order was most recently reauthorized on September 3, 2009, with authority continuing until October 30, 2009.

60. ~~(TS//SI//OC/NF)~~ As noted above, *see supra* note 12, on January 15, 2009, the Department of Justice ("DOJ") submitted a compliance incident report related to the Business Records Order to the FISC, based on information provided to DOJ by the NSA, which indicated that the NSA's prior reports to the FISC concerning implementation of the FISC Telephone Business Records Order had not accurately reported the extent to which NSA had been querying the telephony meta data acquired from carriers. In sum, this compliance incident related to a process whereby currently tasked telephony selectors (*i.e.*, phone numbers) reasonably believed to be associated with authorized counter terrorism foreign intelligence targets under Executive Order 12333 were reviewed against the incoming telephony metadata to determine if that number had been in contact with a number in the United States. This process occurred prior to a formal determination by NSA that reasonable, articulable suspicion existed that the selector was associated with [redacted] and was not consistent with NSA's prior descriptions of the process for querying telephony meta data.

61. ~~(TS//SI//OC/NF)~~ By Order dated March 2, 2009, the FISC directed that the NSA may continue to acquire call detail records of telephony meta data in accordance with the FISC Telephone Business Record Orders, but was prohibited from accessing data acquired except in a limited manner. In particular, the Government could request through a motion that the FISC authorize querying of the telephony meta data for purposes of obtaining foreign intelligence on a case-by-case basis (unless otherwise necessary to protect against imminent threat to human life, subject to report to the FISC the next business day). In addition, following the Government's disclosures concerning compliance with the FISC Orders, the FISC imposed other obligations, including to report on its ongoing review of the matter and to file affidavits describing the continuing value of the telephony meta data collection to the national security of the United States and to certify that the information sought is relevant to an authorized investigation. The Government completed its end-to-end review and submitted its report and the required affidavits to the FISC on August 3, 2009. In that report, the Government outlined the steps NSA had taken to address and correct the instances of noncompliance with FISC Orders, as well as the remedial safeguards put in place to monitor and ensure compliance with such Orders in the future. The FISC most recently renewed the Telephone Business Records Order on September 3, 2009. This latest renewal restored to NSA the authority to make RAS determinations on telephone identifiers nominated by NSA personnel to use in conducting contact chaining [redacted]

62. ~~(TS//TSP//SI//OC/NF)~~ NSA is committed to working with the FISC on this and other compliance issues to ensure that this vital intelligence tool works appropriately and effectively. For purposes of this litigation, and the privilege assertions now made by the DNI and by the NSA, the intelligence sources and methods described herein remain highly

classified and the disclosure that [redacted] would compromise vital NSA sources and methods and result in exceptionally grave harm to national security.

63. ~~(TS//TSP//SI//OC/NF)~~ (c) *Content Collection*: 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, *inter alia*, electronic surveillance of telephone and Internet communications [redacted] where the Government determined that there was probable cause to believe that (1) one of the communicants is a member or agent of [redacted] and (2) 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 that was occurring as part of the TSP became subject to the approval of the FISA Court and the TSP was not reauthorized.[27]

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

64. ~~(TS//SI//OC/NF)~~ The Foreign Telephone and Email Order remained in effect until the Protect America Act ("PAA") was enacted in August 2007. 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. 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 Government with all information, facilities, and assistance necessary to accomplish the acquisition" of necessary intelligence information, *id.* § 1805B(e). Such directives were issued to telecommunications companies and the NSA conducted content surveillance of overseas targets under the PAA through their facilities.

65. ~~(TS//SI//OC/NF)~~ Beginning in September 2008, expiring directives that had been issued under the PAA for content surveillance of overseas targets (including surveillance of specific [redacted] targets overseas) were replaced by new directives for such surveillance issued pursuant to the FISA Amendments Act of 2008. Title I of the FISA Amendments Act of 2008 authorizes the targeting of persons outside of the United States without individual FISC orders but subject to directives issued to carriers by the Director of National Intelligence and the Attorney General under Section 702(h) of the FISA for the continuation of overseas surveillance

[redacted]

under this new authority. *See* 50 U.S.C. § 1881a(h) (as added by the FISA Act of 2008, P.L. 110-261).

66. ~~(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 surveillance on numerous multiple targets overseas without the need to obtain advance court approval for each target, but none has entailed the kind of indiscriminate content surveillance dragnet on telephone and Internet communications that the plaintiffs allege.

3. (U) Plaintiffs' Allegations that Telecommunications Companies have Assisted the NSA with the Alleged Activities

67. (U) The third 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 telecommunications providers have assisted the NSA with alleged intelligence activities. Plaintiffs allege that they are customers of telecommunications carriers such as AT&T and Verizon, and that these companies participated in the alleged surveillance activities that the plaintiffs seek to challenge. As set forth below, confirmation or denial of a relationship between the NSA and any telecommunications carriers on alleged intelligence activities would cause exceptionally grave harm to national security.

68. ~~(TS//TSP//SI-[redacted]//OC/NF)~~ Because the NSA is not engaged in the indiscriminate dragnet of the content of domestic and international communications as the

plaintiffs allege, no telecommunications carriers have assisted the NSA with any such activity.[28]

[redacted]

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

[redacted]

[28] ~~(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 FISA Act Amendments Act of 2008, *see* 50 U.S.C. § 1885a, [redacted]

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

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

[redacted]

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

[redacted]

[redacted]

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

[redacted]

74. (TS//SI//OC/NF)

75. (TS//SI//OC/NF)

[redacted]

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

[redacted]

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

[redacted].

[redacted]

VII. (U) Risks of Allowing Litigation to Proceed

77. ~~(TS//TSP//SI//~~ [redacted] ~~//OC/NF)~~ Upon examination of the allegations, claims, facts, and issues raised by this case, 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 does not occur, proving why that is so, [redacted] would directly implicate highly classified intelligence information and activities. Similarly, to the extent the plaintiffs' "dragnet" allegation implicates the bulk collection of non-content information and records containing transactional meta data about communications, addressing the plaintiffs' claims 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

---

[33] ~~(TS//SI//~~ [redacted] ~~//OC/NF)~~ [redacted] *See* Classified *In Camera, Ex Parte* Declaration of Deborah A. Bonanni, National Security Agency ¶¶ 78-79, *Jewel v. NSA*, 08-cv-4373-VRW (submitted Apr. 3, 2009).

information, including critically sensitive information about NSA sources, methods, operations, targets, [redacted] 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 this case 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.

78. ~~(TS//SI//NF)~~ The United States has an overwhelming interest in detecting and thwarting further mass casualty attacks by al Qaeda. The United States has already suffered one 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 continues to possess the ability and clear, stated 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. According to the most recent intelligence analysis, attacking the U.S. Homeland remains one of al Qaeda's top operational priorities, *see* Classified *In Camera Ex Parte* Declaration of Admiral Dennis C. Blair, Director of National Intelligence, and al Qaeda will keep trying for high-impact attacks as long as its central command structure is functioning and affiliated groups are capable of furthering its interests.

79. ~~(TS//SI//NF)~~ Al Qaeda 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 agents of al Qaeda 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

80. (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 that concerns the functions of the NSA. Public disclosure of the aforementioned intelligence sources, methods and activities could reasonably be expected to cause exceptionally grave harm to the national security of the United States. Consequently, 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 exceptionally grave harm to the national security of the United States.

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

DATE: 30 Oct 09

KEITH B. ALEXANDER
LTG, USA
Director
National Security Agency