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 Trial Counsel
PAUL E. AHERN
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
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 This Document Relates Solely To: *Shubert et al. v. United States of America et. al.* (Case No. 07-cv-00693-VRW)	**No. M:06-cv-01791-VRW** **EXHIBIT 2 TO GOVERNMENT DEFENDANTS' MEMORANDUM IN SUPPORT OF RENEWED MOTION TO DISMISS AND FOR SUMMARY JUDGMENT** **PUBLIC DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR OF THE NATIONAL SECURITY AGENCY** Date: December 15, 2009 Time: 10:00 a.m. Courtroom: 6, 17th Floor Chief Judge Vaughn R. Walker

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

I. Introduction

1. 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. 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' allegations 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. Summary

3. 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.

III. Background Information

A. The National Security Agency

4. 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.[1]

5. 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.

6. 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.

[1] 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."

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.

7. 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. September 11, 2001 and the al Qaeda Threat

8. 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.

9. 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). 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.

10. 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.

11. 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.

12. 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[2] 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").[3]

INFORMATION SUBJECT TO PRIVILEGE ASSERTION

13. I understand that the plaintiffs in this lawsuit allege that they are customers of telecommunications companies, *see* Amended Compl. ¶¶ 5-8, and that the NSA, with the assistance of telecommunications carriers, has indiscriminately intercepted the content of the

---

[2] 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).

[3] 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.

communications of millions of ordinary Americans as part an alleged presidentially authorized "Program" after 9/11. *See, e.g.* Amended Compl. ¶¶ 1-4; 47-96. Plaintiffs specifically allege that, pursuant to the alleged Program, the NSA continues to acquire the content of virtually all of the phone calls, emails, instant messages, text messages, web and other communications, both international and domestic, of practically every American, including the plaintiffs. *See, e.g.*, Amended Compl. ¶¶ 1-4. Plaintiffs also appear to allege that the NSA is collecting "call data," again presumably including information concerning the plaintiffs' communications. *See id.* ¶ 58.

14. 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. 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. 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.

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

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

INFORMATION SUBJECT TO PRIVILEGE AND HARM OF DISCLOSURE

15. As set forth in my classified declaration submitted for the Court's *in camera*, *ex parte* review, disclosure of information in the foregoing categories would cause exceptionally grave harm to national security. I briefly summarize the harms at issue below.

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

16. 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 and in my classified declaration for *in camera*, *ex parte* review, disclosure of such information would cause exceptionally grave harm to the national security.

17. 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. 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.

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

1. Plaintiffs' Allegations of a Communications Dragnet

18. 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.

(a) Information Related to the Terrorist Surveillance Program

19. 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, as I have previously stated in my prior declaration in this action. (*See* Dkt. 295 ¶ 16 in 06-cv-1791-VRW). 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.

(b) Plaintiffs' Allegations Concerning the Collection of Communications Records

20. As noted above, plaintiffs also appear to allege that the NSA is collecting non-content "call data" of people in the United States, presumably including information concerning the plaintiffs' communications. *See, e.g.*, Amended Compl. ¶¶ 5-8, 58. Confirmation or denial of any information concerning whether the NSA collects communication records would also disclose information about whether or not the NSA utilizes particular intelligence sources and methods and, thus, the NSA's capabilities or lack thereof, and would cause exceptionally grave harm to national security.

2. Plaintiffs' Allegations that Telecommunications Companies have Assisted the NSA with the Alleged Activities

21. Finally, I am also supporting the DNI's assertion of privilege, and asserting the NSA's statutory privilege, over information that may tend to confirm or deny whether or not any telecommunications provider has assisted the NSA with alleged intelligence activities. Plaintiffs allege that they are customers of telecommunications carriers that participated in the alleged surveillance activities that the plaintiffs seek to challenge. Disclosure of any information that may tend to confirm or deny whether any particular telecommunications carrier assists the NSA with alleged intelligence activities would cause exceptionally grave harm to national security.

* * *

22. Any further elaboration on the public record concerning these matters would reveal information that would cause the very harm that my privilege assertion and the DNI's privilege assertion are intended to prevent. As noted, my separate classified declaration, submitted solely for *in camera*, *ex parte* review, provides a more detailed explanation of the information and harms to national security at issue.

CONCLUSION

23. 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