STUART F. DELERY
Acting Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
VINCENT M. GARVEY
Deputy Branch Director
ANTHONY J. COPPOLINO
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782/Fax: (202) 616-8460
Attorneys for the United States and Government Defendants Sued in their Official Capacities

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CAROLYN JEWEL, *et al.* Plaintiffs, v. NATIONAL SECURITY AGENCY *et al.* Defendants.	**No. 08-cv-4873-JSW** **PUBLIC DECLARATION OF FRANCES J. FLEISCH, NATIONAL SECURITY AGENCY** Date: November 2, 2012 Time: 9:00 a.m. Courtroom 11, 19th Floor Judge Jeffrey S. White

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

I. Introduction

1. I am the Executive Director for the National Security Agency (NSA), an intelligence agency within the Department of Defense. I have held this position since June 2010. As the Executive Director, I serve as an adjunct to the Deputy Director for all NSA matters. Under our internal regulations, and in the absence of the Director and Deputy Director, I am

responsible for directing the NSA, overseeing the operations undertaken to carry out its mission and, by specific charge of the President and the Director of National Intelligence, protecting NSA activities and intelligence sources and methods. I have been designated an original TOP SECRET classification authority under Executive Order No. 13526, 75 Fed. Reg. 707 (2009) and Department of Defense Directive No. 5200.1-R, Information and Security Program Regulation, 32 C.F.R. § 159a.12 (2000).

2. The purpose of this declaration is to support an assertion of the military and state secrets privilege (hereafter, "state secrets privilege") by the Director of National Intelligence ("DNI") as the head of the Intelligence Community, as well as the DNI's assertion of a statutory privilege under the National Security Act, to protect information related to NSA activities described herein below. General Keith B. Alexander, the Director of the National Security Agency, has been sued in his official and individual capacity in the above captioned litigation and has recused himself from the decision on whether to assert privilege in his official capacity. As the Executive Director, and by specific delegation of the Director, I am authorized to review the materials associated with this litigation, prepare whatever declarations I determine are appropriate, and determine whether to assert the NSA's statutory privilege. Through this declaration, I hereby invoke and assert the NSA's statutory privilege set forth in Section 6 of the National Security Agency Act of 1959, Public Law No. 86-36 (codified as a note to 50 U.S.C. § 402) ("NSA Act"), to protect the information related to NSA activities described herein below. The statements made herein are based on my personal knowledge of NSA activities and operations, and on information made available to me as the Executive Director of the NSA. I have executed a classified declaration concerning this matter solely for the Court's *in camera, ex parte* review.

II. Summary

3. In the course of my official duties, I have been advised of the above-captioned *Jewel* action, as well as a related action in *In re NSA Telecommunications Records Litigation* (M:06-cv-1791)---*Shubert v. Obama* (07-cv-00693), and I have reviewed the allegations raised in this litigation, including the Complaint filed in the *Jewel* action on September 18, 2008, and the Second Amended Complaint ("SAC") filed in the *Shubert* action on May 8, 2012.[1] In sum, plaintiffs allege that, after the 9/11 attacks, the NSA received presidential authorization to engage in "dragnet" communications surveillance in concert with major telecommunications companies. *See, e.g.*, *Jewel* Compl. ¶¶ 2-3; *Shubert* SAC ¶¶ 1-7. Plaintiffs allege that the presidentially-authorized activities at issue in this litigation went beyond the "Terrorist Surveillance Program" ("TSP"), which was publicly acknowledged by the President in December 2005 and was limited to the interception of specific international communications involving persons reasonably believed to be associated with al Qaeda and affiliated terrorist organizations. Rather, plaintiffs allege that other intelligence activities were also authorized by the President after 9/11, and that, with the assistance of telecommunication companies including AT&T and Verizon, the NSA has indiscriminately intercepted the content and obtained the communications records of millions of ordinary Americans as part of an alleged presidentially-authorized "Program" after 9/11. *See Jewel* Compl. ¶¶ 2-13; 39-97; *Shubert* SAC ¶¶ 1-7; 57-58; 60-91.

[1] This public declaration and my classified declaration submitted solely for *in camera*, *ex parte* review, addresses and asserts privilege with respect to allegations raised in both the *Jewel* and *Shubert* actions. In addition, the harm to national security that would result from the disclosure of NSA sources and methods at issue in this litigation is applicable to similar allegations concerning NSA activities raised in other lawsuits in *In re NSA Telecommunications Records Litigation* (M:06-cv-1791).

4. I cannot disclose on the public record the specific nature of NSA information or activities implicated by the plaintiffs' allegations. As described further below, the disclosure of information related to the NSA's activities, sources and methods implicated by the plaintiffs' allegations reasonably could be expected to cause exceptionally grave damage to the national security of the United States. In addition, it is my judgment that sensitive state secrets are so central to the subject matter of the litigation that any attempt to proceed in the case risks disclosure of the classified privileged national security information described herein and exceptionally grave damage to the national security of the United States. In particular, the fact that there has been public speculation about alleged NSA activities, including in media reports, books, or plaintiffs' declarations, does not diminish the need to protect intelligence sources and methods from further exposure. The process of sorting out whether any allegation is true, partly true, or wholly false, would necessarily risk or require disclosure of the intelligence sources and methods and confirm to our adversaries whether or not, or to what extent, the NSA utilizes certain sources and methods, and thereby cause exceptionally grave damage to the national security.

III. Background Information

A. The National Security Agency

5. The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. The NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate signals intelligence (SIGINT) information, of which communications intelligence ("COMINT") is a

significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations. *See* Executive Order 12333, § 1.7(c), as amended.[2]

6. The NSA's SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities set forth in E.O. No. 12333, § 1.7(c)(2). 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.

7. 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.

8. 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

---

[2] Executive Order 12333, reprinted as amended in 50 U.S.C § 401 note, generally describes the NSA's authority to collect foreign intelligence that is not subject to the FISA definition of electronic surveillance, including activities undertaken abroad. Section 1.7(c) of E.O. 12333, as amended, specifically authorizes the NSA to "Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information for foreign intelligence and counterintelligence purposes to support national and departmental missions."

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

9. 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.

10. On September 14, 2001, a national emergency was declared "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." Presidential Proclamation No. 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001). The United States also immediately began plans for a military response directed at al Qaeda's training grounds and havens in Afghanistan. On September 14, 2001, both Houses of Congress passed a Joint Resolution authorizing the President of the United States "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11. Authorization for Use of Military Force, Pub. L. No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept. 18, 2001) ("Cong. Auth."). Congress also expressly acknowledged that the attacks rendered it "necessary and appropriate" for the United States to exercise its right "to protect United States citizens both at home and abroad," and acknowledged in particular that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." *Id.* pmbl.[3]

[3] Following the 9/11 attacks, the United States also immediately began plans for a military response directed at al Qaeda's training grounds and havens in Afghanistan. A Military Order was issued stating that the attacks of September 11 "created a state of armed conflict," *see* Military Order by the President § 1(a), 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001), and that al Qaeda terrorists "possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the United States Government," and concluding that "an extraordinary emergency exists for national defense purposes." Military Order, § 1(c), (g), 66 Fed. Reg. at 57833-34. Indeed, shortly after the attacks, NATO took the unprecedented step of invoking article 5 of the

11. As a result of the unprecedented attacks of September 11, 2001, the United States found itself immediately propelled into a conflict with al Qaeda and its associated forces, a set of groups that possesses the evolving capability and intention of inflicting further attacks on the United States. That conflict is continuing today, at home as well as abroad. Moreover, the conflict against al Qaeda and its allies is a very different kind of conflict, against a very different enemy, than any other conflict or enemy the Nation has previously faced. Al Qaeda and its affiliates operate not as a traditional nation-state but as a diffuse, decentralized network of individuals, cells, and loosely associated, often disparate groups, that act sometimes in concert, sometimes independently, and sometimes in the United States, but always in secret—and their mission is to destroy lives and to disrupt a way of life through terrorist acts. Al Qaeda works in the shadows; secrecy is essential to al Qaeda's success in plotting and executing its terrorist attacks.

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[4] 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").[5]

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.

[4] 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).

[5] 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

IV. Information Protected by Privilege

13. I understand that the plaintiffs in *Jewel* and *Shubert* allege that they are customers of telecommunications companies and that the NSA, with the assistance of telecommunications carriers, has indiscriminately intercepted the content of the communications of millions of ordinary Americans, including the plaintiffs, as part an alleged presidentially authorized "Program" after 9/11.[6] In addition, the plaintiffs in *Jewel* and *Shubert* allege that the NSA, again with the alleged assistance of telecommunication carriers, has been and is continuing to collect the private telephone and Internet communication transactional records of millions of Americans.[7]

---

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.

[6] Specifically, the *Jewel* Plaintiffs allege that, pursuant to a presidentially authorized program after the 9/11 attacks, the NSA, with the assistance of AT&T, acquired and continues to acquire the content of phone calls, emails, instant messages, text messages, web and other communications, both international and domestic, of millions of ordinary Americans --- "practically every American who uses the phone system or the Internet"--- including the Plaintiffs. *See Jewel* Complaint ¶¶ 7, 9, 10; *see also id.* at ¶¶ 39-97. The *Shubert* Plaintiffs similarly allege that the contents of "virtually every telephone, Internet and email communication sent from or received within the United States since shortly after September 11, 2001," including Plaintiffs' communications, are being "searched, seized, intercepted, and subject to surveillance without a warrant, court order or any other lawful authorization in violation of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1810." *See Shubert* SAC ¶ 1; *see also id.* ¶¶ 5, 7.

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

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 statutory 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 such as AT&T and Verizon, indiscriminately intercepts the content of communications and also collects the communication records of millions of Americans as part of an alleged "Program" authorized by the President after 9/11. *See, e.g.*, *Jewel* Comp. ¶¶ 2-13; 39-97; *Shubert* SAC ¶¶ 1-9; 57-58; 62-91.

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

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

(iii) Information that may tend to confirm or deny whether AT&T, Verizon (and to the extent relevant or necessary, any other telecommunications carrier), have provided assistance to the NSA in connection with any alleged activity; *see, e.g.*, *Jewel* Complaint ¶¶ 2, 7-8, 10; 13 50-97; *Shubert* SAC ¶¶ 6, 10-13; 66-68.

V. Harm of Disclosure of Privileged Information

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 damage to national security. I briefly summarize the harms at issue below.

A. Information Concerning Whether the Plaintiffs Have Been Subject to the 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, disclosure of such information would cause exceptionally grave damage 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 these two cases and others that specific individuals are not targets of surveillance, but later refuse to comment (as it would have to) in a case involving an actual target, an actual or potential adversary of the United States could easily deduce by comparing such responses that the person in the latter case is a target. The harm of revealing targets of foreign intelligence surveillance should be obvious. If an individual knows or suspects he is a target of U.S. intelligence activities, he would naturally tend to alter his behavior to take new precautions against surveillance. In addition, revealing who is not a target would indicate who has avoided surveillance and what may be a secure channel for communication. Such information could lead an actual or potential adversary, secure in the knowledge that he is not under surveillance, to help a hostile foreign adversary convey information; alternatively, such a person may be unwittingly utilized or even forced to convey

information through a secure channel to a hostile foreign adversary. Revealing which channels are free from surveillance and which are not would also reveal sensitive intelligence methods and thereby could help any adversary evade detection and capitalize on limitations in NSA's capabilities.

B. Information Related to NSA Activities, Sources, or Methods Implicated by 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 litigate the plaintiffs' claims and allegations, including that: (1) the NSA is indiscriminately intercepting the content of communications of millions of ordinary Americans, *see e.g., Jewel* Complaint ¶¶ 7, 9, 10; *Shubert* SAC ¶¶ 1, 5, 7; and (2) that the NSA is collecting the private telephone and Internet transactional records of Americans with the assistance of telecommunications carriers, again including information concerning the plaintiffs' telephone and Internet communications. See *Jewel* Complaint ¶¶ 7, 10, 11, 13, 82-97; *see Shubert* SAC ¶ 102. As described above, the scope of the government's privilege assertion includes but is not limited to: (1) information concerning the now inoperative "Terrorist Surveillance Program" and any other NSA activities that would be at risk of disclosure or required in demonstrating that the NSA has not engaged in content "dragnet" surveillance activities that the plaintiffs allege; and (2) information concerning whether or not the NSA obtains transactional communications records from telecommunications companies. As set forth below, the disclosure of such information would cause exceptionally grave damage to national security.

(1) Information Concerning Plaintiffs' Content Surveillance Allegations and the TSP.

19. After the existence of the TSP was officially acknowledged in December 2005, the Government stated that this activity was limited to the interception of the content of certain communications for which there were reasonable grounds to believe that: (1) such communication originated or terminated outside the United States; and (2) a party to such communication is a member or agent of al Qaeda or an affiliated terrorist organization. Nonetheless, plaintiffs' allege that the NSA indiscriminately intercepts the content of communications of millions of ordinary Americans. *See e.g., Jewel* Complaint ¶¶ 7, 9, 10; *see Shubert* SAC ¶¶ 1, 5, 7. As the Government has also previously stated,[8] plaintiffs' allegation that the NSA has undertaken indiscriminate surveillance of the content[9] of millions of communications sent or received by people inside the United States after 9/11 under the TSP is false. But to the extent the NSA must demonstrate that content surveillance under the TSP was so limited, and was not plaintiffs' alleged content "dragnet," or demonstrate that the NSA has not otherwise engaged in the alleged content "dragnet," highly classified NSA intelligence sources and methods about the operation of the TSP and current NSA intelligence activities would be subject to disclosure or the risk of disclosure. The disclosure of whether and to what extent the NSA utilizes certain intelligence sources and methods would reveal to foreign adversaries the NSA's capabilities, or lack thereof, enabling them to either evade particular channels of

---

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

[9] As noted above, 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).

communications that are being monitored, or exploit channels of communications that are not subject to NSA activities – in either case risking exceptionally grave damage to national security. As set forth in my classified declaration, a range of operational details concerning the Terrorist Surveillance Program, as well as other NSA sources and methods, remains properly classified and privileged from disclosure, and could not be revealed to address plaintiffs' content "dragnet" allegations.

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

20. As noted above, plaintiffs in *Jewel* and *Shubert* also allege that the NSA is collecting the private telephone and Internet transaction records of millions of Americans, again including information concerning the plaintiffs' telephone and Internet communications. *See, e.g., Jewel* Complaint ¶¶ 7, 10, 11, 13, 82-97; *see Shubert* SAC ¶ 102. Again as set forth in my classified declaration, 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 damage to national security.

(3) Information Concerning Plaintiffs' Allegations that Telecommunications Carriers Provided Assistance to the NSA

21. The final major category of NSA intelligence sources and methods as to which I am supporting the DNI's assertion of privilege, and asserting the NSA's statutory privilege, concerns information that may tend to confirm or deny whether or not AT&T and Verizon (or to the extent necessary whether or not any other telecommunications provider) has assisted the NSA with alleged intelligence activities. The *Jewel* plaintiffs and three of the *Shubert* plaintiffs allege that they are customers of AT&T, and that AT&T participated in the alleged surveillance activities that the plaintiffs seek to challenge. Additionally, at least one *Shubert* plaintiff also

claims to be a customer of Verizon, and that Verizon similarly participated in the alleged surveillance activities that the plaintiffs seek to challenge. As again set forth in more detail in my classified declaration, confirmation or denial of a relationship between the NSA and AT&T, Verizon, or any other telecommunication carrier on alleged intelligence activities would cause exceptionally grave damage to national security. Confirming or denying such allegations of assistance would reveal to foreign adversaries whether or not NSA utilizes particular intelligence sources and methods and, thus, either compromise actual sources and methods or reveal that NSA does not utilize a particular source and method. Such facts would allow individuals, to include America's adversaries, to accumulate information and draw conclusions about how the U.S. Government collects communications, its technical capabilities, and its sources and methods.[10] Any U.S. Government confirmation or denial would also replace speculation with certainty for hostile foreign adversaries who are balancing the risk that a particular channel of communication may not be secure against the need to communicate efficiently. Such confirmation or denial would allow adversaries to focus with certainty on a particular channel that is secure.

22. Indeed, Congress recognized the need to protect the identities of telecommunications carriers alleged to have assisted the NSA when it enacted provisions of the FISA Amendments Act of 2008 that barred lawsuits against telecommunication carriers alleged

---

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

to have assisted the NSA after the 9/11 attacks. In enacting this legislation, the Senate Select Committee on Intelligence, after extensive oversight of the Terrorist Surveillance Program, found that "electronic surveillance for law enforcement and intelligence purposes depends in great part on the cooperation of private companies that operate the nation's telecommunications system." S. Rep. 110-209 (2007) at 9 (accompanying S. 2248, Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007). Notably, the SSCI expressly stated that, in connection with alleged post-9/11 assistance, "it would be inappropriate to disclose the names of the electronic communication service providers from which assistance was sought, the activities in which the Government was engaged or in which the providers assisted, or the details regarding any such assistance." *Id.* The Committee added that the "identities of persons or entities who provide assistance to the intelligence community are properly protected as sources and methods of intelligence." *Id.*

* * *

23. Any further elaboration on the public record concerning the foregoing 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.

VI. Conclusion

24. 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 Act with respect to the information described herein which concerns the functions of the NSA. Moreover, because proceedings in this case risk disclosure of privileged and classified intelligence-related

information, I respectfully request that the Court not only protect that information from disclosure but also dismiss this case to prevent exceptional harm to the national security of the United States.

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

DATE: 9.11.12

Frances J. Fleisch
Executive Director
National Security Agency