

1 STUART F. DELERY
2 Assistant Attorney General
3 JOSEPH H. HUNT
4 Director, Federal Programs Branch
5 ANTHONY J. COPPOLINO
6 Deputy Branch Director
7 JAMES J. GILLIGAN
8 Special Litigation Counsel
9 MARCIA BERMAN
10 Senior Trial Counsel
11 BRYAN DEARINGER
12 RODNEY PATTON
13 Trial Attorneys
14 U.S. Department of Justice
15 Civil Division, Federal Programs Branch
16 20 Massachusetts Avenue, NW
17 Washington, D.C. 20001
18 Phone: (202) 514-2205
19 Fax: (202) 616-8470
20 *Attorneys for the United States and Government*
21 *Defendants Sued in their Official Capacities*

22
23 **UNITED STATES DISTRICT COURT**
24 **NORTHERN DISTRICT OF CALIFORNIA**
25 **SAN FRANCISCO DIVISION**
26

27 CAROLYN JEWEL, *et al.*) Case No. 08-cv-4373-JSW
28)
29 Plaintiffs,)
30)
31 v.)
32)
33 NATIONAL SECURITY AGENCY, *et al.*)
34)
35 Defendants.)

36 _____)
37) Case No. 07-cv-693-JSW
38 VIRGINIA SHUBERT, *et al.*)
39) **UNCLASSIFIED DECLARATION**
40 Plaintiffs,) **OF FRANCES J. FLEISCH,**
41) **NATIONAL SECURITY AGENCY**
42 v.)
43)
44 BARACK OBAMA, *et al.*) No Hearing Scheduled
45) Courtroom 11, 19th Floor
46 Defendants.) Judge Jeffrey S. White
47 _____)
48)

1 **UNCLASSIFIED DECLARATION OF FRANCES J. FLEISCH**
2 **NATIONAL SECURITY AGENCY**

3
4 I, Frances J. Fleisch, do hereby state and declare as follows:
5

6 **I. INTRODUCTION**

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

21 2. The purpose of this declaration is to support an assertion of the military and state
22 secrets privilege (hereafter, “state secrets privilege”) by the Director of National Intelligence
23 (“DNI”) as the head of the Intelligence Community, as well as the DNI’s assertion of a statutory
24 privilege under the National Security Act, to protect information related to the NSA activities
25 described below that may be necessary to adjudicate the claims at issue in this litigation.

26 Through this declaration, I also hereby invoke and assert the NSA’s statutory privilege set forth

1 in Section 6 of the National Security Agency Act of 1959, Public Law No. 86-36 (codified at 50
2 U.S.C. 3601 *et seq.*) (“NSA Act”), to protect the information related to the NSA activities
3 described herein below. General Keith B. Alexander, the Director of the NSA, has been sued in
4 his official and individual capacities in the above-captioned litigation and has recused himself
5 from the decision on whether to assert privilege in his official capacity. As the Acting Deputy
6 Director, and by specific delegation of the Director, I am authorized to review the materials
7 associated with this litigation, prepare whatever declarations I determine are appropriate, and
8 determine whether to assert the NSA’s statutory privilege. The statements made herein are based
9 on my personal knowledge of NSA activities and operations, and on information made available
10 to me as the Acting Deputy Director of the NSA. Contemporaneous with this declaration, I have
11 executed a classified declaration solely for the Court’s *in camera, ex parte* review, concerning
12 the same matters addressed in this public declaration.

13 **II. SUMMARY**

14 3. In the course of my official duties, I have been advised that plaintiffs in this
15 litigation allege that, following the terrorist attacks of September 11, 2001, the NSA, pursuant to
16 presidential authorization and with the assistance of plaintiffs’ telecommunications companies
17 (namely, AT&T and Verizon), indiscriminately intercepted the content and obtained the
18 communications records of millions of ordinary Americans as part of an alleged “dragnet”
19 communications surveillance. The Government has previously asserted the state secrets
20 privilege in these cases, most recently in September 2012, to protect from disclosure highly
21 sensitive intelligence-gathering information relevant to confirming or negating plaintiffs’
22 allegations. This declaration responds to the Court’s order that the Government explain the
23 impact of recent official disclosures about NSA intelligence-gathering activities on the national

1 security issues in the litigation, as reflected in its state secrets privilege assertion. July 23, 2013
2 Amended Order (ECF No. 153 at 25); Sept. 27, 2013 Transcript of Proceedings at 7.¹

3 4. The Government's recent official disclosures follow a series of unprecedented,
4 unauthorized, and unlawful disclosures, by a former NSA contractor, of Top Secret documents
5 concerning certain classified NSA surveillance programs. The media revealed those
6 unauthorized disclosures beginning in June 2013. These disclosures are now risking, and in
7 some cases causing, the exceptionally grave damage to national security that the Government has
8 previously identified to the Court, including the loss of valuable intelligence and, specifically,
9 information that may assist in detecting or preventing a future mass casualty terrorist attack.

10 5. The Government responded to the recent unlawful disclosures by officially
11 acknowledging the existence of certain programs because of the importance of correcting
12 inaccurate information to the public about those programs, despite the harm to national security
13 that such an official acknowledgement would cause. In sum, the Government confirmed the
14 existence and some information concerning (1) the telephony metadata program, in which the
15 NSA obtains, pursuant to orders issued by the Foreign Intelligence Surveillance Court ("FISC"),
16 telephone company business records in bulk containing certain non-content information about
17 phone calls made, such as the phone numbers dialed, and the date, time, and duration of the calls,
18 and uses that information to identify unknown terrorist operatives; (2) a previous program of
19 bulk collection of certain Internet metadata, such as the "to" and "from" lines of an email and the
20 date and time the email was sent, also authorized by the FISC and also for counter-terrorism

¹ This declaration supplants all prior privilege assertions. In order to focus on the information which remains subject to this privilege assertion, this declaration does not repeat or address all topics that were addressed in prior declarations. The Court is respectfully referred to prior declarations for additional background.

1 purposes; and (3) certain information about the Government's use of authority conferred by
2 Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), to collect, for foreign
3 intelligence purposes, certain communications of non-U.S. persons located outside the United
4 States, pursuant to approval of the FISC.

5 6. In addition, the Government has now declassified the existence of the two
6 metadata collection activities that were conducted prior to FISC authorization, under presidential
7 authorizations issued by President Bush in the wake of the September 11 attacks. But for many
8 reasons vital to national security, the classified sources and methods (many of which the NSA
9 continues to utilize today), intelligence gathered, and operational details of what has been called
10 the President's Surveillance Program ("PSP") must remain protected from public disclosure to
11 avoid even greater damage to national security than is already occurring as a result of the
12 unlawful disclosures. To the extent this information is at risk of disclosure in litigating
13 plaintiffs' claims, the Government continues to assert the state secrets privilege and applicable
14 statutory privileges over that information. In particular, and in unclassified terms, the privilege
15 applies to information about whether plaintiffs themselves have been subject to any of the
16 surveillance activities they complain about; classified intelligence sources and methods of the
17 NSA programs at issue, such as the identities of any telecommunications carriers and facilities
18 that provided assistance to the NSA; and intelligence collected under the programs..

19 7. For the reasons detailed below and further detailed in my classified declaration,
20 the Government continues to assert the state secrets privilege in these cases, as described in my
21 declaration, notwithstanding the Government's recent official disclosures.

1 **III. BACKGROUND**

2 **A. The National Security Agency**

3 8. The NSA was established by Presidential Directive in 1952 as a separately
4 organized agency within the Department of Defense. The NSA's foreign intelligence mission
5 includes the responsibility to collect, process, analyze, produce, and disseminate signals
6 intelligence ("SIGINT") information, of which COMINT is a significant subset, for (a) national
7 foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military
8 operations. *See* Executive Order 12333, § 1.7(c), as amended.²

9 9. SIGINT consists of three subcategories: (1) COMINT; (2) electronic intelligence
10 ("ELINT"); and (3) foreign instrumentation signals intelligence ("FISINT"). COMINT is
11 defined as "all procedures and methods used in the interception of communications and the
12 obtaining of information from such communications by other than the intended recipients." 18
13 U.S.C. § 798. COMINT includes information derived from the interception of foreign and
14 international communications, such as voice, facsimile, and computer-to-computer information
15 conveyed via a number of means. ELINT is technical intelligence information derived from
16 foreign non-communications electromagnetic radiations except atomic detonation or radioactive
17 sources---in essence, radar systems affiliated with military weapons platforms (*e.g.*, anti-ship)
18 and civilian systems (*e.g.*, shipboard and air traffic control radars). FISINT is derived from the

² Executive Order 12333, reprinted as amended in 50 U.S.C § 3001 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."

1 intercept of foreign electromagnetic emissions associated with the testing and operational
2 deployment of non-U.S. aerospace, surface, and subsurface systems.

3 10. The NSA's SIGINT responsibilities include establishing and operating an
4 effective unified organization to conduct SIGINT activities set forth in EO 12333, § 1.7(c)(2), as
5 amended. In performing its SIGINT mission, the NSA has developed a sophisticated worldwide
6 SIGINT collection network that acquires, among other things, foreign and international
7 electronic communications and related information. The technological infrastructure that
8 supports the NSA's foreign intelligence information collection network has taken years to
9 develop at a cost of billions of dollars and untold human effort. It relies on sophisticated
10 collection and processing technology.

11 11. There are two primary reasons for gathering and analyzing foreign intelligence
12 information. The first, and most important, is to gain information required to direct U.S.
13 resources as necessary to counter external threats and in support of military operations. The
14 second reason is to obtain information necessary to the formulation of U.S. foreign policy.
15 Foreign intelligence information provided by the NSA is thus relevant to a wide range of
16 important issues, including military order of battle; threat warnings and readiness; arms
17 proliferation; international terrorism; counter-intelligence; and foreign aspects of international
18 narcotics trafficking.

19 12. The NSA's ability to produce foreign intelligence information depends on its
20 access to foreign and international electronic communications. Foreign intelligence produced by
21 COMINT activities is an extremely important part of the overall foreign intelligence information
22 available to the United States and is often unobtainable by other means. Public disclosure of
23 either the capability to collect specific communications or the substance of the information
24 derived from such collection itself can easily alert targets to the vulnerability of their

1 communications. Disclosure of even a single communication holds the potential of revealing
2 intelligence collection techniques that are applied against targets around the world. Once alerted,
3 targets can frustrate COMINT collection by using different or new encryption techniques, by
4 disseminating disinformation, or by utilizing a different communications link. Such evasion
5 techniques may inhibit access to the target's communications and therefore deny the United
6 States access to information crucial to the defense of the United States both at home and abroad.
7 COMINT is provided special statutory protection under 18 U.S.C. § 798, which makes it a crime
8 to knowingly disclose to an unauthorized person classified information "concerning the
9 communication intelligence activities of the United States or any foreign government."

10 **B. September 11, 2001, and the al Qaeda Threat**

11 13. On September 11, 2001, the al Qaeda terrorist network launched a set of
12 coordinated attacks along the East Coast of the United States. Four commercial jetliners, each
13 carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al
14 Qaeda operatives. Those operatives targeted the Nation's financial center in New York with two
15 of the jetliners, which they deliberately flew into the Twin Towers of the World Trade Center.
16 Al Qaeda targeted the headquarters of the Nation's Armed Forces, the Pentagon, with the third
17 jetliner. Al Qaeda operatives were apparently headed toward Washington, D.C. with the fourth
18 jetliner when passengers struggled with the hijackers and the plane crashed in Shanksville,
19 Pennsylvania. The intended target of this fourth jetliner was most likely the White House or the
20 Capitol, strongly suggesting that al Qaeda's intended mission was to strike a decapitating blow to
21 the Government of the United States—to kill the President, the Vice President, or Members of
22 Congress. The attacks of September 11 resulted in approximately 3,000 deaths—the highest
23 single-day death toll from hostile foreign attacks in the Nation's history. In addition, these

1 attacks shut down air travel in the United States, disrupted the Nation's financial markets and
2 government operations, and caused billions of dollars of damage to the economy.

3 14. On September 14, 2001, a national emergency was declared "by reason of the
4 terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the
5 continuing and immediate threat of further attacks on the United States." Presidential
6 Proclamation No. 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001). On September 14, 2001, both
7 Houses of Congress passed a Joint Resolution authorizing the President of the United States "to
8 use all necessary and appropriate force against those nations, organizations, or persons he
9 determines planned, authorized, committed, or aided the terrorist attacks" of September 11.
10 Authorization for Use of Military Force, Pub. L. No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept.
11 18, 2001) ("Cong. Auth."). Congress also expressly acknowledged that the attacks rendered it
12 "necessary and appropriate" for the United States to exercise its right "to protect United States
13 citizens both at home and abroad," and acknowledged in particular that "the President has
14 authority under the Constitution to take action to deter and prevent acts of international terrorism
15 against the United States." *Id.* pmb1.³

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 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.

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

13 16. The 9/11 attacks posed significant challenges for the NSA’s signals intelligence
14 mission. Global telecommunications networks, especially the Internet, have developed in recent
15 years into a loosely interconnected system—a network of networks—that is ideally suited for the
16 secret communications needs of loosely affiliated terrorist cells. Hundreds of Internet service
17 providers, or “ISPs,” and other providers of communications services offer a wide variety of
18 global communications options, often free of charge.

19 17. Our efforts against al Qaeda and its affiliates therefore present critical challenges
20 for the Nation’s communications intelligence capabilities. First, in this type of conflict, more so
21 than in any other we have ever faced, communications intelligence is essential to our ability to
22 identify the enemy and to detect and disrupt its plans for further attacks on the United States.
23 Communications intelligence often is the only means we have to learn the identities of particular
24 individuals who are involved in terrorist activities and the existence of particular terrorist threats.

1 Second, at the same time that communications intelligence is more important than ever, the
2 decentralized, non-hierarchical nature of the enemy and their sophistication in exploiting the
3 agility of modern telecommunications make successful communications intelligence more
4 difficult than ever. It is against this backdrop that the risks presented by this litigation should be
5 assessed, in particular the risks of disclosing NSA sources and methods implicated by the claims
6 being raised.

7 **C. Plaintiffs' Allegations and the Government's Prior Assertions of Privilege**

8 18. In the course of my official duties, I have been advised of the *Jewel* and *Shubert*
9 cases, and I have reviewed the allegations raised in this litigation, including the Complaint filed
10 in the *Jewel* action on September 18, 2008, and the Second Amended Complaint ("SAC") filed
11 in the *Shubert* action on May 8, 2012. In sum, plaintiffs allege that, after the 9/11 attacks, the
12 NSA received presidential authorization to engage in "dragnet" communications surveillance in
13 concert with major telecommunications companies. *See, e.g., Jewel* Compl. ¶¶ 2-3, *Shubert*
14 SAC ¶¶ 1-7. Plaintiffs allege that, pursuant to presidential authorization and with the assistance
15 of telecommunication companies (including AT&T and Verizon), the NSA indiscriminately
16 intercepted the content and obtained the communications records of millions of ordinary
17 Americans. Plaintiffs seek relief in this litigation that would prohibit such collection activities,
18 even though they were later transitioned to FISC-authorized programs and remain so to the
19 extent the programs continue.

20 19. In addition, I am familiar with the previous classified declarations filed in these
21 cases in September and November 2012. In those declarations, the DNI and the NSA asserted
22 the state secrets privilege over the following broad categories of information: (1) any
23 information that may tend to confirm or deny whether particular individuals, including plaintiffs,
24 have been subject to the alleged NSA intelligence activities; and (2) any information concerning

1 NSA intelligence activities, sources, or methods that may relate to or be necessary to adjudicate
2 plaintiffs' allegations, including allegations that the NSA, with the assistance of
3 telecommunications carriers such as AT&T and Verizon, indiscriminately intercepts the content
4 of communications and collects the communication records of millions of Americans as part of
5 an alleged program authorized by the President after 9/11. This latter category included (i)
6 information concerning the scope and operation of the now inoperative Terrorist Surveillance
7 Program ("TSP") regarding the interception of the content of certain international
8 communications reasonably believed to involve a member or agent of al Qaeda or an affiliated
9 terrorist organization,⁴ and any other information related to demonstrating that the NSA does not
10 otherwise engage in the content surveillance "dragnet" alleged by plaintiffs; (ii) information
11 concerning whether or not the NSA obtained from telecommunications companies such as
12 AT&T and Verizon communication transactional records as alleged in the complaints; and (iii)
13 information that may tend to confirm or deny whether AT&T, Verizon, or other
14 telecommunications carriers have provided assistance to the NSA in connection with any of the
15 alleged activities.

16 **D. Official Disclosures Since September 2012**

17 20. In the wake of unauthorized disclosures, beginning in June 2013, about
18 intelligence-gathering activities conducted by the NSA, the DNI, at the direction of the President
19 and in light of the President's transparency initiative, has declassified and made public certain

⁴ In December 2005, then-President Bush publicly acknowledged the existence of a presidentially-authorized NSA activity that later came to be called the TSP under which the NSA was authorized to intercept the content of specific international communications (*i.e.*, to or from the United States) involving persons reasonably believed to be associated with al Qaeda and affiliated terrorist organizations. The term "content" is used herein to refer to the substance, meaning, or purport of a communication, as defined in 18 U.S.C. § 2510(8), as distinguished from the type of addressing or routing information referred to herein as "metadata."

1 information about a number of sensitive programs undertaken under the authority of the FISA.
2 Certain of the information that the DNI has declassified concerns the allegations raised in this
3 litigation, and this information has been described in great detail in the classified declarations
4 referenced above. In addition, the President has declassified the fact of the existence of two
5 portions of the discontinued President's Surveillance Program, which also concern the
6 allegations at issue in this litigation. I summarize these various official disclosures below.

7 **1. Collection of Bulk Telephony Metadata Under Section 215 of the FISA**

8 21. First, since May 2006, under a provision of the FISA known as Section 215 and
9 codified at 50 U.S.C. § 1861, the NSA obtains, pursuant to orders of the FISC, bulk telephony
10 metadata – business records created by telecommunications service providers that include such
11 information as the telephone numbers placing and receiving calls, and the time and duration of
12 those calls.⁵ The Government has declassified and publicly disclosed a number of “primary”
13 orders of the FISC to the Government authorizing it to carry out the bulk telephony metadata
14 program. The Government has acknowledged only one “secondary” FISC order, however, to
15 one telecommunications service provider (Verizon Business Network Services, Inc. (“VBNS”)),
16 and for only one approximately 90-day period of time (from April 25, 2013 to July 19, 2013).
17 The Government acknowledged this secondary order only after the order was disclosed
18 unlawfully and without authorization. This is the only FISC order identifying any particular
19 provider that has been declassified and, since the disclosure of this order in June 2013, the
20 United States has continued to protect against any further disclosures of FISC orders directed at

⁵ Under the terms of the FISC's orders, the NSA is authorized to collect information including, as to each call, the telephone numbers that placed and received the call, other session-identifying information (e.g., International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card number, and the date, time, and duration of a call.

1 any provider under the telephony metadata program. While the authentication of that order
2 means that the identity of one participating provider has been officially acknowledged for the
3 particular time period of that order, the order was limited to VBNS, did not identify any other
4 provider, did not relate to any other corporate component of Verizon other than VBNS, and was
5 of limited duration (expiring on July 19, 2013). There has been no official acknowledgement of
6 whether or not VBNS assisted the NSA with the FISC telephony metadata program either before
7 or after the period covered by the April 2013 order, or whether VBNS continues to participate in
8 the program. The identities of the providers that furnish assistance to the NSA under the
9 telephony metadata program, including VBNS, as to any other time period other than the
10 approximately 90-day duration of that order, have not been declassified and remains currently
11 and properly classified.

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

21 23. The NSA stores and analyzes this information under carefully controlled
22 circumstances and under stringent supervision and oversight by all three branches of
23 Government. The vast majority of the metadata are never seen by any person. Rather, the NSA
24 has been authorized to query the archived data solely with identifiers, typically telephone

1 numbers, for which there are facts giving rise to a reasonable, articulable suspicion (“RAS”) that
2 the number is associated with one or more of the foreign terrorist organizations that are the
3 subject of FBI investigations previously identified to the FISC. Where the identifier is
4 reasonably believed to be used by a U.S. person, the NSA may not make the RAS determination
5 solely based on activities protected by the First Amendment.

6 24. The accessible results of an approved query are limited to records of
7 communications within three “hops” from the seed identifier.⁶ That is, the query results may
8 only include identifiers having a direct contact with the seed (the first “hop”), identifiers having a
9 direct contact with the first “hop” identifiers (the second “hop”), and identifiers having a direct
10 contact with second “hop” identifiers (the third “hop”). By querying the metadata using the RAS
11 standard, NSA intelligence analysts are able to: (1) detect domestic identifiers calling foreign
12 identifiers associated with one of the foreign terrorist organizations and discover identifiers that
13 the foreign identifiers are in contact with; (2) detect foreign identifiers associated with a foreign
14 terrorist organization calling into the U.S. and discover which domestic identifiers are in contact
15 with the foreign identifiers; and (3) detect possible terrorist-related communications occurring
16 between communicants located inside the U.S.

17 25. The Government has also publicly disclosed FISC orders and opinions concerning
18 various failures to fully implement and comply with FISC-ordered procedures for the telephony
19 metadata collection program. These compliance incidents were due to human error and
20 technological issues. In 2009, the Government reported these problems to the FISC (and
21 Congress) and remedied them, and the FISC (after temporarily suspending the Government’s

⁶ A “seed” is an initial identifier used to generate a query.

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

3 **2. Bulk Collection of Internet Metadata**

4 26. Second, the Government has recently declassified and acknowledged the
5 existence of FISC-authorized bulk collection of Internet metadata carried out under the "pen
6 register, trap and trace" ("PRTT") provision of the FISA. The data collected included certain
7 routing, addressing, and signaling information such as the "to" and "from" lines of an email and
8 the date and time the email was sent, but not the content of an email or the subject line. Certain
9 telecommunications service providers were compelled to provide this transactional information,
10 which the NSA analyzed to obtain foreign intelligence information. The FISC's orders
11 authorizing this collection required the Government to comply with minimization procedures
12 limiting the retention and dissemination of the metadata, including a requirement of a reasonable,
13 articulable suspicion that selection terms used to query the bulk data were associated with
14 foreign terrorist organizations.⁷ This program of bulk Internet metadata collection was
15 terminated in 2011, because it did not meet the operational expectations the NSA had for it.

16 **3. Collection of Communications Content Pursuant to Section 702 of FISA.**

17 27. Third, the Government has publicly revealed certain information about its use of
18 authority conferred by Section 702 of the FISA to collect, for foreign intelligence purposes,
19 certain communications of non-U.S. persons located outside the United States, pursuant to
20 approval of the FISC. Section 702 facilitates the targeted acquisition of foreign intelligence

⁷ Similar to the telephony metadata program (*see supra* ¶ 34), the Government has also publicly disclosed FISC orders and opinions concerning various failures to fully implement and comply with FISC-ordered procedures for the Internet metadata collection program. These compliance incidents were due to human error and technological issues. In 2009, the Government reported these problems to the FISC (and Congress) and remedied them.

1 information concerning foreign targets located outside the United States under court oversight.
2 Electronic communication service providers are compelled to supply information to the
3 Government pursuant to authorized directives issued by the Attorney General and the DNI.

4 28. Once targeted surveillance under Section 702 has been authorized, the NSA takes
5 the lead in tasking relevant telephone and electronic communications selectors to target specific
6 non-U.S. persons reasonably believed to be located outside the United States. Consistent with
7 the statute, the NSA's targeting procedures require that there be an appropriate, documented
8 foreign intelligence purpose for the acquisition and that the selector be used by a non-U.S.
9 person reasonably believed to be located outside the United States.

10 29. Once a target has been approved, the NSA uses two means to acquire the target's
11 electronic communications. First, it acquires such communications directly from compelled
12 U.S.-based providers. This has been publicly referred to as the NSA's PRISM collection.
13 Second, in addition to collection directly from providers, the NSA performs "upstream
14 collection" of Internet communications. The NSA has strict minimization and dissemination
15 procedures, and as is the case with the telephony metadata program, the NSA's Section 702
16 collection activities are subject to extensive oversight by all three branches of the Government.

17 30. As with the telephony metadata program, the Government has also disclosed
18 compliance incidents involving its Section 702 collection activities. In an opinion issued on
19 October 3, 2011, the FISC found the NSA's proposed minimization procedures as applied to the
20 NSA's upstream collection of Internet transactions containing multiple communications, or
21 "MCTs," deficient. Oct. 3, 2011 FISC Op., 2011 WL 10945618. In response, the NSA modified
22 its proposed procedures and the FISC subsequently determined that the NSA adequately
23 remedied the deficiencies such that the procedures met the applicable statutory and constitutional

1 requirements, and allowed the collection to continue. Aug. 24, 2012 FISC Op., 2012 WL
2 9189263, at *2-3; Nov. 30, 2011 FISC Op., 2011 WL 10947772.

3 **4. Presidentially Authorized NSA Activities After 9/11**
4

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

16 32. Starting on October 4, 2001, President Bush authorized the Secretary of Defense
17 to employ the capabilities of the Department of Defense, including the NSA, to collect foreign
18 intelligence by electronic surveillance in order to detect and prevent acts of terrorism within the
19 United States. President Bush authorized the NSA to collect: (1) the contents of certain
20 international communications, a program that was later referred to as the TSP; and (2) telephony
21 and Internet non-content metadata in bulk, subject to various conditions.

22 33. President Bush issued authorizations approximately every 30-60 days. Although
23 the precise terms changed over time, each presidential authorization required the minimization of
24 information collected concerning American citizens to the extent consistent with the effective

1 accomplishment of the mission of detection and prevention of acts of terrorism within the United
2 States. The NSA applied additional internal constraints on the presidentially-authorized
3 activities.

4 34. Over time, the presidentially-authorized activities transitioned to the authority of
5 the FISA. The collection of communications content pursuant to presidential authorization
6 ended in January 2007 when the Government transitioned the TSP to the authority of the FISA
7 and under the orders of the FISC. In August 2007, Congress enacted the Protect America Act
8 (“PAA”) as a temporary measure. The PAA, which expired in February 2008, was replaced by
9 the FISA Amendments Act of 2008 (“FAA”), which was enacted in July 2008 and remains in
10 effect today. Today, content collection is conducted pursuant to section 702 of the FISA. The
11 metadata activities also were transitioned to orders of the FISC. The bulk collection of telephony
12 metadata transitioned to the authority of the FISA in May 2006 and is collected pursuant to
13 Section 215 of FISA. The bulk collection of Internet metadata was transitioned to the authority
14 of the FISA in July 2004 and was collected pursuant to Section 402 of FISA. In December 2011,
15 the Government decided not to seek reauthorization of the bulk collection of Internet metadata.

16 **IV. INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE**

17 35. While information about the existence of the components of the PSP has now
18 been declassified, specific operational details concerning the program’s scope, operation, the
19 sources and methods it utilized, and intelligence it produced remain properly classified and are
20 subject to the DNI’s state secrets privilege assertion and my own assertion of NSA’s statutory
21 privilege in this declaration. In general and unclassified terms, the DNI’s assertion of the state
22 secrets privilege and my statutory privilege assertion encompasses the following categories of
23 still-classified information and properly protected national security information concerning NSA
24 activities:

1 **A. Persons Subject to Intelligence Activities:** information that would tend to confirm
2 or deny whether particular individuals, including the named plaintiffs, have been
3 subject to any NSA intelligence activities;

4
5 **B. Operational Information Concerning NSA Intelligence Activities:** information
6 concerning the scope and operational details of NSA intelligence activities that may
7 relate to or be necessary to adjudicate plaintiffs' allegations, including:

8
9 (1) Communications Content Collection: information concerning the
10 scope or operational details of NSA intelligence activities that may relate
11 to or be necessary to adjudicate plaintiffs' claims that the NSA
12 indiscriminately intercepts the content of communications, *see, e.g., Jewel*
13 Complaint ¶¶ 9, 10, 73-77; *Shubert* SAC ¶¶ 1, 2, 7, 64-70, including:

14
15 (a) *TSP Information*: information concerning the scope
16 and operation of the now inoperative TSP regarding the
17 interception of the content of certain international
18 communications reasonably believed to involve a
19 member or agent of al Qaeda or an affiliated terrorist
20 organization;

21
22 (b) *FISA Section 702*: information concerning
23 operational details related to the collection of
24 communications under FISA section 702; and

25
26 (c) Any other information related to demonstrating that
27 the NSA has not otherwise engaged in the content-
28 surveillance dragnet that the plaintiffs allege.

29
30 (2) Communications Records Collection: information concerning the
31 scope or operational details of NSA intelligence activities that may relate
32 to or be necessary to adjudicate plaintiffs' claims regarding the NSA's
33 bulk collection of telephony and Internet non-content communications
34 records ("metadata"), *see, e.g., Jewel* Complaint ¶¶ 10, 11, 13, 73-77, 82-
35 97; *Shubert* SAC ¶¶ 102;

1
2 **C. Telecommunication Provider Identities:** information that may tend to
3 confirm or deny whether AT&T or Verizon (and to the extent relevant or necessary,
4 any other telecommunications carrier) has provided assistance to the NSA in
5 connection with any intelligence activity, including the collection of communications
6 content or non-content transactional records alleged to be at issue in this litigation.
7

8 **V. HARM OF DISCLOSURE OF PRIVILEGED INFORMATION**

9 **A. Information Concerning Whether Plaintiffs Have Been Subject**
10 **to the Alleged NSA Activities**

11 36. The first major category of information as to which I am supporting the DNI's
12 assertion of privilege, and asserting the NSA's own statutory privilege, concerns information as
13 to whether particular individuals, including the named plaintiffs in this lawsuit, have been
14 subject to alleged NSA intelligence activities. As set forth below and in my classified
15 declaration, confirmation or denial of such information by the NSA reasonably could be
16 expected to cause exceptionally grave damage to the national security. The named plaintiffs in
17 the *Jewel* and *Shubert* cases allege that the content of their own telephone and Internet
18 communications has been and continues to be subject to unlawful search and seizure by the
19 NSA, along with the content of communications of millions of ordinary Americans.⁸ Further,

⁸ 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 messaged, web and other communications, both international and domestic, of millions of ordinary Americans – “practically every American who uses the phone system or the Internet” – including the plaintiffs. *See Jewel* Compl. ¶¶ 7, 9, 10; *see also id.* at ¶¶ 39-97. The *Shubert* plaintiffs allege that the contents of “virtually every telephone, Internet and email communication sent from or received within the United States since shortly after September 11, 2001,” including plaintiffs’ communications, are being “searched, seized, intercepted, and subject to surveillance without a warrant, court order or any other lawful authorization in violation of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1810.” *See Shubert* SAC ¶ 1; *see also id.* ¶¶ 5, 7.

1 the named plaintiffs allege that the NSA has been and is continuing to collect and analyze the
2 private telephone and Internet transaction records of millions of Americans, with the assistance
3 of telecommunication carriers, again including information concerning the plaintiffs' telephone
4 and Internet communications.⁹

5 37. As a matter of course, the NSA cannot publicly confirm or deny whether any
6 individual is or has been subject to intelligence-gathering activities because to do so would tend
7 to reveal actual targets or subjects. The harm of revealing the identities of persons who are the
8 actual targets or subjects of foreign intelligence gathering is relatively straightforward. If an
9 individual knows or suspects he is a target or subject of U.S. intelligence activities, he would
10 naturally tend to alter his behavior to take new precautions against such scrutiny. In addition,
11 revealing who is not a target or subject of intelligence gathering would indicate who has avoided
12 surveillance or collection and what may be a secure channel for communication. Such
13 information could lead an actual or potential adversary, secure in the knowledge that he is not
14 under government scrutiny, to help a hostile foreign adversary convey information; alternatively,
15 such a person may be unwittingly utilized or even forced to convey information through a secure
16 channel to a foreign adversary. Revealing which channels are free from surveillance and which
17 are not would also reveal sensitive intelligence methods and thereby could help any adversary
18 evade detection and capitalize on limitations in NSA's capabilities. Similar harms would result
19 from confirming or denying whether a person's communications have been subject to collection

⁹ Specifically, the *Jewel* plaintiffs allege that the NSA has “unlawfully solicited and obtained from telecommunications companies the complete and ongoing disclosure of the private telephone and internet transactional records” of millions of ordinary Americans, including plaintiffs. *See Jewel* Compl. ¶¶ 7, 10, 11, 13, 82-97. They further claim the NSA analyzes this information. *Id.* ¶ 11. The *Shubert* plaintiffs allege that “NSA now monitors huge volumes of records of domestic emails and Internet searches...[and] receives this so-called ‘transactional’ data from...private companies...” *See Shubert* SAC ¶ 102.

1 even where it may be assumed a person is law-abiding and not likely to be an actual target or
2 subject of such activity. For example, if the NSA were to confirm that specific individuals have
3 not been targets of or subject to collection (*i.e.*, whether their communications have been
4 intercepted), but later refuse to comment (as it would have to) in a situation involving an actual
5 target or subject, an actual or potential adversary of the United States could likewise seek such
6 confirmation or denial and then easily deduce by comparing such responses that the person in the
7 latter instance is or has been a target of or subject to surveillance or other intelligence-gathering
8 activity. In addition, disclosure of whether a person's communications have or have not been
9 targeted or intercepted through the targeting of a third party would reveal whether a particular
10 channel of communication is secure and also reveal to third-party targets whether their own
11 communications may be secure.

12 **B. Operational Information Concerning NSA Intelligence**
13 **Activities**

14 38. I am also supporting the DNI's assertion of privilege and asserting the NSA's
15 statutory privilege over any other still-classified facts concerning NSA intelligence activities,
16 sources, or methods that may relate to or be necessary to litigate the plaintiffs' claims and
17 allegations, including that: (1) the NSA is indiscriminately intercepting the content of
18 communications of millions of ordinary Americans, *see e.g.*, *Jewel* Complaint ¶¶ 7, 9, 10;
19 *Shubert* SAC ¶¶ 1, 5, 7; and (2) that the NSA is collecting the private telephone and Internet
20 transactional records of Americans with the assistance of telecommunications carriers, again
21 including information concerning the plaintiffs' telephone and Internet communications. *See*
22 *Jewel* Complaint ¶¶ 7, 10, 11, 13, 82-97; *see Shubert* SAC ¶ 102. As described above, the scope
23 of the Government's privilege assertion includes but is not limited to still-classified information
24 concerning (1) the collection of communication content under the now inoperative TSP as well

1 as pursuant to authority of FISA Section 702, and any other NSA activities that would be at risk
2 of disclosure or required in demonstrating that the NSA has not engaged in content “dragnet”
3 surveillance activities that plaintiffs allege; and (2) information that may relate to or be necessary
4 to adjudicate plaintiffs’ claims regarding the NSA’s bulk collection of telephony and Internet
5 communication records. As set forth below and in my classified declaration, the disclosure of
6 such information would cause exceptionally grave harm to national security.

7 **1. Information Concerning Plaintiffs’ Content Surveillance Allegations**

8 39. After the existence of the TSP was officially acknowledged in December 2005,
9 the Government stated that this activity was limited to the interception of the content of certain
10 communications for which there were reasonable grounds to believe that: (1) such
11 communication originated or terminated outside the United States; and (2) a party to such
12 communication is a member or agent of al Qaeda or an affiliated terrorist organization.

13 Nonetheless, plaintiffs’ allege that the NSA indiscriminately intercepts the content of
14 communications of millions of ordinary Americans. *See e.g., Jewel* Complaint ¶¶ 7, 9, 10; *see*
15 *Shubert* SAC ¶¶ 1, 5, 7. As the Government has also previously stated,¹⁰ plaintiffs’ allegation
16 that the NSA has undertaken indiscriminate surveillance of the content¹¹ of millions of
17 communications sent or received by people inside the United States after 9/11 under the TSP is
18 false. But in order to disprove plaintiffs’ claim that the NSA indiscriminately collected the

¹⁰ *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).

¹¹ Again, the term “content” is used herein to refer to the substance, meaning, or purport of a communication as defined in 18 U.S.C. § 2510(8).

1 content of the communications of millions of Americans, the NSA would have to disclose the
2 specifics of its content collection activities. Under the TSP, the NSA was directed pursuant to
3 presidential authorization to intercept the content of only those international telephone and
4 Internet communications for which there were reasonable grounds to believe that such
5 communications involved a member or agent of al Qaeda or an affiliated terrorist organization.
6 To the extent the NSA must demonstrate that content surveillance under the TSP was so limited,
7 and was not plaintiffs' alleged content "dragnet," or demonstrate that the NSA has not otherwise
8 engaged in the alleged content "dragnet," highly classified NSA intelligence sources and
9 methods about the operation of the TSP and current NSA intelligence activities (including under
10 FISA Section 702) would be subject to disclosure or the risk of disclosure. The disclosure of
11 whether and to what extent the NSA utilizes certain intelligence sources and methods would
12 reveal to foreign adversaries the NSA's capabilities, or lack thereof, enabling them to either
13 evade particular channels of communications that are being monitored, or exploit channels of
14 communication that are not subject to NSA activities, in either case risking exceptionally grave
15 damage to national security. As set forth below and in my classified declaration, a range of
16 operational details concerning the TSP, as well as other NSA sources and methods, remains
17 properly classified and privileged from disclosure, and could not be revealed to address
18 plaintiffs' content "dragnet" allegations.

19 40. Authorization of the TSP was intended to address an important gap in NSA's
20 intelligence collection activities---namely, that significant changes in communications
21 technology since the enactment of the FISA in 1978 meant that the NSA faced great difficulties
22 in identifying foreign terrorist operatives who were communicating with individuals within the
23 United States. FISA established the framework for court approval of the U.S. Government's
24 efforts to conduct foreign intelligence surveillance of individuals in the United States. When

1 FISA was enacted in 1978, most international communications to or from the United States were
2 transmitted via satellite or radio technology. Congress intentionally excluded the vast majority
3 of satellite or radio communications from the definition of “electronic surveillance” in the FISA.
4 See 50 U.S.C. §1801(f).

5 41. Since the time FISA was enacted, sweeping advances in modern
6 telecommunications technology upset the balance struck by Congress in 1978. By 2001, most
7 international communications to or from the United States were carried on a wire and many
8 domestic communications had increasingly become wireless. As a result of this change in
9 communications technology, the NSA’s collection from inside the United States of international
10 communications (previously carried primarily via radio transmission) had shrunk considerably
11 and the Government was forced to prepare FISA applications if it wished to collect the
12 communications of non-U.S. persons located overseas. These circumstances presented a
13 significant concern in the exceptional circumstances after 9/11.

14 **2. Information Concerning Plaintiffs’ Communications Records Collection**
15 **Allegations**
16

17 42. Plaintiffs also allege that the NSA is collecting the private telephone and Internet
18 transaction records of millions of Americans, again including information concerning plaintiffs’
19 telephone and Internet communications. *See, e.g., Jewel* Complaint ¶¶ 7, 10, 11, 13, 8, 13, 82-
20 97; *see Shubert* SAC ¶ 102. To address these allegations would risk or require disclosure of
21 NSA sources and methods and reasonably could be expected to cause exceptionally grave
22 damage to national security. While the Government has declassified the existence of the
23 telephony and Internet metadata collections, and some information concerning those programs as
24 authorized by the FISC, significant operational details concerning these activities remain
25 properly classified, including the identity of communication providers who may have assisted in

1 this collection, and other sources and method of collection and analysis. As set forth below and
2 in my classified declaration, disclosure of this information reasonably could be expected to cause
3 grave damage to national security.

4 **(a) Collection of Bulk Telephony Metadata**

5
6 43. As with the operational details concerning the NSA's collection of
7 communications content, I am supporting the DNI's state secrets privilege assertion, and
8 asserting NSA's statutory privilege, over still-classified information that may relate to or be
9 necessary to litigate plaintiffs' claims as they relate to the alleged collection of telephony
10 metadata.

11 44. The still classified operational details concerning the collection of telephony
12 metadata include, but are not necessarily limited to, whether metadata of plaintiffs' telephone
13 communications were actually collected by the NSA from plaintiffs' particular communications
14 providers; whether any metadata of plaintiffs' telephone communications, if collected, were
15 viewed or analyzed by anyone at the NSA; information demonstrating the scope of the telephony
16 metadata collection program; and information demonstrating the need for and effectiveness of
17 the program

18 45. As set forth in this declaration, following the unauthorized disclosure in June
19 2013 of one FISC order issued as part of the telephony metadata program, the Government
20 confirmed the authenticity of one order, issued on April 25, 2013, by the FISC to a particular
21 Verizon Communications subsidiary, Verizon Business Network Services (VBNS), thereby
22 confirming the participation of VBNS in the program for the duration of that order
23 (approximately 90 days). This is the only FISC order identifying any particular provider under
24 this program that has been declassified, and since the disclosure of this order in June 2013, the

1 United States has not confirmed or denied the past or current participation of any specific
2 provider in the telephony metadata program apart from the participation of VBNS for the
3 approximately 90 day duration of the now-expired April 25, 2013, FISC order. As explained in
4 my classified declaration, the continued protection of whether or not, or to what extent, a
5 particular telecommunications provider assisted the NSA under FISC order or otherwise remains
6 an extraordinarily sensitive and significant matter that the Government continues to protect to
7 avoid even greater harm to national security than has already occurred since June 2013.

8 46. **(b) Internet Metadata Collection**

9 47. I am also supporting the DNI's privilege assertion, and asserting the NSA's
10 statutory privilege, over still-classified operational details concerning the NSA's bulk collection
11 of Internet metadata under presidential authorization.. Disclosure of these details, which are set
12 forth in my classified declaration, reasonably could be expected to cause exceptionally grave
13 damage to national security, for the reasons set forth in my classified declaration.

14 3. **Information Concerning Whether or Not Any Specific Carrier Provided**
15 **Assistance to the NSA**

16
17 48. I am also supporting the DNI's state secrets privilege assertion, and asserting
18 NSA's statutory privilege, over information relating to which carriers have assisted the NSA
19 under presidential authorization and other authorities. The *Jewel* plaintiffs and three of the
20 *Shubert* plaintiffs allege that they are customers of AT&T, and that AT&T participated in the
21 alleged intelligence-gathering activities that the plaintiffs seek to challenge. Additionally, at
22 least one *Shubert* plaintiff also claims to be a customer of Verizon, and that Verizon similarly
23 participated in the alleged intelligence-gathering activities that the plaintiffs seek to challenge.
24 The harm from officially acknowledging whether or not any specific carrier has assisted the NSA
25 is significant, as set forth in my classified declaration, and continues to exist notwithstanding the

1 recent official disclosures. While the Government has declassified some information concerning
2 the nature and scope of the programs described above and in my classified declaration --
3 including that it collects telephony and Internet metadata in bulk, from multiple
4 telecommunication providers -- and has also confirmed the authenticity of a single now-expired
5 FISC order issued to a single carrier that had been unlawfully disclosed, it has not otherwise
6 declassified information concerning the identities of companies that are or were subject to FISC
7 orders under NSA intelligence-gathering programs, or have otherwise assisted the NSA.

8 **IV. CONCLUSION**

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

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

