

1 MICHAEL F. HERTZ
2 Acting Assistant Attorney General
3 DOUGLAS N. LETTER
4 Terrorism Litigation Counsel
5 JOSEPH H. HUNT
6 Director, Federal Programs Branch
7 VINCENT M. GARVEY
8 Deputy Branch Director
9 ANTHONY J. COPPOLINO
10 Special Litigation Counsel
11 U.S. Department of Justice
12 Civil Division, Federal Programs Branch
13 20 Massachusetts Avenue, NW
14 Washington, D.C. 20001
15 Phone: (202) 514-4782
16 Fax: (202) 616-8460

17 *Attorneys for the United States and
18 Government Defendants Sued in their
19 Official Capacities*

20 UNITED STATES DISTRICT COURT

21 NORTHERN DISTRICT OF CALIFORNIA

22 CAROLYN JEWEL, *et al.*) No. 08-cv-4873-VRW
23 Plaintiffs,)
24 v.) CLASSIFIED DECLARATION
25 NATIONAL SECURITY AGENCY *et al.*) OF DEBORAH A. BONANNI,
26 Defendants.) NATIONAL SECURITY AGENCY
27)
28) EX PARTE, IN CAMERA
29) SUBMISSION
30)
31) Date: June 25, 2009
32) Time: 2:30 p.m.
33) Courtroom 6, 17th Floor
34)
35) Chief Judge Vaughn R. Walker

Derived From: NSA/CSSM 1-52
Dated: 20090403
Declassify On: 20340403

Classified In Camera, Ex Parte Declaration of Deborah A. Bonanni, National Security Agency
Carolyn Jewel, et al. v. National Security Agency, et al. (No. 08-cv-4873-VRW)

(U) Table of Contents

- I. (U) Introduction
 - II. (U) Summary
 - III. (U) Classification of Declaration
 - IV. (U) Background Information
 - A. (U) The National Security Agency
 - B. (U) September 11, 2001 and the al Qaeda Threat.
 - C. (U) Summary of NSA Activities After 9/11 to Meet al Qaeda Threat
 - V. (U) NSA Information Protected by Privilege Assertions
 - VI. (U) Description of Information Subject to Privilege and the Harm of Disclosure
 - A. (U) Information That May Tend to Confirm or Deny Whether or Not the Plaintiffs Have Been Subject to the Alleged NSA Activities
 - B. (U) Information Related to NSA Activities, Sources, and Methods Implicated by Plaintiffs' Allegations
 - 1. (U) Plaintiffs' Allegations of a Communications Dragnet
 - (a) (U) Information Related to Terrorist Surveillance Program
 - (b) (U) Plaintiffs' Allegations Concerning the Collection of Communication Records
 - 2. (FIS//SI//OCANE) Information Concerning Current FISA Authorized Activities and Specific FISC Orders.
 - 3. (U) Plaintiffs' Allegations that AT&T Provided Assistance to the NSA with the Alleged Activities
 - VII. (U) Risks of Allowing Litigation to Proceed
 - VIII. (U) Summary and Conclusion

TOP SECRET//TSP//SI [REDACTED] //ORCON/NOFORN
CLASSIFIED DECLARATION OF DEBORAH A. BONANNI
NATIONAL SECURITY AGENCY

(U) I, Deborah A. Bonanni, do hereby state and declare as follows:

I. (U) Introduction

1. (U) I am the Chief of Staff for the National Security Agency (NSA), an intelligence agency within the Department of Defense. I have held this position since February 2006. As the Chief of Staff, under our internal regulations, and in the absence of the Deputy Director and the 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. 12958, 60 Fed. Reg. 19825 (1995), as amended on March 25, 2003, and Department of Defense Directive No. 5200.1-R, Information Security Program Regulation, 32 C.F.R. § 159a.12 (2000).

2. (U) The purpose of this declaration is to support an assertion of the military and state secrets privilege (hereafter "state secrets privilege") by the Director of National Intelligence ("DNI") as the head of the intelligence community, as well as the DNI's assertion of a statutory privilege under the National Security Act, to protect information related to NSA activities described herein below. Lieutenant General Keith Alexander, the Director of the National Security Agency, has been sued in his official and individual capacity in the above captioned case and has recused himself from the decision of whether to assert the statutory privilege in his official capacity. As the Deputy Director is currently out of the office on temporary duty, by operation of our internal regulations 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 Chief of Staff of the NSA.

II. (U) Summary

3. (U) In the course of my official duties, I have been advised of this litigation and I have reviewed the allegations in the Complaint in this case. In sum, plaintiffs allege that, after the 9/11 attacks, the NSA received presidential authorization to engage in surveillance activities far broader than the publicly acknowledged "Terrorist Surveillance Program" ("TSP"), which involved the interception of specific international communications involving persons reasonably believed to be associated with al Qaeda and affiliated terrorist organizations. Plaintiffs allege that the NSA, with the assistance of telecommunication companies including AT&T, 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 Complaint at ¶¶ 2-13; 39-97. I cannot disclose on the public record the nature of any NSA information implicated by the plaintiffs' allegations. However, as described further below, the disclosure of information related to the NSA's activities, sources and methods implicated by the plaintiffs' allegations reasonably could be expected to cause exceptionally grave damage to the national security of the United States and, for this reason, are encompassed by the DNI's state secrets and statutory privilege assertions, as well as by my assertion of the NSA statutory privilege, and should be protected from disclosure in this case. In addition, it is my judgment that sensitive state secrets are so central to the subject matter of the litigation that any attempt to proceed in the case risks the disclosure of the classified privileged national security information

described herein and exceptionally grave damage to the national security of the United States.

4. ~~(TS//TSP//SI//OC/NF)~~ The allegations in this lawsuit put at issue the disclosure
of information concerning several highly classified and critically important NSA intelligence
activities that commenced after the 9/11 terrorist attacks, but which are now conducted pursuant
to authority of the Foreign Intelligence Surveillance Act ("FISA"), including ongoing activities
conducted under orders approved by the Foreign Intelligence Surveillance Court ("FISC").

8 Plaintiffs' allegation that the NSA undertakes indiscriminate surveillance of the *content*¹ of
9 millions of communications sent or received by people inside the United States---under the now
10 defunct-TSP or otherwise---is false, as discussed below. The NSA's collection of the content of
11 communications under the TSP was directed at international communications in which a
12 participant was reasonably believed to be associated with al Qaeda or an affiliated organization
13 and did not constitute the kind of dragnet collection of the content of millions of Americans'
14 telephone or Internet communications that the plaintiffs allege. Although the existence of the
15 TSP has been acknowledged, the details of that program remain highly classified, along with
16 details of related content surveillance activities undertaken after the TSP pursuant to orders of
17 the FISC. This information could not be disclosed to address or disprove or otherwise litigate
18 the plaintiffs' allegation of a content dragnet without causing exceptional harm to NSA's sources
21 and methods of gathering intelligence---including methods currently used to detect and prevent
22 further terrorist attacks under the authority of the FISA.

24 5. ~~(TS//TSP//SI//OC/NF)~~ In addition, as the Court should also be aware from prior
25 classified declarations submitted by the NSA in related proceedings, the NSA has collected,
26 pursuant to presidential authorization and currently under subsequent FISC orders, non-content

¹ ~~(TS//SI//OC/NF)~~ The term "content" is used herein to refer to the substance, meaning,
or purport of a communication, as defined in 18 U.S.C. § 2510(8), as opposed to the type of
addressing or routing information referred throughout this declaration as "meta data."

1 information (i.e., meta data) about telephone and Internet communications in order to enable
2 highly sophisticated analytical tools that can uncover the contacts [REDACTED] of
3 members or agents of [REDACTED]² As noted above and detailed
4 below, the content surveillance subject to presidential authorization after 9/11 was not the
5 content dragnet surveillance that plaintiffs allege, and the collection of non-content information,
6 while significant in scope remains a highly classified matter currently under FISA authorization.
7 For the NSA to attempt to explain, clarify, disprove, or otherwise litigate plaintiffs' allegations
8 regarding a communications dragnet would require the NSA to confirm the existence of, or
9 disclose facts concerning, intelligence sources and methods for the collection of non-content
10 information related to communications, as well as current NSA operations under FISC Orders---
11 disclosures that would cause exceptional harm to national security.
12

13
14 6. (TS//SI [REDACTED]//TSP//OC/NF) In addition, plaintiffs' allegation that
15 telecommunications carriers, in particular AT&T, assisted the NSA in alleged intelligence
16 activities cannot be confirmed or denied without risking exceptionally grave harm to national
17 security. Because the NSA has not undertaken the alleged dragnet collection of communications
18 content, no carrier has assisted in that alleged activity. [REDACTED]
19

20
21
22
23
24
25
26
27 ² (TS//SI//OC/NF) Certain FISC Orders are also directed at [REDACTED]
28 Because the allegations in the complaint reference activities
 authorized after 9/11, which were directed at [REDACTED] any
 further references to the FISC Orders will focus solely on activities under the orders directed at
 [REDACTED]

1 [REDACTED]
2 [REDACTED] Disclosure of [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED] would cause exceptionally grave damage to the
6 national security.
7

8 7. (TS//SI- [REDACTED] //TSP//OC/NF) Accordingly, the DNI's state secrets and
9 statutory privilege assertions, and my own statutory privilege assertion, seek to protect against
10 the disclosure of the highly classified intelligence sources and methods put at issue in this case
11 and vital to the national security of the United States, including: (1) any information that would
12 tend to confirm or deny whether particular individuals, including the named plaintiffs, have been
13 subject to the alleged NSA intelligence activities; (2) information concerning NSA intelligence
14 sources and methods, including facts demonstrating that the content collection under the TSP
15 was limited to specific al Qaeda and associated terrorist-related international communications
16 and was not a content surveillance dragnet as plaintiffs allege; (3) facts that would tend to
17 confirm or deny the existence of the NSA's bulk meta data collection and use, and any
18 information about those activities; and (4) the fact that [REDACTED]
19

20 [REDACTED] The fact that there has been public speculation
21 about alleged NSA activities does not diminish the need to protect intelligence sources and
22 methods from further exposure. Official confirmation and disclosure of the classified privileged
23 national security information described herein would cause exceptionally grave damage to the
24 national security. For these reasons, as set forth further below, I request that the Court uphold
25 the state secrets and statutory privilege assertions that the DNI and I now make, and protect the
26 information described in this declaration from disclosure.
27
28

III. (U) Classification of Declaration

1 8. (S//SI//NF) This declaration is classified TOP SECRET//TSP//SI-ECI
2 [REDACTED] ORCON/NOFORN pursuant to the standards in Executive Order No. 12958, as amended
3 by Executive Order No. 13292. Under Executive Order No. 12958, information is classified
4 "TOP SECRET" if unauthorized disclosure of the information reasonably could be expected to
5 cause exceptionally grave damage to the national security of the United States; "SECRET" if
6 unauthorized disclosure of the information reasonably could be expected to cause serious
7 damage to national security; and "CONFIDENTIAL" if unauthorized disclosure of the
8 information reasonably could be expected to cause identifiable damage to national security. At
9 the beginning of each paragraph of this declaration, the letter or letters in parentheses
10 designate(s) the degree of classification of the information the paragraph contains. When used
11 for this purpose, the letters "U," "C," "S," and "TS" indicate respectively that the information is
12 either UNCLASSIFIED, or is classified CONFIDENTIAL, SECRET, or TOP SECRET³.
13

14 9. (S//SI//NF) Additionally, this declaration also contains Sensitive Compartmented
15 Information (SCI), which is "information that not only is classified for national security reasons
16 as Top Secret, Secret, or Confidential, but also is subject to special access and handling
17 requirements because it involves or derives from particularly sensitive intelligence sources and
18 methods." 28 C.F.R. § 17.18(a). Because of the exceptional sensitivity and vulnerability of such
19 information, these safeguards and access requirements exceed the access standards that are
20

21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

1 normally required for information of the same classification level. Specifically, this declaration
2 references communications intelligence (COMINT), also referred to as special intelligence (SI),
3 which is a subcategory of SCI. COMINT or SI identifies SCI that was derived from exploiting
4 cryptographic systems or other protected sources by applying methods or techniques, or from
5 intercepted foreign communications.

6
7 10. (TS//SI-[REDACTED]//TSP//OC/NF) This declaration also contains information
8 related to or derived from the Terrorist Surveillance Program (TSP), a controlled access signals
9 intelligence program under presidential authorization in response to the attacks of September 11,
10 2001. Although TSP was publicly acknowledged by then-President Bush in December 2005,
11 details about the program remain highly classified and strictly compartmented. Information
12 pertaining to this program is denoted with the special marking "TSP" and requires more
13 restrictive handling.
14 [REDACTED]

15
16
17
18
19
20
21
22 11. (S//SI//NF) In addition to the fact that classified information contained herein
23 may not be revealed to any person without authorization pursuant to Executive Order 12958, as
24 amended, this declaration contains information that may not be released to foreign governments,
25 foreign nationals, or non-U.S. citizens without permission of the originator and in accordance
26
27
28 [REDACTED]

1 with DNI policy. This information is labeled 'NOFORN.' The "ORCON" designator means
2 that the originator of the information controls to whom it is released.

3 **IV. (U) Background Information**

4 **A. (U) The National Security Agency**

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

11 13. (FIPS//SI) Signals intelligence (SIGINT) consists of three subcategories:
12 (1) communications intelligence (COMINT); (2) electronic intelligence (ELINT); and (3) foreign
13 instrumentation signals intelligence (FISINT). Communications intelligence (COMINT) is
14 defined as "all procedures and methods used in the interception of communications and the
15 obtaining of information from such communications by other than the intended recipients." 18
16 U.S.C. § 798. COMINT includes information derived from the interception of foreign and
17 international communications, such as voice, facsimile, and computer-to-computer information
18 conveyed via a number of means [REDACTED]

19 [REDACTED]. Electronic intelligence (ELINT) is technical intelligence information derived from
20 foreign non-communications electromagnetic radiations except atomic detonation or radioactive
21 sources-in essence, radar systems affiliated with military weapons platforms (e.g., anti-ship) and
22 civilian systems (e.g., shipboard and air traffic control radars). Foreign instrumentation signals

23
24
25
26
27
28 ⁵ (U) Section 1.7(c) of E.O. 12333, as amended, specifically authorizes the NSA to
"Collect (including through clandestine means), process, analyze, produce, and disseminate
signals intelligence information for foreign intelligence and counterintelligence purposes to
support national and departmental missions."

1 intelligence (FISINT) is derived from non-U.S. aerospace surfaces and subsurface systems which
2 may have either military or civilian applications.

3 14. (S//SI//NIP) The NSA's SIGINT responsibilities include establishing and
4 operating an effective unified organization to conduct SIGINT activities set forth in Executive
5 Order No. 12333, § 1.12(b), as amended. In performing its SIGINT mission, NSA has
6 developed a sophisticated worldwide SIGINT collection network that acquires, among other
7 things, foreign and international electronic communications and related information. The
8 technological infrastructure that supports the NSA's foreign intelligence information collection
9 network has taken years to develop at a cost of billions of dollars and untold human effort. It
10 relies on sophisticated collection and processing technology.

11 15. (U) There are two primary reasons for gathering and analyzing foreign
12 intelligence information. The first, and most important, is to gain information required to direct
13 U.S. 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 16. (S//SI//NIP) The NSA's ability to produce foreign intelligence information
20 depends on its access to foreign and international electronic communications. Foreign
21 intelligence produced by COMINT activities is an extremely important part of the overall foreign
22 intelligence information available to the United States and is often unobtainable by other means.
23 Public disclosure of either the capability to collect specific communications or the substance of
24 the information derived from such collection itself can easily alert targets to the vulnerability of

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

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

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

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

3 18. (U) 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). The United States also
7 immediately began plans for a military response directed at al Qaeda's training grounds and
8 havens in Afghanistan. On September 14, 2001, both Houses of Congress passed a Joint
9 Resolution authorizing the President of the United States "to use all necessary and appropriate
10 force against those nations, organizations, or persons he determines planned, authorized,
11 committed, or aided the terrorist attacks" of September 11. Authorization for Use of Military
12 Force, Pub. L. No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept. 18, 2001) ("Cong. Auth.").
13 Congress also expressly acknowledged that the attacks rendered it "necessary and appropriate"
14 for the United States to exercise its right "to protect United States citizens both at home and
15 abroad," and acknowledged in particular that "the President has authority under the Constitution
16 to take action to deter and prevent acts of international terrorism against the United States." *Id.*
17 pmb.
18

19 19. (U) Also after the 9/11 attacks, a Military Order was issued stating that the attacks
20 of September 11 "created a state of armed conflict," see Military Order by the President § 1(a),
21 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001), and that al Qaeda terrorists "possess both the
22 capability and the intention to undertake further terrorist attacks against the United States that, if
23 not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of
24 property, and may place at risk the continuity of the operations of the United States
25 Government," and concluding that "an extraordinary emergency exists for national defense
26
27
28

1 purposes." Military Order, § 1(c), (g), 66 Fed. Reg. at 57833-34. Indeed, shortly after the
2 attacks, on October 2, 2001, NATO took the unprecedented step of invoking Article 5 of the
3 North Atlantic Treaty, which provides that an "armed attack against one or more of [the parties]
4 shall be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63
5 Stat. 2241, 2244, 34 U.N.T.S. 243, 246.

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

19 21. (TS//SI//NF) The Classified *In Camera, Ex Parte* Declaration of Admiral Dennis
20 C. Blair, Director of National Intelligence, details the particular facets of the continuing al Qaeda
21 threat and, thus, the exigent need for the NSA intelligence activities described here. The NSA
22 activities are directed at that threat, [REDACTED]

23
24
25
26
27
28 Global telecommunications networks, especially the Internet, have [REDACTED]

TOP SECRET//ISP//SI [REDACTED]//ORCON/NOFORN

1 developed in recent years into a loosely interconnected system—a network of networks—that is
2 ideally suited for the secret communications needs of loosely affiliated terrorist cells. Hundreds
3 of Internet service providers, or “ISPs,” and other providers of communications services offer a
4 wide variety of global communications options, often free of charge. [REDACTED]

5 [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 22. (TS//SI//NF) [REDACTED]

9 [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 [REDACTED]

26 [REDACTED]

27 [REDACTED]

28 6 (TS//SI//OC/NF) [REDACTED]

1
2 23. (TS//SI//OC/NF) Our efforts against al Qaeda and its affiliates therefore present
3 critical challenges for the Nation's communications intelligence capabilities. First, in this new
4 kind of war, more than in any other we have ever faced, communications intelligence is essential
5 to our ability to identify the enemy and to detect and disrupt its plans for further attacks on the
6 United States. Communications intelligence often is the only means we have to learn the
7 identities of particular individuals who are involved in terrorist activities and the existence of
8 particular terrorist threats. Second, at the same time that communications intelligence is more
9 important than ever, the decentralized, non-hierarchical nature of the enemy and their
10 sophistication in exploiting the agility of modern telecommunications make successful
11 communications intelligence more difficult than ever. It is against this backdrop that the risks
12 presented by this litigation should be assessed, in particular the risks of disclosing particular
13 NSA sources and methods implicated by the claims.

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

15 24. (TS//SI//OC/NF) After the September 11 attacks, the NSA received presidential
16 authorization and direction to detect and prevent further terrorist attacks within the United States
17 by intercepting the content of telephone and Internet communications for which there were
18 reasonable grounds to believe that (1) such communications originated or terminated outside the
19 United States and (2) a party to such communication was a member or agent of al Qaeda or an
20 affiliated terrorist organization. The existence of this activity was disclosed by then-President
21 Bush in December 2005 (and subsequently referred to as the "Terrorist Surveillance Program" or
22 "TSP").⁷

23
24
25
26
27
28

⁷ (U) On January 17, 2007, the Attorney General made public the general facts that new orders of the Foreign Intelligence Surveillance Court had been issued that authorized the Government to target for collection international communications into or out of the United States

25. (TS//TSP//SI//OC/NF) In more specific and classified terms, the NSA has

utilized a number of critically important intelligence sources and methods to meet the threat of another mass casualty terrorist attack on the United States—methods that were designed to work in tandem and continue to this day under authority of the FISC. As noted above, one such method involved the program publicly acknowledged by then-President Bush as the TSP, in which the NSA intercepted the content of telephone and Internet communications pursuant to presidential authorization.⁸ As described further below, under the TSP, NSA did not engage in plaintiffs' alleged dragnet surveillance of communication content, but intercepted the content of particular communications where reasonable grounds existed to believe one party involved a member of agent or al Qaeda or affiliated terrorist organization based on particular "selectors" (phone numbers or Internet addresses) associated with that target. In addition to collecting the content of particular communications, the NSA has also collected *non-content* communication information known as "meta data." Specifically, after the 9/11 attacks, the NSA collected bulk meta data related to *telephony* communications for the purpose of conducting targeted analysis to

19 where there is probable cause to believe that one of the communicants is a member or agent of al
20 Qaeda or an associated terrorist organization; that, as a result of these orders, any electronic
21 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.

⁸ ~~FFS/TSP/SI/OC/NF~~ The first presidential authorization of the TSP was on October 4, 2001, and the TSP was reauthorized approximately every 30-60 days throughout the existence of the program. The documents authorizing the TSP also contained the authorizations for the meta data activities described herein. The authorizations, moreover, evolved over time, and during certain periods authorized other activities (this declaration is not intended to and does not fully describe the authorizations and the differences in those authorizations over time). [REDACTED]

26 *See In Camera, Ex Parte*
27 Classified Declaration of Lt. Gen. Keith B. Alexander at ¶ 62, MDL No. 06-1791-VRW (N.D.
Cal.) (relating to all actions against the MCI and Verizon Defendants) (submitted Apr. 20, 2007)

Telephony meta data is information derived from call detail

records that reflect non-content information such as, but not limited to, the date, time, and duration of telephone calls, as well as the phone numbers used to place and receive the calls.⁹ In addition, since the 9/11 attacks, the NSA has collected bulk meta data related to *Internet* communications. *Internet* meta data is header/router/addressing information, such as the "to," "from," "cc," and "bcc" lines, as opposed to the body or "re" lines, of a standard email.

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

9 - TS/ST

RESPONSE

¹⁰ ~~(TS//SI//OCAN)~~ As also described further (¶ 64-67 *infra*), the FISC has extended these orders with some modifications, and the Foreign Telephone and Email Order later expired in August 2007 and was supplanted by authority enacted by Congress first under the Protect

1 27. ~~(TS//SI//OC/NF)~~ Second, with respect to the collection of telephony meta data,
2 since May 2006 certain telecommunication providers have been required by an order of the FISC
3 to produce to the NSA on a daily basis all telephony meta data that they create ("FISC Telephone
4 Business Records Order"). The FISC Telephone Business Records Order has been reauthorized
5 approximately every 90 days since it was first issued. Although this collection is broad in scope,
6 the NSA was authorized by the FISC to query the archived telephony data with identified
7 telephone numbers for which there are facts giving rise to a reasonable, articulable suspicion that
8 the number is associated with [REDACTED] (hereafter referred to
9 as a "RAS" determination).¹¹ Historically, only a tiny fraction of telephony meta data records
10 collected by the NSA has actually been presented to a trained professional for analysis. As
11 discussed further below (*see ¶¶ 49-57 infra*), while the vast majority of records are thus never
12 viewed by a human at the NSA, it is still necessary to collect the meta data in bulk in order to
13 utilize sophisticated and vital analytical tools for tracking the contacts [REDACTED]
14 [REDACTED] for protecting the national security of the United States.
15
16

17
18
19
20 America Act and then the FISA Amendments Act of 2008 to authorize foreign intelligence
21 surveillance of targets located overseas without individual court orders.

22 ¹¹ ~~(TS//SI//OC/NF)~~ As set forth further below (*¶ 61-63 infra*), NSA's compliance with
23 this limitation in the FISC Order has been subject to further proceedings in the FISC that
24 commenced with a compliance report by the government on January 15, 2009, which indicated
25 that the NSA had also been querying incoming telephony meta data with selectors for
26 counterterrorism targets subject to NSA surveillance under Executive Order 12333, as to which
27 the NSA had not made a "RAS" determination. On March 2, 2009, the FISC renewed the Order
28 authorizing the bulk provision to NSA of business records containing telephony meta data from
telecommunications carriers [REDACTED] but subjected that activity to new limitations,
including that the NSA may query the meta data only after a motion is granted on a case-by-case
basis (unless otherwise necessary to protect against imminent threat to human life). The FISC
also required the Government to report to the FISC on its review of revisions to the meta data
collection and analysis process, and that report shall include affidavits describing the value of the
collection of telephony meta data authorized by the FISC Telephone Business Records Order.

1 28. (FIS//SI//OC/NP) Third, beginning in July 2004, the collection of Internet meta

2 data in bulk has been conducted pursuant to an order of the FISC authorizing the use of a pen
3 register and trap and trace device ("FISC Pen Register Order" or "PRTT Order"). See 18 U.S.C.
4 § 3127 (defining "pen register" and "trap and trace device"). Pursuant to the FISC Pen Register
5 Order, which has been reauthorized approximately every 90 days since it was first issued, the
6 NSA is authorized to collect, in bulk, meta data associated with electronic communications
7 [REDACTED]

8 [REDACTED] on the Internet.¹² [REDACTED]

9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]

13 Although the NSA collects email meta data in bulk [REDACTED]
14 [REDACTED] it has been authorized by the FISC to query the archived meta data only using email
15 addresses for which there are facts giving rise to a reasonable, articulable suspicion that the email
16 address is associated with [REDACTED] (similar restrictions were
17 in place under the presidential authorization). As with bulk telephony meta data collection, bulk
18 Internet meta data collection is necessary to allow the NSA to use critical and unique analytical
19 capabilities to track the contacts (even retrospectively) [REDACTED] of known
20 terrorists. Like telephony meta data activities, Internet meta data collection and analysis are vital
21

22
23
24
25

26 ¹² (FIS//SI//OC/NP) [REDACTED]
27 [REDACTED]
28 [REDACTED]

tools for protecting the United States from attack, and, accordingly, information pertaining to those activities is highly classified.¹³

3 V. (U) Information Protected by Privilege

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

- 7
- 8 A. Information that may tend to confirm or deny whether the
9 plaintiffs have been subject to any alleged NSA intelligence
activity that may be at issue in this matter; and
- 10
- 11 B. Any information concerning NSA intelligence activities,
12 sources, or methods that may relate to or be necessary to
13 adjudicate plaintiffs' allegations, including allegations that
14 the NSA, with the assistance of telecommunications
carriers such as AT&T, indiscriminately intercepts the
content of communications and also collects the
communication records of millions of Americans as part of
an alleged presidentially authorized "Program" after 9/11.
See, e.g., Complaint at ¶¶ 2-13; 39-97.

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

- 17
- 18 (i) Information concerning the scope and operation
19 of the now inoperative "Terrorist Surveillance Program"
20 ("TSP") regarding the interception of the content of certain
21 one-end international communications reasonably believed
22 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
- 23
- 24 (ii) Information concerning whether or not the NSA
25 obtained from telecommunications companies such as

26

27 ¹³ (TSP//TSP//SI//OC/NP) As the NSA has previously advised the Court in related
28 proceedings, and describes further below (see note 23 *infra*), the bulk collection of Internet meta
data pursuant to presidential authorization ceased in █████ 2004. See *In Camera, Ex Parte*
Classified Declaration of Lt. Gen. Keith B. Alexander at ¶ 31 n.8, MDL No. 06-1791-VRW
(N.D. Cal.) (relating to all actions against the MCI and Verizon Defendants) (submitted Apr. 20,
2007).

(iii) Information that may tend to confirm or deny whether AT&T (and to the extent relevant or necessary, any other telecommunications carrier), has provided assistance to the NSA in connection with any alleged activity.

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

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

30. (U) The first major category of information as to which I am supporting the DNI's assertion of privilege, and asserting the NSA's own statutory privilege, concerns information as to whether particular individuals, including the named plaintiffs in this lawsuit, have been subject to alleged NSA intelligence activities. As set forth below, disclosure of such information would cause exceptionally grave harm to the national security.

-FS/SH

31. (TS/TSP/SLW/OC/NF) The five named plaintiffs in this case—Tash Hepting, Gregory Hicks, Carolyn Jewel, Erik Knutzen and Joice Walton have alleged that, pursuant to a presidentially authorized program after the 9/11 attacks, the NSA, with the assistance of AT&T, has 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, as well as private telephone and Internet transaction records of millions of AT&T customers, again including information concerning the plaintiffs’ telephone and Internet communications. See, e.g., Complaint ¶¶ 7, 9, 10; see also ¶¶ 39-97. As set forth herein, the NSA does not engage in “dragnet” surveillance of the content of communications as plaintiffs allege.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

19 (TS//SI) [REDACTED]

20 32. (TS//TSP//SI//OC/NF) [REDACTED]

21

22

23

¹⁴ (TS//SI//OC/NF) [REDACTED]

24

25

26

27

28

¹⁵ (TS//TSP//SI//OC/NF) [REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12

13 33. (TS//TSP//SI//OC/NP)

14
15
16
17
18
19
20

34. (U) As a matter of course, the NSA cannot publicly confirm or deny whether any individual is subject to surveillance activities because to do so would tend to reveal actual targets. For example, if the NSA were to confirm in this case and others that specific individuals

21
22
23

16 (TS//TSP//SI//OC/NP)

24
25
26
27
28

17 (TS//SI//OC/NP) NSA has estimated that it collects Internet metadata associated with approximately [REDACTED]

[REDACTED]

With respect to telephony meta data, NSA has previously estimated that, prior to the 2006 FISC Order, about [REDACTED] telephony meta data records was presented to an analyst for review, see *Classified In Camera, Ex Parte Declaration of Lieutenant General Keith B. Alexander in Shubert, et al. v. Bush, et al.*, (Case No. 07-cv-693) (dated May 25, 2007) ¶ 27, and the scope of that disparity remains generally the same.

1 are not targets of surveillance, but later refuse to comment (as it would have to) in a case
2 involving an actual target, an actual or potential adversary of the United States could easily
3 deduce by comparing such responses that the person in the latter case is a target. There can be
4 great harm in revealing targets of foreign intelligence surveillance. If an individual knows or
5 suspects he is a target of U.S. intelligence activities, he would naturally tend to alter his behavior
6 to take new precautions against surveillance. In addition, revealing who is not a target would
7 indicate who has avoided surveillance and reveal the limitations of NSA's capabilities. Such
8 information could lead an actual or potential adversary, secure in the knowledge that he is not
9 under surveillance, to convey information; alternatively, such a person may be unwittingly
10 utilized or even forced to convey information through a secure channel to a hostile foreign
11 adversary. In short, revealing which channels are free from surveillance and which are not
12 would also reveal sensitive intelligence methods and thereby could help any adversary evade
13 detection and capitalize on limitations in NSA's capabilities.¹⁸

16 35. (TSP//SI [REDACTED] //OC/NP) [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]

18 (TSP//SI//OC/NP) [REDACTED]

1
2
3
4
5
6
7

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

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

11 36. (U) I am also supporting the DNI's assertion of privilege and asserting the NSA's
12 statutory privilege over any other facts concerning NSA intelligence activities, sources, or
13 methods that may relate to or be necessary to litigate the plaintiffs' claims and allegations,
14 including that (i) the NSA is indiscriminately intercepting the content of communications of
15 millions of ordinary Americans, *see, e.g.*, Complaint ¶¶ 7, 9, 10, and (ii) that the NSA is
16 collecting the private telephone and Internet transaction records of millions of AT&T customers,
17 again including information concerning the plaintiffs' telephone and Internet communications.
18 *See e.g.*, Complaint ¶¶ 7, 9, 10, 13, 82-97. As described above, the scope of the government's
19 privilege assertion includes but is not limited to: (1) facts concerning the operation of the now
20 inoperative Terrorist Surveillance Program and any other NSA activities needed to demonstrate
21 that the TSP was limited to the interception of the content of one-end international
22 communications reasonably believed to involve a member or agent of al Qaeda or an affiliated
23 terrorist organization and that the NSA does not otherwise conduct the content surveillance
24 dragnet that the plaintiffs allege; and (2) information concerning whether or not the NSA obtains
25 transactional communication records from telecommunications companies such as AT&T as
26
27
28

plaintiffs allege. As set forth below, the disclosure of such information would cause exceptionally grave harm to national security.

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

4 37. (U) After the existence of the TSP was officially acknowledged in December
5 2005, the Government stated that the NSA's collection of the content of communications under
6 the TSP was directed at international communications in which a participant was reasonably
7 believed to be associated with al Qaeda or an affiliated organization. Plaintiffs' allegation that
8 the NSA has undertaken indiscriminate surveillance of the content of millions of
9 communications sent or received by people inside the United States after 9/11 under the TSP is
10 therefore false, again as the Government has previously stated.¹⁹ But to the extent the NSA must
11 demonstrate that content surveillance under the TSP was so limited, and was not plaintiffs'
12 alleged content dragnet, or demonstrate that the NSA has not otherwise engaged in the alleged
13 content dragnet, highly classified NSA intelligence sources and methods about the operation of
14 the TSP and NSA intelligence activities would be subject to disclosure or the risk of disclosure.
15 The disclosure of whether and to what extent the NSA utilizes certain intelligence sources and
16 methods would reveal to foreign adversaries the NSA's capabilities, or lack thereof, enabling
17 them to either evade particular channels of communications that are being monitored, or exploit
18 channels of communications that are not subject to NSA activities---in either case risking
19 exceptionally grave harm to national security.

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

22 39. (~~TSP/TSP/SI//OCANP~~) First, interception of the content of communications
23 under the TSP was triggered by a range of information, including sensitive foreign intelligence,

19 See, e.g., Public Declaration of NSA Director Alexander in the *Shubert* action (07-cv-693-VRW) at ¶ 16.

TOP SECRET//TSP//SI [REDACTED]//ORCON//NOFORN

1 obtained or derived from various sources indicating that a particular phone number or email
2 address is reasonably believed by the U.S. Intelligence Community to be associated with a
3 member or agent of al Qaeda or an affiliated terrorist organization. Professional intelligence
4 officers at the NSA undertook a careful but expeditious analysis of that information, and
5 considered a number of possible factors, in determining whether it would be appropriate to target
6 a telephone number or email address under the TSP. Those factors included whether the target
7 phone number or email address was: (1) reasonably believed by the U.S. Intelligence
8 Community, based on other authorized collection activities or other law enforcement or
9 intelligence sources, to be used by a member or agent of al Qaeda or an affiliated terrorist
10 organization; [REDACTED]
11
12
13
14
15
16
17
18
19
20
21
22
23
24

25 _____
26 20 (TS//TSP//SI//OC/NF) [REDACTED]
27
28

TOP SECRET//TSP//SI- [REDACTED]//FOUO//NOFORN

1 40. (TS//TSP//SI//FOUO) Once the NSA determined that there were reasonable
2 grounds to believe that the target is a member or agent of al Qaeda or an affiliated terrorist
3 organization, the NSA took steps to focus the interception on the specific al Qaeda-related target
4 and on communications of that target that were to or from a foreign country. In this respect, the
5 NSA's collection efforts were [REDACTED] that the NSA had
6 reasonable grounds to believe carry the "one-end" foreign communications of members or agents
7 of al Qaeda or affiliated terrorist organizations.

9 41. (TS//TSP//SI//FOUO) [REDACTED]

10

11

12

13

14

15

16

17

18

42. (TS//TSP//SI- [REDACTED]//FOUO//NOFORN) [REDACTED]

19

20

21

22

23

24

25

26

27

28

1

2

3

4

5

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

10

11

12

13

[REDACTED] so that the only communications
intercepted were those to or from the targeted number of an individual who was reasonably
believed to be a member or agent of al Qaeda or an affiliated terrorist organization.

14

15

16

17

18

19

44. (TS//TSP//SI//OC/NP) For the interception of the content of Internet
communications under the TSP, the NSA used identifying information obtained through its
analysis of the target, such as email addresses [REDACTED] to target for collection the
communications of individuals reasonably believed to be members or agents of al Qaeda or an
affiliated terrorist organization. [REDACTED]

20

21

22

23

24

25

26

27

28

²¹ (TS//TSP//SI- [REDACTED]//OC/NP)

1 [REDACTED]

2 [REDACTED]

3 [REDACTED] The NSA did not search the content of the

4 communications [REDACTED] with "key words" other than the targeted selectors

5 themselves. Rather, the NSA targeted for collection only email addresses [REDACTED]

6 [REDACTED] associated with suspected members or agents of al Qaeda or affiliated terrorist

7 organizations, or communications in which such [REDACTED] were mentioned. In

8 addition, due to technical limitations of the hardware and software, incidental collection of non-

9 target communications has occurred, and in such circumstances the NSA applies its

10 minimization procedures to ensure that communications of non-targets are not disseminated. To

11 the extent such facts would be necessary to dispel plaintiffs' erroneous content dragnet

12 allegations, they could not be disclosed without revealing highly sensitive intelligence methods.

13 45. (TFS//TSP//SI//OCANF) In addition to procedures designed to ensure that the TSP

14 was limited to the international communications of al Qaeda members and affiliates, the NSA

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

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 [REDACTED]

26 [REDACTED]

27 [REDACTED]

28 [REDACTED]

1
2
3 46. (TS//TSP//SI) #OCNIP
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

The

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

22 (U//FOUO) In addition, in implementing the TSP, the NSA applied the existing Legal Compliance and Minimization Procedures applicable to U.S. persons to the extent not inconsistent with the presidential authorization. See United States Signals Intelligence Directive (USSID) 18. These procedures require that the NSA refrain from intentionally acquiring the communications of U.S. persons who are not the targets of its surveillance activities, that it destroy upon recognition any communications solely between or among persons in the U.S. that it inadvertently acquires, and that it refrain from identifying U.S. persons in its intelligence reports unless a senior NSA official determines that the recipient of the report requires such information in order to perform a lawful function assigned to it and the identity of the U.S. person is necessary to understand the foreign intelligence or to assess its significance.

47. (F/S//TSP//SI//OC/NF) In addition to these facts about the TSP, facts about other
1 NSA intelligence activities would be needed to address or prove that the NSA does not conduct
2 the alleged content dragnet. [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]

10 [REDACTED] In short, there is no other "dragnet" program authorized by the President after 9/11
11 under which the NSA intercepts the content of virtually all domestic and international
12 communications as the plaintiffs allege. Again, however, information about NSA content
13 surveillance activities beyond the TSP could not be disclosed in order to address and rebut
14 plaintiffs' allegation without revealing specific NSA sources and methods and thereby causing
15 exceptionally grave damage to national security.²³
16 [REDACTED]
17

18 **(b) (U) Plaintiffs' Allegations Concerning the Collection of Communication
Records.**

19 48. (U) As noted above, plaintiffs also allege that the NSA is collecting the private
20 telephone and Internet transaction records of millions of AT&T customers, again including
21 information concerning the plaintiffs' telephone and Internet communications. See, e.g.,
22 [REDACTED]

23 ²³ (F/S//TSP//SI//OC/NF) To the extent relevant to this case, additional facts about the
24 operational details of the TSP and subsequent FISA authorized content surveillance activities
25 also could not be disclosed without exceptional harm to national security, including for example
26 information that would demonstrate the operational swiftness and effectiveness of utilizing
content surveillance in conjunction with the meta data activities. As noted, [REDACTED]

27 [REDACTED] the TSP, in conjunction with meta data
28 collection and analysis described herein, allowed the NSA to obtain rapidly not only the content
of a particular communication, but connections between that target and others who may form a
web of al Qaeda conspirators.

1 Complaint ¶¶ 7, 9, 10, 13, 82-97. Confirmation or denial of any information concerning whether
2 the NSA collects communication records would also disclose information about whether or not
3 the NSA utilizes particular intelligence sources and methods and, thus, the NSA's capabilities or
4 lack thereof, and would cause exceptionally grave harm to national security.

5 49. ~~(TS//SI//OC/NF)~~ In addition to implicating the NSA's content collection
6 activities authorized after the 9/11 attacks, the plaintiffs' allegations also put directly at issue the
7 NSA's bulk collection of non-content communication meta data. As explained above, the NSA
8 has not engaged in the alleged dragnet of communication content, and, as now explained below,
9 to address plaintiffs' allegations concerning the bulk collection of non-content information
10 would require disclosure of NSA sources and methods that would cause exceptional harm to
11 national security. As also explained herein, these meta data collection activities are now subject
12 to the orders and supervision of the FISC.
13
14

15 50. ~~(TS//SI~~ ██████████ ~~4OC/NF)~~ As noted above, starting in October 2001, and since
16 2004 pursuant to the FISC Pen Register Order, the NSA collected bulk meta data associated with
17 electronic communications ██████████
18
19

20
21 See ¶¶ 25, 28, *supra*.²⁴ ██████████
22

23
24 ²⁴ ~~(TS//TSP//SI//OC/NF)~~ ██████████
25
26
27
28

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

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

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

1
2 [REDACTED] The only effective means by which NSA analysts are able continuously
3 to keep track of such operatives is through meta data collection and analysis.
4
5

6 **(TS//SI) Technical Details of Analytic Capabilities**
7

8 52. ~~(TS//SI//OC/NF)~~ In particular, the bulk collection of Internet and telephony meta
9 data allows the NSA to use critical and unique analytical capabilities to track the contacts [REDACTED]
10

11 through the use of two highly sophisticated tools known as "contact-chaining" [REDACTED]
12

13 Contact-chaining allows the NSA to identify telephone numbers and email addresses
14 that have been in contact with known [REDACTED] numbers and addresses; in turn, those
15 contacts can be targeted for immediate query and analysis as new [REDACTED] numbers
16 and addresses are identified. When the NSA performs a contact-chaining query on a terrorist-
17 associated telephone identifier, [REDACTED]
18
19
20
21
22
23
24

25 53. ~~(TS//SI//OC/NF)~~ [REDACTED]
26
27
28

1
2
3
4
5
6
7

8 54. -(TS//SI//OC/NF)-

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

25 55. -(TS//SI- [REDACTED] //OC/NF)- Because it is impossible to determine in advance
26 which particular piece of meta data will turn out to identify a terrorist, collecting meta data in
27 *bulk* is vital for the success of contact-chaining [REDACTED] NSA analysts know that the
28 terrorists' telephone calls are located somewhere in the billions of data bits; what they cannot

1 know ahead of time is exactly where. The ability to accumulate meta data substantially increases
2 NSA's ability to detect and identify these targets. One particular advantage of bulk meta data
3 collection is that it provides a historical perspective on past contact activity that cannot be
4 captured in the present or prospectively. Such historical links may be vital to identifying new
5 targets, because the meta data may contain links that are absolutely unique, pointing to potential
6 targets that otherwise would be missed. [REDACTED]

8 [REDACTED]
9
10
11 These sources and methods enable the NSA to segregate some of that very
12 small amount of otherwise undetectable but highly valuable information from the overwhelming
13 amount of other information that has no intelligence value whatsoever—in colloquial terms, to
14 find at least some of the needles hidden in the haystack. If employed on a sufficient volume of
15 data, contact chaining [REDACTED] can expose [REDACTED] and contacts
16 that were previously unknown. [REDACTED]

19 [REDACTED]
20
21
22 56. (TSP//SI//NF) The foregoing discussion is not hypothetical. As noted previously,
23 since inception of the first FISC Telephone Business Records Order, NSA has provided 275
24 reports to the FBI. These reports have provided a total of 2,549 telephone identifiers as being in
25 contact with identifiers associated with [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

1
2
3
4 57. (TS//SI//OC/NF) Accordingly, adjudication of plaintiffs' allegations concerning
5 the collection of non-content meta data and records about communication transactions would risk
6 or require disclosure of critical NSA sources and methods for [REDACTED] contacts of
7 terrorist communications as well as the existence of current NSA activities under FISC Orders.
8 Despite media speculation about these activities, official confirmation and disclosure of the
9 NSA's bulk collection and targeted analysis of telephony meta data would confirm to all of our
10 foreign adversaries [REDACTED] the existence of these critical intelligence
11 capabilities and thereby severely undermine NSA's ability to gather information concerning
12 terrorist connections and cause exceptional harm to national security.
13
14

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

17 58. (TS//TSP//SI//OC//NF) I am also supporting the DNI's state secrets privilege
18 assertion, and asserting NSA's statutory privilege, over information concerning the various
19 orders of the Foreign Intelligence Surveillance Court mentioned throughout this declaration that
20 authorize NSA intelligence collection activities, as well as NSA surveillance activities conducted
21 pursuant to the Protect America Act ("PAA") and current activities authorized by the FISA
22 Amendments Act of 2008. As noted herein, the three NSA intelligence activities initiated after
23 the September 11 attacks to detect and prevent a further al Qaeda attack—(i) content collection
24 of targeted al Qaeda and associated terrorist-related communications under what later was called
25 the TSP; (ii) internet meta data bulk collection; and (iii) telephony meta data bulk collection—
26 have been subject to various orders of the FISC (as well as FISA statutory authority) and are no
27
28

longer being conducted under presidential authorization. The bulk collection of non-content transactional data for internet communications was first authorized by the FISC in the July 2004 FISC Pen Register Order, and the bulk collection of non-content telephony meta data was first authorized by the FISC in May 2006. The existence and operational details of these orders, and of subsequent FISC orders reauthorizing these activities, remain highly classified and disclosure of this information would cause exceptional harm to national security.²⁵ In addition, while the Government has acknowledged the general existence of the January 10, 2007 FISC Orders authorizing electronic surveillance similar to that undertaken in the TSP, the content of those orders, and facts concerning the NSA sources and methods they authorize, cannot be disclosed without likewise causing exceptional harm to national security. Subsequent content surveillance sources and methods utilized by the NSA under the PAA and, currently, under the FISA Amendments Act of 2008 likewise cannot be disclosed. I summarize below the proceedings that have occurred under authority of the FISA or the FISC.

59. (TSP//SI//OC//NF) (a) *Internet Meta Data*: Pursuant to the FISC Pen Register Order, which has been reauthorized approximately every 90 days after it was first issued, NSA is authorized to collect in bulk [REDACTED] meta data associated with electronic communications [REDACTED]

25 (TSP//SI//OC//NF) For this reason, the FISC Telephone Business Records Order and FISC Pen Register Orders prohibit any person from disclosing to any other person that the NSA has sought or obtained the telephony meta data, other than to (a) those persons to whom disclosure is necessary to comply with the Order; (b) an attorney to obtain legal advice or assistance with respect to the production of meta data in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. The FISC Orders further provide that any person to whom disclosure is made pursuant to (a), (b), or (c) shall be subject to the nondisclosure requirements applicable to a person to whom the Order is directed in the same manner as such person.

1
2
3
4
5 [REDACTED] The NSA is authorized to query the archived
6 meta data collected pursuant to the FISC Pen Register Order using email addresses for which
7 there were facts giving rise to a reasonable, articulable suspicion that the email
8 address was associated with [REDACTED]. The FISC Pen Register
9 Order was most recently reauthorized on [REDACTED] 2009, and requires continued assistance by the
10 providers through [REDACTED] 2009.

11
12
13 60. (TS//~~SI//OC//NF~~) (b) Telephony Meta Data: Beginning in May 2006, the NSA's
14 bulk collection of telephony meta data, previously subject to presidential authorization, was
15 authorized by the FISC Telephone Business Records Order. Like the FISC Pen Register Order,
16 the FISC Telephone Business Records Order was reauthorized approximately every 90 days.
17 Based on the finding that reasonable grounds existed that the production was relevant to efforts
18 to protect against international terrorism, the Order required [REDACTED] to
19 produce to the NSA "call detail records" or "telephony metadata" pursuant to 50 U.S.C. §
20 1861(c) (authorizing the production of business records for, inter alia, an investigation to protect
21 against international terrorism). Telephony meta data was compiled from call detail data
22 maintained by the providers in the ordinary course of business that reflected non-content
23 information such as the date, time, and duration of telephone calls, as well as the phone numbers
24 used to place and receive the calls. The NSA was authorized by the FISC to query the archived
25 telephony meta data solely with identified telephone numbers for which there were facts giving
26

²⁶ (TS//~~SI//OC//NF~~) [REDACTED]

rise to a reasonable, articulable suspicion that the number was associated with [REDACTED]

[REDACTED] (or a "RAS" determination). The FISC Telephone Business Records Order was most recently reauthorized on March 2, 2009, but subject to new specific limitations, which I summarize next.

61. ~~(TS//SI//OC/NF)~~ As noted above (note 11 *supra*), on January 15, 2009, the Department of Justice ("DOJ") submitted a compliance incident report related to the Business Records Order to the FISC, based on information provided to DOJ by the NSA, which indicated that the NSA's prior reports to the FISC concerning implementation of the FISC Telephone Business Records Order had not accurately reported the extent to which NSA had been querying the telephony meta data acquired from carriers. In sum, this compliance incident related to a process whereby currently tasked telephony selectors (*i.e.* phone numbers) reasonably believed to be associated with authorized counter terrorism foreign intelligence targets associated with [REDACTED]

15 [REDACTED] under Executive Order 12333 were reviewed against
16 the incoming telephony metadata to determine if that number had been in contact with a number
17 in the United States. This process occurred prior to a formal determination by NSA that
18 reasonable articulable suspicion existed that the selector was associated with [REDACTED]

20 [REDACTED] and was not consistent with NSA's prior descriptions of the
21 process for querying telephony meta data.

22 62. ~~(TS//SI//OC/NF)~~ By Order dated March 2, 2009, the FISC has directed that the
23 NSA may continue to acquire call detail records of telephony meta data in accordance with the
24 FISC Telephone Business Record Orders, but is prohibited from accessing data acquired except
25 in a limited manner. In particular, the Government may request through a motion that the FISC
26 authorize querying of the telephony meta data for purposes of obtaining foreign intelligence on a
27 case-by-case basis (unless otherwise necessary to protect against imminent threat to human life,
28

1 subject to report to the FISC the next business day). In addition, the FISC imposed other
2 obligations on the Government, including to report on its ongoing review of the matter and to file
3 affidavits describing the continuing value of the telephony meta data collection to the national
4 security of the United States and to certify that the information sought is relevant to an
5 authorized investigation.

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

11 [REDACTED] would
12 compromise vital NSA sources and methods and result in exceptionally grave harm to national
13 security.

14 64. ~~(TS//TSP//SI//OC//NF~~) (c) Content Collection: On January 10, 2007, the FISC
15 issued orders authorizing the Government to conduct certain electronic surveillance that had
16 been occurring under the TSP. Those Orders included [REDACTED]

17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED] the "Foreign Telephone and Email Order," which
25 authorized, *inter alia*, electronic surveillance of telephone and Internet communications [REDACTED]
26 [REDACTED] where the Government determined that there was probable
27 cause to believe that (1) one of the communicants is a member or agent of [REDACTED]
28 [REDACTED] and (2) the communication is to or from a foreign country (*i.e.*,

1 a one-end foreign communication to or from the United States). Thereafter, any electronic
2 surveillance that was occurring as part of the TSP became subject to the approval of the FISA
3 Court and the TSP was not reauthorized.²⁷

4 65. (TS//SI//OC/NF) The Foreign Telephone and Email Order remained in effect
5 until the Protect America Act ("PAA") was enacted in August 2007. Under the PAA, the FISA's
6 definition of "electronic surveillance" was clarified to exclude "surveillance directed at a person
7 reasonably believed to be located outside the United States." 50 U.S.C. § 1805A. The PAA
8 authorized the DNI and the Attorney General to jointly "authorize the acquisition of
9 foreign intelligence information concerning persons reasonably believed to be outside the
10 United States" for up to one year, *id.* § 1805B(a), and to issue directives to communications
11 service providers requiring them to "immediately provide the Government with all information,
12 facilities, and assistance necessary to accomplish the acquisition" of necessary intelligence
13 information, *id.* § 1805B(e). Such directives were issued [REDACTED] and the NSA conducted
14 content surveillance of overseas targets under the PAA [REDACTED]

15 66. (TS//SI//OC/NF) Beginning in [REDACTED] 2008, expiring directives that had been
16 issued under the PAA for content surveillance of overseas targets (including surveillance of
17 specific [REDACTED] targets overseas) were replaced by new directives for such surveillance

22 27 (TS//SI//OC/NF) [REDACTED]
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939

1 security.

2 69. -~~(TS//TSP//SI [REDACTED]//OC/NF)~~ Because the NSA is not engaged in the
3 indiscriminate dragnet of the content of domestic and international communications as the
4 plaintiffs allege, [REDACTED]

5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED] can reasonably be
12 [REDACTED]

13 expected to cause exceptionally grave harm to national security.

14 70. -~~(TS//TSP//SI [REDACTED]//OC/NF)~~ [REDACTED]

15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

²⁸ ~~(TS//TSP//SI [REDACTED]//OC/NF)~~ On September 19, 2008, then-Attorney General Mukasey submitted a classified declaration and certification to this Court authorized by Section 802 of the Foreign Intelligence Surveillance Act Amendments Act of 2008, *see* 50 U.S.C. § 1885a,

1
2
3
4
5
6
7
8
9
10
11
12
13

14 71. TPS//SI-[REDACTED]//OC/NF-[REDACTED]

15
16
17
18
19
20
21

22
23
24
25
26
27
28

29 TPS//SI//OC/NF-[REDACTED]

1
2
3
4
5
6
7
8
9
10

72. (TS//SI-[REDACTED]//OC/NF)

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

³⁰ (TS//SI//OC/NF)

TOP SECRET//TSP//SI- [REDACTED]//ORCON/NOFORN

73. -(TS//SI- [REDACTED]//OC/NF) [REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

26. -(TS//TSP//SI- [REDACTED]//OC/NF) [REDACTED]

27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

19 75. (TSP//SI-[REDACTED] 400END)

20
21
22
23
24
25
26
27
28

TOP SECRET//~~TS//SI~~

~~NOFORN~~

1

2

3

4

5

6

7

76. (T~~S//SI~~) ~~NOFORN~~

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

³¹ (T~~S//SI~~) ~~NOFORN~~

1

2

3

4

5

6

7

77. (TSP//SI//NF)

8

9

10

11

12

13

14

15

16

17

18

78. (TSP//TSP//SI- [REDACTED] //OC/NF)

19

20

21

22

32 (TSP//TSP//SI- [REDACTED] //OC/NF)

23

24

25

26

27

28

1
2
3
4
5
6
7
8
9
10
11
12
13
14

15 (a) (TS//TSP//SI [REDACTED]//OC/NF) [REDACTED]

16
17
18
19
20
21
22
23

25 (b) (TS//TSP//SI [REDACTED]//OC/NF) [REDACTED]

26
27
28

1
2
3
4
5
6
7
8
9
10
11
12

13 79. (TS//TSP//SI [REDACTED] /OC/NF) [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]

18 33 (TS//TSP//SI [REDACTED] /OC/NF) [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]

23 34 (TS//TSP//SI [REDACTED] /OC/NF) [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

1

2

3

4

BS

5

6

VII. (U) Risks of Allowing Litigation to Proceed

7

80. -~~(TS//TSP//SI//OC/NF)~~ Upon examination of the allegations, claims, facts, and issues raised by this case, it is my judgment that sensitive state secrets are so central to the subject matter of the litigation that any attempt to proceed will substantially risk the disclosure of the privileged state secrets described above. Although plaintiffs' alleged content surveillance dragnet does not occur, proving why that is so, [REDACTED]

11

12

[REDACTED] would directly implicate highly classified intelligence information and activities. Similarly, attempting to address plaintiffs' allegations with respect to the bulk collection of non-content information and records containing transactional meta data about communications would also compromise currently operative NSA sources and methods that are essential to protecting national security, including for detecting and preventing a terrorist attack. [REDACTED]

20

21

22

In my judgment, any effort to probe the outer-bounds of such classified information would pose

23

24

25

26

27

28

³⁵ ~~(TS//TSP//SI//OC/NF)~~ In its prior classified declarations in this action, the NSA has set forth specific examples of how the intelligence sources and methods utilized by the NSA after the 9/11 attacks, including content surveillance under the TSP and pursuant to subsequent FISA authority, as well as non-content meta data collection and analysis, have led to the development by the NSA of actionable intelligence and important counter-terrorism efforts. See, e.g., Classified *In Camera*, *Ex Parte* Declaration of LTG Keith B. Alexander in *Shubert, et al. v. Bush, et al.*, (Case No. 07-cv-693) (dated May 25, 2007) at 35-43, ¶¶ 58-61. To the extent that such information would be relevant to any litigation in this action, however, they could not be disclosed without revealing specific NSA intelligence information, sources, and methods, and are subject to the government's privilege assertion.

1 inherent and significant risks of the disclosure of that information, including critically sensitive
2 information about NSA sources, methods, operations, targets [REDACTED]. Indeed, any
3 effort merely to allude to those facts in a non-classified fashion could be revealing of classified
4 details that should not be disclosed. Even seemingly minor or innocuous facts, in the context of
5 this case or other non-classified information, can tend to reveal, particularly to sophisticated
6 foreign adversaries, a much bigger picture of U.S. intelligence gathering sources and methods.
7

8 81. (TS//SI//NF) The United States has an overwhelming interest in detecting and
9 thwarting further mass casualty attacks by al Qaeda. The United States has already suffered one
10 attack that killed thousands, disrupted the Nation's financial center for days, and successfully
11 struck at the command and control center for the Nation's military. Al Qaeda continues to
12 possess the ability and clear, stated intent to carry out a massive attack in the United States that
13 could result in a significant loss of life, as well as have a devastating impact on the U.S.
14 economy. According to the most recent intelligence analysis, attacking the U.S. Homeland
15 remains one of al Qaeda's top operational priorities, see *Classified In Camera Ex Parte*
16 Declaration of Admiral Dennis C. Blair, Director of National Intelligence, and al Qaeda will
17 keep trying for high-impact attacks as long as its central command structure is functioning and
18 affiliated groups are capable of furthering its interests.
19

20 82. (TS//SI//NF) Al Qaeda seeks to use our own communications infrastructure
21 against us as they secretly attempt to infiltrate agents into the United States, waiting to attack at a
22 time of their choosing. One of the greatest challenges the United States confronts in the ongoing
23 effort to prevent another catastrophic terrorist attack against the Homeland is the critical need to
24 gather intelligence quickly and effectively. Time is of the essence in preventing terrorist attacks,
25 and the government faces significant obstacles in finding and tracking agents of al Qaeda as they
26 manipulate modern technology in an attempt to communicate while remaining undetected. The
27
28

1 NSA sources, methods, and activities described herein are vital tools in this effort.

2 **VIII. (U) Conclusion**

3 83. (U) In sum, I support the DNI's assertion of the state secrets privilege and
4 statutory privilege to prevent the disclosure of the information described herein and detailed
5 herein. I also assert a statutory privilege under Section 6 of the National Security Act with
6 respect to the information described herein which concerns the functions of the NSA. Moreover,
7 because proceedings in this case risk disclosure of privileged and classified intelligence-related
8 information, I respectfully request that the Court not only protect that information from
9 disclosure but also dismiss this case to prevent exceptional harm to the national security of the
10 United States.
11

12 I declare under penalty of perjury that the foregoing is true and correct.
13

14 DATE: 3 April 2009



15 DEBORAH A. BONANNI
16 Chief of Staff
17 National Security Agency