

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY)	MDL Dkt. No. 06-1791-VRW
TELECOMMUNICATIONS RECORDS)	
LITIGATION)	CLASSIFIED DECLARATION
)	OF LT. GEN. KEITH B.
)	ALEXANDER, DIRECTOR,
<u>This Document Relates to:</u>)	NATIONAL SECURITY
)	AGENCY
)	
<i>Shubert v. Bush</i> , Case No. 07-693)	SUBMITTED <i>IN CAMERA</i>,
)	<i>EX PARTE</i>
)	
)	Hon. Vaughn R. Walker

***IN CAMERA, EX PARTE* DECLARATION OF LIEUTANANT GENERAL KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY**

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

I. (U) Introduction

1. (U) I am the Director of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I am responsible for directing the NSA, overseeing the operations undertaken to carry out its mission and, by specific charge of the President and the Director of National Intelligence, protecting NSA activities and intelligence sources and methods. I have been designated an original TOP SECRET classification authority under Executive Order No. 12958, 60 Fed. Reg. 19825 (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

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: MR

1 privilege under the National Security Act. Specifically, in the course of my official duties, I
2 have been advised of this litigation and the allegations in the Plaintiffs' complaint. As described
3 herein, various classified facts related to the Plaintiffs' claims are subject to the DNI's state
4 secrets privilege assertion. The disclosure of this information, which relates to NSA intelligence
5 information, activities, sources, methods, and relationships, reasonably could be expected to
6 cause exceptionally grave damage to the national security of the United States. In addition, it is
7 my judgment that sensitive state secrets are so central to the subject matter of the litigation that
8 any attempt to proceed in the case risks the disclosure of the secrets described herein and
9 exceptionally grave damage to the national security of the United States. Through this
10 declaration, I also hereby invoke and assert the NSA's statutory privilege set forth in section 6 of
11 the National Security Agency Act of 1959, Public Law No. 86-36 (codified as a note to 50 USC.
12 § 402) ("NSA Act"), to protect the information related to NSA activities described below. The
13 statements made herein are based on my personal knowledge of NSA activities and operations,
14 and on information available to me as Director of the NSA.

15 **II. (U) Summary**

16 3. ~~(TS//SI//TSP//OC/NF)~~ Plaintiffs in this lawsuit allege that the NSA conducts a
17 "dragnet" surveillance program involving the interception of "virtually every telephone, internet
18 and/or email communication that has been sent from or received within the United States since
19 2001." Amended Compl. ¶¶ 1, 4. That allegation is false. As set forth below, there is no such
20 "dragnet" program, [REDACTED]

21 [REDACTED] Rather, as I have previously advised the Court, the NSA has conducted targeted
22 content surveillance aimed at al Qaeda and affiliated terrorist organizations pursuant to the
23 President's Terrorist Surveillance Program ("TSP") and recent orders of the Foreign Intelligence

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 Surveillance Court ("FISC" or "FISA Court"). As the Court is also aware, the NSA has
2 collected, pursuant to Presidential authorization and subsequent FISC orders, non-content
3 information (*i.e.*, meta data) about telephone and Internet communications in order to enable
4 highly sophisticated analytical tools that can uncover the contacts [REDACTED] of
5 members or agents of [REDACTED]. To demonstrate that these or
6 other NSA activities do not constitute the dragnet that Plaintiffs allege, however, would require
7 the disclosure of highly classified intelligence information, sources, and methods. Indeed,
8 although the existence of the TSP has been acknowledged, the details of that program—as well
9 as the details of the related content surveillance authorized by the FISC—remain highly
10 classified, and the meta data activities have never been acknowledged by the United States and
11 likewise remain highly classified.

12 4. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ In addition, Plaintiffs allege that Verizon and
13 AT&T have cooperated in the alleged dragnet program. *See* Amended Compl. ¶¶ 5-8. Neither
14 company assisted with the alleged dragnet program, because no such dragnet exists. [REDACTED]

15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 the disclosure of [REDACTED]
20 [REDACTED] would cause exceptionally grave damage to the national security.

21 5. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ Accordingly, the protection of the classified
22 information put at risk by this case, including the following, is vital to the national security of the
23 United States: (1) any information that would tend to confirm or deny whether particular

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 individuals such as the named Plaintiffs have been subject to any NSA intelligence activities;
2 (2) information about NSA intelligence activities, including facts demonstrating that the TSP
3 was limited to al Qaeda-related international communications and was not a content surveillance
4 dragnet as Plaintiffs allege; (3) facts that would tend to confirm or deny the existence of the
5 NSA's meta data activities, and any information about those activities; and (4) the fact that
6 [REDACTED] Any
7 disclosure or official confirmation of this information would cause exceptionally grave damage
8 to the national security.

9 6. (U) For these reasons, as set forth further below, the state secrets and statutory
10 privilege assertions that the DNI and I are making should be upheld and the information
11 described in this declaration should be protected from disclosure. I also believe that any further
12 litigation of this case poses exceptionally grave risks to the national security.

13 **(U) Table of Contents**

14 7. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ To facilitate the Court's review, this
15 declaration is organized as follows:

- 16 I. Introduction
- 17 II. Summary
- 18 III. Classification of Declaration
- 19 IV. Background Information
 - 20 A. The National Security Agency
 - 21 B. September 11, 2001 and the Continuing al Qaeda Threat
- 22 V. Information Protected by Privilege
- 23 VI. Description of Information Subject to Privilege and the Harm of Disclosure

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 A. Information That May Tend to Confirm or Deny Whether or Not the Plaintiffs
2 Have Been Subject to Any Alleged NSA Activities That May Be at Issue in This
3 Matter

- 3 1. [REDACTED]
4 2. [REDACTED]
5 3. Harm of Disclosure

6 B. Information Concerning NSA Activities, Sources, and Methods, and the Harm of
7 Disclosure

- 8 1. Information Concerning Plaintiffs' Allegations of a Content Surveillance
9 "Dragnet"
10 2. Additional Classified Information Concerning the TSP
11 3. Information Concerning Meta Data Activities
12 4. Information Demonstrating the Success of TSP and Meta Data Activities
13 5. Information Concerning the FISC Orders

14 C. Information That May Tend to Confirm or Deny Whether Verizon/MCI
15 and/or AT&T Has Assisted the NSA with the Alleged Intelligence
16 Activities, and the [REDACTED]

17 VII. Risks of Allowing Litigation to Proceed

18 VIII. Summary and Conclusion

19 **III. (U) Classification of Declaration**

20 8. ~~(S)~~ This declaration is classified TOP SECRET//COMINT- [REDACTED]

21 [REDACTED] ~~//TSP//ORCON/NOFORN//MR~~ pursuant to the standards in Executive Order No.

22 12958, as amended by Executive Order No. 13292. Under Executive Order No. 12958,

23 information is classified "TOP SECRET" if unauthorized disclosure of the information

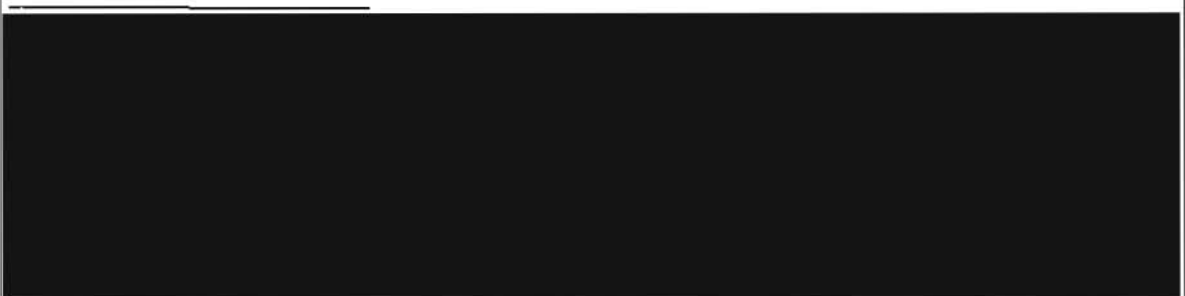
24 reasonably could be expected to cause exceptionally grave damage to the national security of the

United States; "SECRET" if unauthorized disclosure of the information reasonably could be

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 expected to cause serious damage to national security; and "CONFIDENTIAL" if unauthorized
2 disclosure of the information reasonably could be expected to cause identifiable damage to
3 national security. At the beginning of each paragraph of this declaration, the letter or letters in
4 parentheses designate(s) the degree of classification of the information the paragraph contains.
5 When used for this purpose, the letters "U," "C," "S," and "TS" indicate respectively that the
6 information is either UNCLASSIFIED, or is classified CONFIDENTIAL, SECRET, or TOP
7 SECRET.¹

8 9. ~~(S)~~ Additionally, this declaration also contains Sensitive Compartmented
9 Information (SCI), which is "information that not only is classified for national security reasons
10 as Top Secret, Secret, or Confidential, but also is subject to special access and handling
11 requirements because it involves or derives from particularly sensitive intelligence sources and
12 methods." 28 C.F.R. § 17.18(a). Because of the exceptional sensitivity and vulnerability of such
13 information, these safeguards and access requirements exceed the access standards that are
14 normally required for information of the same classification level. Specifically, this declaration
15 references communications intelligence (COMINT), also referred to as special intelligence (SI),
16 which is a subcategory of SCI. COMINT or SI identifies SCI that was derived from exploiting
17 cryptographic systems or other protected sources by applying methods or techniques, or from
18 intercepted foreign communications.



24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 10. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ This declaration also contains information
2 related to or derived from the Terrorist Surveillance Program (TSP), a controlled access signals
3 intelligence program authorized by the President in response to the attacks of September 11,
4 2001. Although the President publicly acknowledged the existence of the TSP in December
5 2005, details about the program remain highly classified and strictly compartmented.
6 Information pertaining to this program is denoted with the special marking "TSP" and requires
7 more restrictive handling. [REDACTED]

8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 11. ~~(S)~~ In addition to the fact that classified information contained herein may not be
15 revealed to any person without authorization pursuant to Executive Order 12958, as amended,
16 this declaration contains information that may not be released to foreign governments, foreign
17 nationals, or non-U.S. citizens without permission of the originator and in accordance with DNI
18 policy. This information is labeled "NOFORN." The "ORCON" designator means that the
19 originator of the information controls to whom it is released. Finally, this document is marked
20 Manual Review ("MR") indicating that it is not subject to automatic declassification at any
21 specific date.

22 [REDACTED]
23 [REDACTED]
24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

2 **A. (U) Background on The National Security Agency**

3 12. (U) The NSA was established by Presidential Directive in 1952 as a separately
4 organized agency within the Department of Defense. Under Executive Order 12333, § 1.12(b),
5 as amended, the NSA's cryptologic mission includes three functions: (1) to collect, process, and
6 disseminate signals intelligence (SIGINT) information, of which COMINT is a significant
7 subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c)
8 the support of military operations; (2) to conduct information security activities; and (3) to
9 conduct operations security training for the U.S. Government.

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

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

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

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

16 16. (S) The NSA's ability to produce foreign intelligence information depends on its
17 access to foreign and international electronic communications. Foreign intelligence produced by
18 COMINT activities is an extremely important part of the overall foreign intelligence information
19 available to the United States and is often unobtainable by other means. Public disclosure of
20 either the capability to collect specific communications or the substance of the information
21 derived from such collection itself can easily alert targets to the vulnerability of their
22 communications. Disclosure of even a single communication holds the potential of revealing
23 intelligence collection techniques that are applied against targets around the world. Once alerted,

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO 06-1791

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

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

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

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

15 19. (U) As the President made clear at the time, the attacks of September 11 "created
16 a state of armed conflict." Military Order, § 1(a), 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001).
17 Indeed, shortly after the attacks, NATO took the unprecedented step of invoking article 5 of the
18 North Atlantic Treaty, which provides that an "armed attack against one or more of [the parties]
19 shall be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63
20 Stat. 2241, 2244, 34 U.N.T.S. 243, 246. The President also determined that al Qaeda terrorists
21 "possess both the capability and the intention to undertake further terrorist attacks against the
22 United States that, if not detected and prevented, will cause mass deaths, mass injuries, and
23 massive destruction of property, and may place at risk the continuity of the operations of the

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 United States Government,” and he concluded that “an extraordinary emergency exists for
2 national defense purposes.” Military Order, § 1(c), (g), 66 Fed. Reg. at 57833-34.

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

15 21. ~~(TS//SI//NF)~~ The *In Camera* Declaration of Michael McConnell, Director of
16 National Intelligence, details the particular facets of the continuing al Qaeda threat and, thus, the
17 exigent need for the NSA intelligence activities described here. The NSA activities are directed
18 at that threat, [REDACTED]

19 [REDACTED]
20 [REDACTED]
21 Global telecommunications networks, especially the Internet, have developed in recent years into
22 a loosely interconnected system—a network of networks—that is ideally suited for the secret
23 communications needs of loosely affiliated terrorist cells. Hundreds of Internet service

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO 07-693; MDL NO. 06-1791

1 providers, or "ISPs," and other providers of communications services offer a wide variety of
2 global communications options, often free of charge. [REDACTED]

3 [REDACTED]
4 [REDACTED]

5 22. ~~(TS//SI//NF)~~ [REDACTED]

6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]

18 23. ~~(TS//SI)~~ Our efforts against al Qaeda and its affiliates therefore present critical
19 challenges for the Nation's communications intelligence capabilities. First, in this new kind of
20 war, more than in any other we have ever faced, communications intelligence is essential to our
21 ability to identify the enemy and to detect and disrupt its plans for further attacks on the United

22 [REDACTED]
23 ³ ~~(TS//SI//OC/NF)~~ [REDACTED]

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 States. Communications intelligence often is the only means we have to learn the identities of
2 particular individuals who are involved in terrorist activities and the existence of particular
3 terrorist threats. Second, at the same time that communications intelligence is more important
4 than ever, the decentralized, non-hierarchical nature of the enemy and their sophistication in
5 exploiting the agility of modern telecommunications make successful communications
6 intelligence more difficult than ever.

7 **C. (U) NSA Activities Critical to Meeting al Qaeda Threat.**

8 24. ~~(TS//SI~~ [REDACTED] ~~/TSP//OC/NF)~~ To meet these challenges and to help detect
9 and prevent another catastrophic terrorist attack within the United States, the NSA has utilized a
10 number of critically important intelligence tools. One such tool was the Terrorist Surveillance
11 Program, which the President authorized specifically to detect and prevent al Qaeda-related
12 terrorist attacks within the United States. Pursuant the TSP, the NSA was authorized to intercept
13 the content⁴ of telephone and Internet communications for which there were reasonable grounds
14 to believe that (1) such communication originated or terminated outside the United States, and
15 (2) a party to such communication was a member or agent of al Qaeda or an affiliated terrorist
16 organization.⁵

17 _____
18 ⁴ ~~(TS//SI~~ [REDACTED] ~~/TSP//OC/NF)~~ The term "content" is used herein to refer to the substance,
19 meaning, or purport of a communication, as defined in 18 U.S.C. § 2510(8), as opposed to the
20 type of addressing or routing information referred throughout this declaration as "meta data."

21 ⁵ ~~(TS//SI~~ [REDACTED] ~~/TSP//OC/NF)~~ The TSP was first authorized by the President on
22 October 4, 2001, and was reauthorized approximately every 30-60 days throughout the existence
23 of the program. The Presidential documents authorizing the TSP also contained the
24 authorizations for the meta data activities described herein. The Presidential authorizations,
moreover, evolved over time, and during certain periods authorized other activities (this
declaration is not intended to and does not fully describe the President's authorizations and the
differences in those authorizations over time). [REDACTED]

24 *See In Camera, Ex Parte* Classified Declaration of Lt. Gen. Keith B. Alexander at
CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 25. ~~(TS//SI//TSP//OC/NF)~~ On January 10, 2007, the FISA Court issued two orders
2 authorizing the Government to conduct certain electronic surveillance that had been occurring
3 under the TSP. As explained more fully below, *see* Section VI.B.5, *infra*, the orders consisted of
4 a [REDACTED]
5 [REDACTED] and a Foreign Telephone and Email Order, which authorized,
6 *inter alia*, electronic surveillance of telephone and Internet communications carried over
7 particularly listed facilities when the Government determines that there is probable cause to
8 believe that (1) one of the communicants is a member or agent of al Qaeda or an associated
9 terrorist organization, and (2) the communication is to or from a foreign country (*i.e.*, a one-end
10 foreign communication to or from the United States). The telephone numbers and email
11 addresses to be targeted under the Foreign Telephone and Email Order were further limited to
12 those that the NSA reasonably believes are being used by persons *outside* the United States.

13 26. ~~(TS//SI//TSP//OC/NF)~~ In light of these intervening FISA Court orders, any
14 electronic surveillance that was occurring as part of the TSP is now being conducted subject to
15 the approval of the FISA Court, and the President determined not to reauthorize the TSP. As
16 described further in Section VI.B.5, *infra*, and as the United States notified this Court on April 9,
17 2007, a Judge of the FISA Court recently [REDACTED]
18 declined to adopt the Government's interpretation of FISA underlying the application for the
19 Foreign Telephone and Email Order. The initial authorization to conduct surveillance under the
20
21

22 ¶ 62, MDL No. 06-1791-VRW (N.D. Cal.) (relating to all actions against the MCI and Verizon
23 Defendants) (submitted Apr. 20, 2007). [REDACTED]

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 Foreign Telephone and Email Order, however, has been extended through May 31, 2007.

2 Further proceedings before the FISA Court are ongoing, and the TSP has not been reauthorized.

3 27. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ In addition to the TSP, the NSA also collects
4 *non-content* communication information known as "meta data." Specifically, after the 9/11
5 attacks, the President authorized the NSA to collect bulk meta data related to *telephony*
6 communications for the purpose of conducting targeted analysis to [REDACTED]

7 [REDACTED] Telephony meta data is information derived from call detail records that reflect non-
8 content information such as the date, time, and duration of telephone calls, as well as the phone
9 numbers used to place and receive the calls. [REDACTED]

10 [REDACTED] since May 2006 certain telecommunication providers
11 have been *required* by an order of the FISA Court to produce to the NSA on a daily basis *all*
12 telephony meta data that they create ("FISC Telephone Records Order").⁶ Although this
13 collection is broad in scope,⁷ the NSA queries the data solely with identified telephone numbers
14 for which there are facts giving rise to a reasonable, articulable suspicion that the number is
15 associated with [REDACTED].⁸ Historically, only a tiny fraction

16 [REDACTED]
17 of telephony meta data records collected by the NSA has actually been presented to a trained

18 _____
19 ⁶ ~~(TS//SI//OC/NF)~~ The FISC Telephone Records Order has been reauthorized
approximately every 90 days since it was first issued.

20 ⁷ ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ [REDACTED]
21 [REDACTED]
22 [REDACTED]

23 ⁸ ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ Even before the FISC issued its Telephone Records
Order, the NSA operated under very similar requirements for accessing the meta data collected
pursuant to the President's authorization.

1 professional for analysis. While the vast majority of records are thus never viewed by a human
2 at the NSA, it is still necessary to collect the meta data in bulk in order to utilize sophisticated
3 analytical tools for tracking the contacts [REDACTED]
4 [REDACTED] Telephony meta data collection and analysis are highly valuable tools for tracking
5 terrorists and are therefore highly classified and strictly compartmented.

6 28. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ In addition, since the 9/11 attacks, the NSA
7 has collected bulk meta data related to *Internet* communications. Internet meta data is
8 header/router/addressing information, such as the "to," "from," "cc," and "bcc" lines, as opposed
9 to the body or "re" lines, of a standard email. The collection of Internet meta data in bulk was
10 conducted pursuant to Presidential authorization from October 2001 [REDACTED], and since
11 July 2004 it has been conducted pursuant to an Order of the Foreign Intelligence Surveillance
12 Court authorizing the use of a pen register and trap and trace device ("FISC Pen Register
13 Order"). See 18 U.S.C. § 3127 (defining "pen register" and "trap and trace device"). Pursuant to
14 the FISC Pen Register Order, which has been reauthorized approximately every 90 days since it
15 was first issued, the NSA is authorized to collect, in bulk, meta data associated with electronic
16 communications [REDACTED] on the Internet.⁹ [REDACTED]

17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED] Although the NSA collects email meta data in

21 ⁹ ~~(TS//SI//OC/NF)~~ [REDACTED]
22 [REDACTED]
23 [REDACTED]

1 bulk [REDACTED], it is only authorized to query the archived meta data using email
2 addresses for which there are facts giving rise to a reasonable, articulable suspicion that the email
3 address is associated with [REDACTED] (similar restrictions were
4 in place under the Presidential authorization). As with bulk telephony meta data collection, and
5 as the FISA Court specifically recognized in finding the bulk Internet meta data collection
6 consistent with the First and Fourth Amendments, the collection of the data in bulk is necessary
7 to allow the NSA to use critical and unique analytical capabilities to track the contacts (even
8 retrospectively) [REDACTED] of known terrorists. Like telephony meta data
9 activities, Internet meta data collection and analysis are highly valuable tools for protecting the
10 United States from attack, and, accordingly, information pertaining to those activities is highly
11 classified and strictly compartmented.

12 29. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ [REDACTED]



24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

30. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

[REDACTED]

On July 14, 2004, the FISC issued the Pen Register Order, restoring the bulk collection of Internet meta data as described above.

V. (U) Information Protected by Privilege

31. (U) As set forth further below, the following categories of information are subject to the DNI's assertion of the state secrets privilege and statutory privilege under the National Security Act, as well as my assertion of the NSA privilege:

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

¹¹ ~~(TS//SI//TSP//OC/NF)~~ As noted, the President reauthorized the TSP, as well as the Internet and telephony meta data activities, approximately every 30-60 days, and each time he did so in a single document covering all three activities (and, at times, other activities). See n.5, *supra*.

¹² ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 A. (U) Information that may tend to confirm or deny whether
2 the Plaintiffs have been subject to any alleged NSA
intelligence activity that may be at issue in this matter; and

3 B. (U) Information concerning NSA intelligence activities,
4 sources, or methods, including:

5 (1) (U) Information concerning the scope and operation of
6 the Terrorist Surveillance Program, including information
7 that may be needed to demonstrate that the TSP was limited
8 to one-end foreign al Qaeda-related communications and
9 that the NSA does not otherwise engage in the content
10 surveillance dragnet that the Plaintiffs allege; and

11 (2) (U) Any other information concerning NSA intelligence
12 activities, sources, or methods that would be necessary to
13 adjudicate the Plaintiffs' claims, including, to the extent
14 applicable, information that would tend to confirm or deny
whether the NSA collects large quantities of
communication records information; and

15 C. (U) Information that may tend to confirm or deny whether
16 Verizon/MCI, AT&T, or any other telecommunications
17 carrier has assisted the NSA with the alleged intelligence
18 activities.

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

20 **A. (U) Information That May Tend to Confirm or Deny Whether the Plaintiffs Have
21 Been Subject to Any Alleged NSA Activities That May Be at Issue in This Matter**

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

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

1. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

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

[REDACTED]

¹³ ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

[REDACTED]

2. ~~(TS//SI//OC/NF)~~ [REDACTED]

34. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~ [REDACTED]

[REDACTED]

3. (U) Harm of Disclosure

35. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

[REDACTED]

First, as a matter of course, the NSA cannot publicly confirm or deny whether any individual is subject to the surveillance activities described herein, because to do so would tend to reveal actual targets. For example, if the NSA were to confirm in this case and others that specific individuals are not targets of surveillance, but later refuse to

¹⁴ ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~ [REDACTED]

[REDACTED]

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 comment (as it would have to) in a case involving an actual target, a person could easily deduce
2 by comparing such responses that the person in the latter case is a target. The harm of revealing
3 targets of foreign intelligence surveillance should be obvious. If an individual knows or suspects
4 he is a target of U.S. intelligence activities, he would naturally tend to alter his behavior to take
5 new precautions against surveillance. [REDACTED]

6 [REDACTED]
7 [REDACTED]
8 [REDACTED] In addition, revealing
9 who is not a target would indicate who has avoided surveillance and who may be a secure
10 channel for communication. Such information could lead a person, secure in the knowledge that
11 he is not under surveillance, to help a hostile foreign adversary convey information;
12 alternatively, such a person may be unwittingly utilized or even forced to convey information
13 through a secure channel. Revealing which channels are free from surveillance and which are
14 not would also reveal sensitive intelligence methods and thereby could help any adversary evade
15 detection.

16 36. ~~(TS//SI-[REDACTED]//OC/NF)~~ [REDACTED]

17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 CLASSIFIED DECLARATION OF LT GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]

5 37. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~ Disclosing any of this information would reveal
6 some of the Nation's most sensitive and important intelligence-gathering methods. For reasons
7 already discussed, such disclosures would cause exceptionally grave damage to the national
8 security by allowing al Qaeda and its affiliates to evade detection, as well as by alerting other
9 foreign adversaries to these critical intelligence-gathering methods. Disclosing whether the NSA
10 currently receives telephony or Internet meta data [REDACTED] would also
11 violate specific provisions of the FISC Telephone Records and FISC Pen Register Orders.

12 **B. (U) Information Concerning NSA Activities, Sources, or Methods, and the Harm of**
13 **Disclosure.**

14 38. (U) The second category of information over which I am supporting the DNI's
15 assertion of privilege and asserting the NSA's statutory privilege is information concerning NSA
16 intelligence activities, sources, and methods that may at issue in this case, including (1) facts
17 concerning the operation of the Terrorist Surveillance Program and any other NSA intelligence
18 activities needed to demonstrate that the TSP was limited as the President stated to the
19 interception of one-end foreign communications reasonably believed to involve a member or
20 agent of al Qaeda or an affiliated terrorist organization, *see* ¶ 24 & n.5, *supra*, and that the NSA
21 does not otherwise conduct a dragnet of content surveillance as the Plaintiffs allege; (2) other
22 classified facts about the operation of the TSP that would be necessary to adjudicate the
23 lawfulness of that program; and (3) facts that would confirm or deny whether the NSA collects

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 large quantities of communication records information. As set forth below, the disclosure of
2 such information would cause exceptionally grave harm to national security.

3 1. **(U) Information Concerning Plaintiffs' Allegations of a Content Surveillance**
4 **"Dragnet."**

5 39. **(U)** In December 2005, President Bush explained that, after the September 11
6 attacks, he authorized the NSA to intercept the content of certain communications for which
7 there are reasonable grounds to believe that (1) such communication originated or terminated
8 outside the United States, and (2) a party to such communication is a member or agent of al
9 Qaeda or an affiliated terrorist organization. The President stated at the time that this activity,
10 now referred to as the Terrorist Surveillance Program, did not involve the collection of purely
11 domestic communications, or international communications with no al Qaeda connection, and
12 these facts were reiterated publicly by the Attorney General and then-Deputy Director of
13 National Intelligence. Nonetheless, I am advised that the Plaintiffs have alleged that, pursuant to
14 a secret NSA program, "virtually every telephone, internet and/or email communication that has
15 been sent from or received within the United States since 2001 has been (and continues to be)
16 searched, seized, intercepted, and subjected to surveillance without a warrant, court order or any
17 other lawful authorization." Amended Compl. ¶ 1. As the President made clear in describing the
18 limited scope of the TSP, such allegations of a content surveillance dragnet are false. But if the
19 NSA had to demonstrate in this case that the TSP was limited as the President stated, and not a
20 dragnet as the Plaintiffs claim, and that the NSA does not otherwise engage in the dragnet that
21 Plaintiffs allege, sensitive and classified facts about the operation of the TSP and NSA
22 intelligence activities would have to be disclosed.

23 40. ~~(TS//SI//TSP//OC/NF)~~ The privileged information that must be protected from
24 disclosure includes the following classified details demonstrating the limited nature of the TSP.
CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 First, interception of the content of communications under the TSP was triggered by a range of
2 information, including sensitive foreign intelligence, obtained or derived from various sources
3 indicating that a particular phone number or email address is reasonably believed by the U.S.
4 Intelligence Community to be associated with a member or agent of al Qaeda or an affiliated
5 terrorist organization. Professional intelligence officers at the NSA undertook a careful but
6 expeditious analysis of that information, and considered a number of possible factors, in
7 determining whether it would be appropriate to target a telephone number or email address under
8 the TSP. Those factors included whether the target phone number or email address was:
9 (1) reasonably believed by the U.S. Intelligence Community, based on other authorized
10 collection activities or other law enforcement or intelligence sources, to be used by a member or
11 agent of al Qaeda or an affiliated terrorist organization;

[REDACTED]

12
13
14
15
16
17
18
19
20 ¹⁵ ~~(TS//SI//TSP//OC/NF)~~

[REDACTED]

21
22
23
24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

[REDACTED]

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

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

43. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~
[REDACTED]

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

[REDACTED]

44. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ The NSA took specific steps in the actual TSP interception process to minimize the risk that the communications of non-targets were intercepted. With respect to telephone communications, specific telephone numbers identified through the analysis outlined above were [REDACTED] so that the only communications intercepted were those to or from the targeted number of an individual who was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization. For Internet communications, 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.¹⁶

¹⁶ ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ [REDACTED]

At no point did the NSA search the content of the communications [REDACTED] with "key words" other than the targeted selectors themselves. Rather, the NSA targeted for collection only email addresses [REDACTED] associated with suspected members or agents of al Qaeda or affiliated terrorist organizations, or communications in which such [REDACTED] were mentioned. In addition, due to technical limitations of the hardware and software currently used, incidental collection of non-target communications has occurred, and in such circumstances the NSA applies its minimization procedures to ensure that communications of non-targets are not disseminated. To the extent such facts would be necessary to dispel Plaintiffs' erroneous dragnet allegations, they could not be disclosed without revealing highly sensitive intelligence methods.

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 45. ~~(TS//SI//TSP//OC/NF)~~ In addition to procedures designed to ensure that the TSP
2 was limited to the international communications of al Qaeda members and affiliates, the NSA
3 also took additional steps to ensure that the privacy rights of U.S. persons were protected. [REDACTED]

4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]

13 46. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]

19 ¹⁷ ~~(U//FOUO)~~ In addition, in implementing the TSP, the NSA applied the existing Legal
20 Compliance and Minimization Procedures applicable to U.S. persons to the extent not
21 inconsistent with the President's authorization. *See* United States Signals Intelligence Directive
22 (USSID) 18. These procedures require that the NSA refrain from intentionally acquiring the
23 communications of U.S. persons who are not the targets of its surveillance activities, that it
24 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.

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

[REDACTED]

47. ~~(TS//SI//TSP//OC/NF)~~ In addition to these facts about the TSP, facts about other NSA intelligence activities would be needed to explain or prove that the NSA does not conduct a dragnet as Plaintiffs allege.

[REDACTED]

None of these activities, however, could be disclosed to address and rebut Plaintiffs' dragnet allegations without causing exceptionally grave damage to the national security.

2. (U) Additional Classified Information Concerning the TSP

48. (U) To the extent the Plaintiffs in this case are challenging the lawfulness of the TSP itself, facts about the operation of that program (which remain highly classified) also could not be disclosed.

CLASSIFIED DECLARATION OF LT GEN KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 49. ~~(TS//SI//TSP//OC/NF)~~ For example, in conjunction with meta data analysis, the
2 TSP provided far greater operational swiftness and effectiveness for identifying the al Qaeda
3 terrorist network in the United States than the traditional procedures that had been used under the
4 Foreign Intelligence Surveillance Act. In order to ascertain as rapidly as possible the potential al
5 Qaeda terrorist threats facing the United States, the NSA must know not only what a foreign
6 terrorist target says in a particular telephone or Internet intercept, but with whom that person has
7 been communicating. To the extent individual court orders for all TSP targets could have been
8 required in advance under traditional FISA procedures, the NSA would have been unable to
9 target communications sent to and from new phone numbers or Internet accounts as quickly, and
10 valuable intelligence could have been lost.

11 50. ~~(TS//SI//TSP//OC/NF)~~ As noted, [REDACTED]
12 [REDACTED]
13 [REDACTED] the TSP, in conjunction with meta data collection and analysis,
14 allowed the NSA to obtain rapidly not only the content of a particular communication, but
15 connections between that target and others who may form a web of al Qaeda conspirators. In
16 some cases, the NSA was able to begin collection on a target phone number in [REDACTED]
17 [REDACTED] to begin collection on a targeted phone number or
18 email address. In contrast, if individual applications have to be prepared and approved through
19 the traditional FISA process before the NSA can target a newly identified phone number or email
20 account associated with al Qaeda, vital information could be lost in the interim. The traditional
21 FISA process is a highly effective tool for many types of surveillance activities, [REDACTED]

22 [REDACTED]
23 [REDACTED]

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 [REDACTED]
2 [REDACTED]

3 [REDACTED] it would have had
4 to stop and demonstrate, through a multi-layered process involving NSA and DOJ counsel, the
5 Attorney General, and the FISA Court, that each of numerous, rapidly changing target numbers
6 or emails requires coverage. Where the gravest of dangers are at stake—a catastrophic mass
7 casualty terrorist attack against the U.S. Homeland and the corresponding need to track
8 thousands of potential terrorists—and where [REDACTED]
9 [REDACTED] to hide their communications and tracks, it is vital that the NSA be able to track multiple
10 communications, contacts, and [REDACTED] as rapidly as possible to fulfill its mission to protect the
11 national security of the United States.

12 51. (TS//SI//TSP//OC/NF) None of the foregoing information about the Terrorist
13 Surveillance Program could be disclosed in this case, however, without causing exceptionally
14 grave harm to the national security. Even though the President has determined not to reauthorize
15 the TSP, revealing how the program operated would provide key insights to foreign adversaries
16 as to how the NSA monitors communications. Information about the specific foreign
17 intelligence factors that triggered interception under the TSP would obviously reveal to foreign
18 adversaries the very facts that would most likely lead to their communications being intercepted,
19 even under the current FISA Court Orders, thereby giving adversaries a roadmap as to how to
20 avoid such interception. [REDACTED]

21 [REDACTED]

22 _____
23 ¹⁸ (TS//SI//TSP//OC/NF) [REDACTED]

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 [REDACTED]
2 [REDACTED]

3 52. ~~(TS//SI//TSP//OC/NF)~~ Likewise, information about the speed and agility with
4 which the NSA can collect content on a target, and how long it might maintain surveillance,
5 would provide invaluable insights for an adversary to devise new and different ways to protect
6 their communications. In particular, disclosure of the NSA's ability to utilize the TSP (or,
7 therefore, the current FISA Court-authorized content collection) in conjunction with contact
8 chaining [REDACTED] would severely undermine efforts to detect terrorist activities.

9 Armed with this knowledge, an adversary could make more robust use [REDACTED]

10 [REDACTED] Also, as noted, [REDACTED]
11 [REDACTED]
12 [REDACTED] Compromise of one NSA
13 method of surveillance, even no longer in use, can easily lead to evasive actions as to other
14 current methods that would deprive U.S. decision-makers of critical information needed to detect
15 [REDACTED] terrorist threats.

16 3. ~~(S)~~ Information Concerning Meta Data Activities

17 53. ~~(TS//SI//TSP//OC/NF)~~ To the extent that the NSA's bulk collection and
18 targeted analysis of communication meta data may be at issue in this case, those activities—as
19 described in paragraphs 27 and 28, above—must also be protected from disclosure.

20 54. ~~(TS//SI//TSP//OC/NF)~~ As noted above, starting in October 2001, and now
21 pursuant to the FISC Pen Register Order, the NSA collected bulk meta data associated with
22 electronic communications [REDACTED]

23 [REDACTED]

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

See ¶ 28, supra.

[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 ¶ 27, supra.* Disclosure of the NSA's meta data collection activities, either before or after FISC authorization, would cause exceptionally grave harm to national security.

55. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~ In particular, the bulk collection of Internet and telephony meta data allows the NSA to use critical and unique analytical capabilities to track the contacts [REDACTED] of members or agents of [REDACTED] [REDACTED] through the use of two highly sophisticated tools known as "contact chaining" and [REDACTED]. Contact-chaining allows the NSA to identify telephone numbers and email addresses that have been in contact with known [REDACTED] numbers and addresses; in turn, those contacts can be targeted for immediate query and analysis as new [REDACTED] numbers and addresses are identified. Obtaining the meta data in bulk, moreover, allows the NSA not only to track the contacts made by a particular telephone number or email address from a certain point in time going forward, but also to trace historically the contacts made with that number or address. This tool has been highly useful in detecting previously unknown terrorist operatives or agents for further surveillance.

56. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~ [REDACTED]

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

[REDACTED]

57. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~

[REDACTED]

58. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ The capability provided by meta data

analysis may be illustrated by an example of when this tool was not utilized. According to the

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 9/11 Commission report, when Khalid al-Mihdhar, one of the 9/11 hijackers, was in the United
2 States from January 2000 to June 2001, he telephoned the home of his wife's family in Yemen.
3 The phone number for this home in Yemen had well-established terrorist connections¹⁹ and was
4 being targeted by the NSA through an overseas collection process that did not have the capability
5 to obtain meta data to help identify the location of incoming calls. At the time, there was no
6 FISA collection on this number, and neither the TSP program, under which the NSA targeted
7 one-end foreign calls into the United States, nor the collection of bulk meta data, which would
8 have allowed analysis of this number to ascertain other contact numbers, were in place. Had the
9 Yemeni phone number been targeted using the TSP and were meta data analysis available, we
10 should have been able to identify that al-Mihdhar was in the United States when he called the
11 number in Yemen, which would have provided leads to investigate the matter further. Indeed,
12 the 9/11 Commission report noted that if the FBI had known that al Mihdhar was in the United
13 States, "investigations or interrogation of [al Mihdhar], and investigation of [his] travel and
14 financial activities could have yielded evidence of connections to other participants in the 9/11
15 plot. The simple fact of [his] detention could have derailed the plan. In any case, the
16 opportunity did not arise." Final Report of the National Commission on Terrorist Attacks Upon
17 the United States ("9/11 Commission Report") at 272. While there is an element of hindsight to
18 this example, and perhaps other actions could have detected al Mihdhar, the existence of the TSP
19 and meta data activities would have provided a highly significant tool that may have proved
20 valuable in detecting the 9/11 plot.

21
22 ¹⁹ ~~(TS//SI//NF)~~ In August 1998, the number was found in the pocket of one of the
23 would-be Kenyan Embassy bombers, who had fled the bomb-laden vehicle at the last minute.

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

59. ~~(TS//SI [REDACTED] //TSP//OC/NF)~~ Based on my experience as Director of the NSA, I believe that the meta data collection activities authorized by the President after 9/11 and subsequently authorized by the FISC are among the most important intelligence tools available to the United States for protecting the Homeland from another catastrophic terrorist attack. In my view, the NSA could not have obtained certain critical intelligence in any other way. These NSA activities have given the United States unparalleled ability to understand [REDACTED]. If employed on a sufficient volume of raw data, contact chaining [REDACTED] can expose [REDACTED] and contacts that were previously unknown. Meta data collection thus enables the NSA to segregate some of that very small amount of otherwise undetectable but highly valuable information from the overwhelming amount of other information that has no intelligence value whatsoever—in colloquial terms, to find at least some of the needles hidden in the haystack. [REDACTED]

[REDACTED]

[REDACTED] Disclosure or confirmation of the NSA's bulk collection and targeted analysis

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 of telephony meta data would confirm to all of our foreign adversaries [REDACTED]
2 [REDACTED] the existence of these critical intelligence capabilities and thereby severely undermine
3 NSA's ability to gather information concerning terrorist connections.

4 **4. ~~(TS//SI//TSP//OC/NF)~~ Information Demonstrating the Success of the
TSP and Meta Data Activities.**

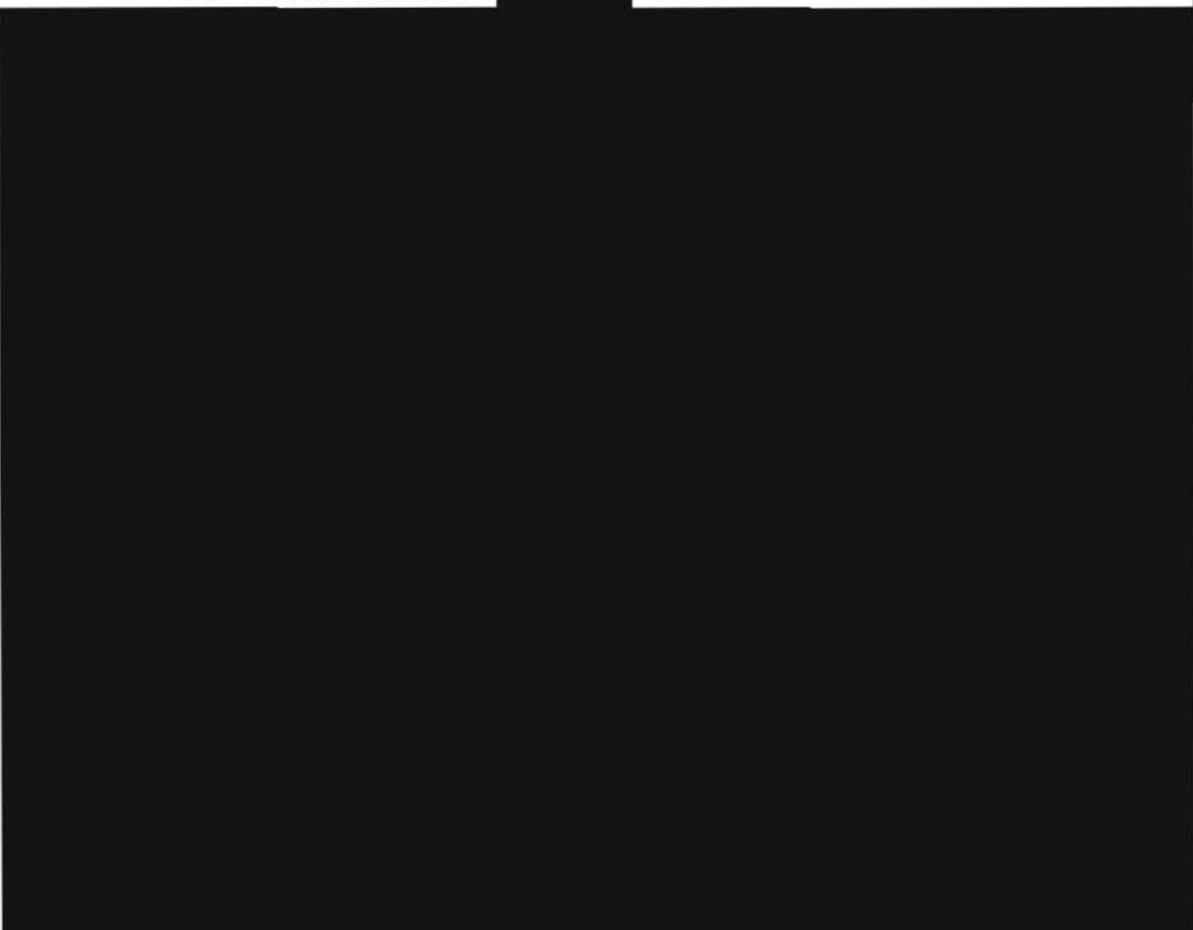
5 60. ~~(TS//SI//TSP//OC/NF)~~ Specific examples of how the TSP, in conjunction with
6 meta data analysis, led to the development by the NSA of actionable intelligence and important
7 counter-terrorism efforts help illustrate the effectiveness and need for the activities. To the
8 extent that such examples would be relevant to any defense of this action, however, those
9 examples could not be disclosed without revealing specific NSA intelligence information,
10 sources, and methods. For instance:

11 **A. ~~(TS//SI//OC/NF)~~** [REDACTED]

12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 As a result of contact chaining undertaken pursuant
20 to meta data analysis, the NSA was able to discover contacts between [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

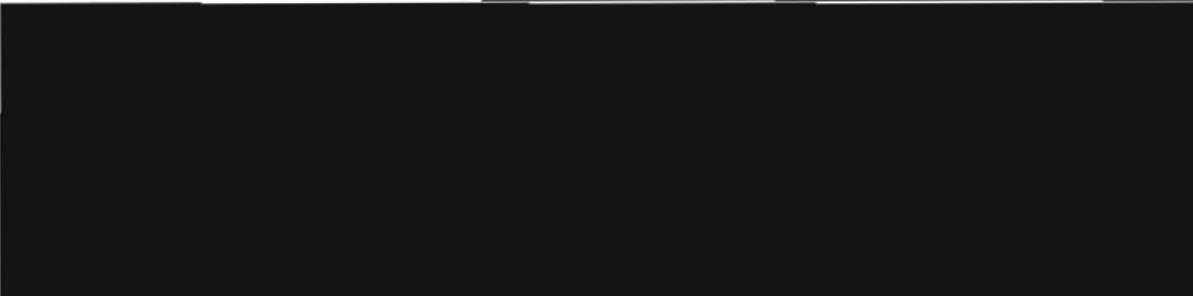
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



B. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

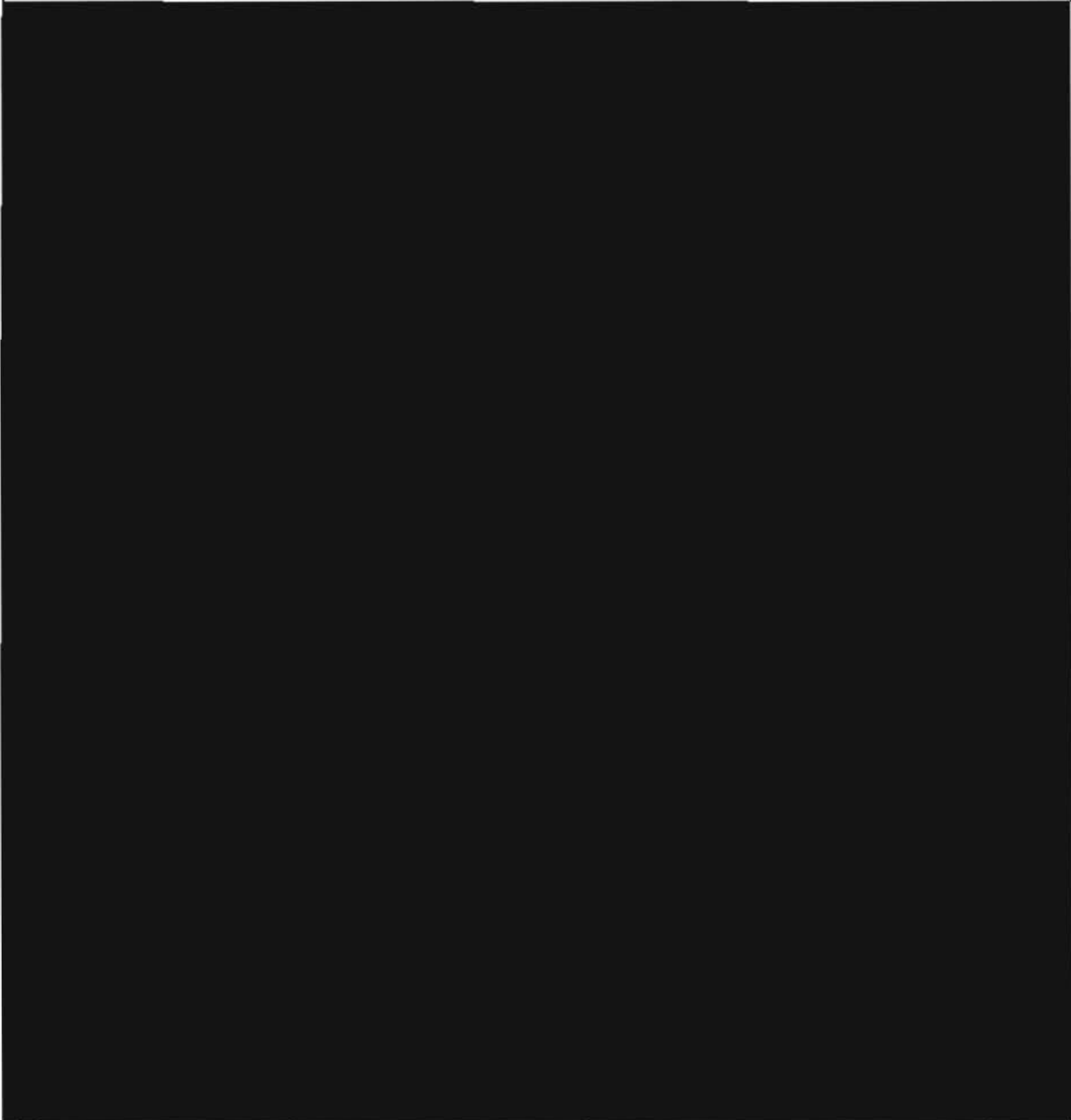


C. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]



CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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



D. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]



DESCRIPTION OF BY GEN. RICHARD ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

[REDACTED]

E. ~~(TS//SI//TSP//OC/NF)~~

[REDACTED]

F. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

[REDACTED]

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

G. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

H. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

I. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

J. ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

CLASSIFIED DECLARATION OF LT GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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



61. ~~(TS//SI//TSP//OC/NF)~~ Information about any of the successes of NSA activities would not only be revealing of the substantive knowledge of the United States Government as to terrorist plans and activities, but would also tend to reveal or confirm to all of our foreign adversaries the sources and methods by which the United States obtained such information.

5. ~~(E)~~ Information Concerning FISC Orders.

62. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ Next, to the extent relevant to the litigation of this case, information concerning the various orders of the Foreign Intelligence Surveillance Court mentioned throughout this declaration must also remain protected from public disclosure. As discussed above, three NSA intelligence activities authorized by the President after the September 11 attacks to detect and prevent a further al Qaeda attack—the TSP, Internet meta data collection, and telephony meta data collection—have been subject to various orders of the FISC and are no longer being conducted under Presidential authorization. The very existence of the meta data FISC orders—the FISC Pen Register Order (first issued in July 2004) and the FISC Telephone Records Order (first issued in May 2006)—remains classified. The President authorized the disclosure of the general existence of the January 10, 2007 FISC orders that

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 authorized electronic surveillance of [REDACTED] individuals in a manner similar to that
2 undertaken in the TSP, and President's authorization of the TSP lapsed in February 2007.

3 Information that may reveal the existence of the undisclosed FISC orders or the substance of any
4 of these orders should be protected from disclosure.

5 63. ~~(TS//SI~~ [REDACTED] ~~//OC//NF)~~ Disclosure of information about and within the
6 FISC orders would obviously reveal intelligence sources and methods currently being utilized by
7 the NSA under Court order and, thus, would cause exceptional harm to national security. For
8 example, as discussed above, the FISC Telephone Records Order requires certain
9 telecommunication companies to produce all of their telephony meta data to the NSA on a daily
10 basis and authorizes the NSA to access its archive of collected telephony meta data only when
11 the NSA has identified a known telephone number reasonably suspected to be associated with [REDACTED]

12 [REDACTED] The Order also provides that a telephone number
13 believed to be used by a U.S. person shall not be regarded as associated with [REDACTED]
14 [REDACTED] solely on the basis of activities that are protected by the First
15 Amendment. The FISC Pen Register Order authorizes the use of a pen register and trap and
16 trace device to collect Internet meta data [REDACTED] on similar
17 terms. Disclosure of these facts would reveal sensitive sources and methods utilized by the NSA
18 to obtain data utilized to track [REDACTED] contacts of [REDACTED]²⁰

19
20 ²⁰ ~~(TS//SI~~ [REDACTED] ~~//OC//NF)~~ For this reason, the FISC Telephone Records Order and
21 FISC Pen Register Orders prohibit any person from disclosing to any other person that the NSA
22 has sought or obtained the telephony meta data, other than to (a) those persons to whom
23 disclosure is necessary to comply with the Order; (b) an attorney to obtain legal advice or
24 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.

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 64. ~~(TS//SI~~ [REDACTED] ~~//OC//NF)~~ The intelligence activities authorized by the FISC
2 Pen Register and FISC Telephone Records Orders must not be compromised by the disclosure of
3 other information. For example, as discussed above, the disclosure of [REDACTED]

4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 Thus, any attempt to address the lawfulness of the meta data activities under Presidential
9 authorization prior to the FISC orders would directly risk disclosure of current NSA operations
10 under FISC Orders.

11 65. ~~(TS//SI~~ [REDACTED] ~~/TSP//OC//NF)~~ The disclosure of information concerning the
12 recent FISC Orders authorizing electronic surveillance would also harm national security. The
13 January 10, 2007 Foreign Telephone and Email Order authorized, among other things, electronic
14 surveillance of telephone and Internet communications [REDACTED]
15 when the Government determines that there is probable cause to believe that (1) one of the
16 communicants is a member or agent of [REDACTED] and (2)
17 the communication is to or from a foreign country, *i.e.*, a one-end foreign communication to or
18 from the United States.²¹ The telephone numbers and email addresses to be targeted (*i.e.*,
19 "selectors") under this order were further limited to those that the NSA reasonably believes are
20 being used by persons *outside* the United States. Under the order, every 30 days the Government
21 is required to submit a report to the FISA Court listing new selectors that the NSA has targeted

22 ²¹ ~~(TS//SI~~ [REDACTED] ~~/TSP//OC//NF)~~
23 [REDACTED] That fact, which is not relevant to this action, is, like
24 the other details in the orders, highly classified.

1 during the previous 30 days and briefly summarizing the basis for the NSA's determination that
2 the probable cause standard has been met.

3 66. ~~(TS//SI//OC//NF)~~ The surveillance under this new FISA Court Foreign
4 Telephone and Email Order, which is subject to detailed minimization and oversight procedures,
5 was authorized for 90 days and indicated that it may be reauthorized by the FISA Court upon
6 application by the Attorney General. The order states that, with each request for reauthorization,
7 the Government is required to present a list of current selectors previously reported to the FISA
8 Court that the Government intends to continue to task for collection under the reauthorization.
9 The order further indicated that, at any time, the FISA Court may request additional information
10 regarding particular selectors, and, if the Court finds that the applicable probable cause standard
11 is not met, it may direct that the surveillance under the order shall cease on the selector(s) in
12 question. This non-traditional order allowed the Government to target for collection
13 communications related to new [REDACTED] selectors used by terrorists without
14 having to seek advance approval from the FISA Court for each individual selector. Upon the
15 initiation of the surveillance authorized under the Foreign Telephone and Email Order, the NSA
16 monitored over [REDACTED] foreign selectors. [REDACTED] the reporting of these initial
17 selectors occurred over a 90-day period.

18 67. ~~(TS//SI//TSP//OC//NF)~~ [REDACTED]

19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

[REDACTED]

²³ While the general existence of the January 2007 orders, as described publicly by the Attorney General, is not classified, the number, nature, and contents of the specific orders described herein are highly classified. Among other things, disclosing to our enemies what surveillance activities, targets and methods are or are not covered by FISA Court orders would reveal sources and methods of intelligence gathering, and enable the enemy to alter its communications to evade detection.

68. ~~(TS//SI//OC/NF)~~ [REDACTED]

²² ~~(TS//SI//OC/NF)~~ [REDACTED]

²³ ~~(TS//SI//TSP//OC/NF)~~ [REDACTED]

[REDACTED] it plans to do so by a process in which it will obtain authorization of the FISA Court for each individual selector.

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 [REDACTED]
2 [REDACTED]
3 [REDACTED] however, did not grant the Government's application to renew the
4 surveillance authority in the Foreign Telephone and Email Order (concerning surveillance
5 targeting telephone numbers and e-mail addresses reasonably believed to be used by persons
6 outside the United States). Rather, it issued an Order and Memorandum opinion on April 3,
7 2007, declining to adopt the interpretation of the Foreign Intelligence Surveillance Act
8 underlying the Government's application for the Foreign Telephone and Email Order. The Court
9 nevertheless ordered that the Government could submit an application for a single extension of
10 the Foreign Telephone and Email Order to May 31, 2007. The Court contemplated that an
11 extension of surveillance authority to May 31 would allow the Government to submit an
12 application that might permit the Court "to authorize at least part of the [requested] surveillance
13 in a manner consistent with [its] order and opinion." On the Government's application, the
14 Court granted a separate order issued on April 5, 2007, extending the surveillance authority
15 granted by the Foreign Telephone and Email Order to May 31, 2007.

16 69. ~~(TS//SI//OC//NF)~~ The Government has reviewed the new FISA Court orders and
17 is working closely with the FISA Court in the hopes of developing an approach for continuing
18 the authorized surveillance beyond May 31, 2007, in a manner consistent with the April 3, 2007,
19 order of the FISA Court. The details of these orders, and targets implicated by the orders, like
20 the operational details and targets of the ongoing FISA Court-approved surveillance, are highly
21 classified. Thus, information about the nature of these recent FISC orders should not be
22 disclosed in this case.

23
24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 C. (U) Information That May Tend to Confirm or Deny Whether Verizon/MCI and/or
2 AT&T Has Assisted the NSA with the Alleged Intelligence Activities

3 70. (U) The third major category of information as to which I am supporting the
4 DNI's assertion of privilege, and asserting the NSA's statutory privilege, concerns information
5 that may tend to confirm or deny whether Verizon/MCI and/or AT&T has assisted the NSA with
6 the alleged intelligence activities. As set forth below, confirmation or denial of such information
7 would cause exceptionally grave harm to national security.

8 1. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~ [REDACTED]

9 71. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ Plaintiffs allege that they are customers of
10 Verizon and/or AT&T, and that those companies participate in the content surveillance dragnet
11 that Plaintiffs allege. See Amended Compl. ¶¶ 5-8. Neither company has participated in the
12 alleged dragnet, because such a program does not exist. [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 ²⁴ ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~ [REDACTED]

23 [REDACTED]

24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1

2

3

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

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

²⁵ ~~(TS//SI//OC/NF)~~ [REDACTED]

23

24

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

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

[REDACTED]

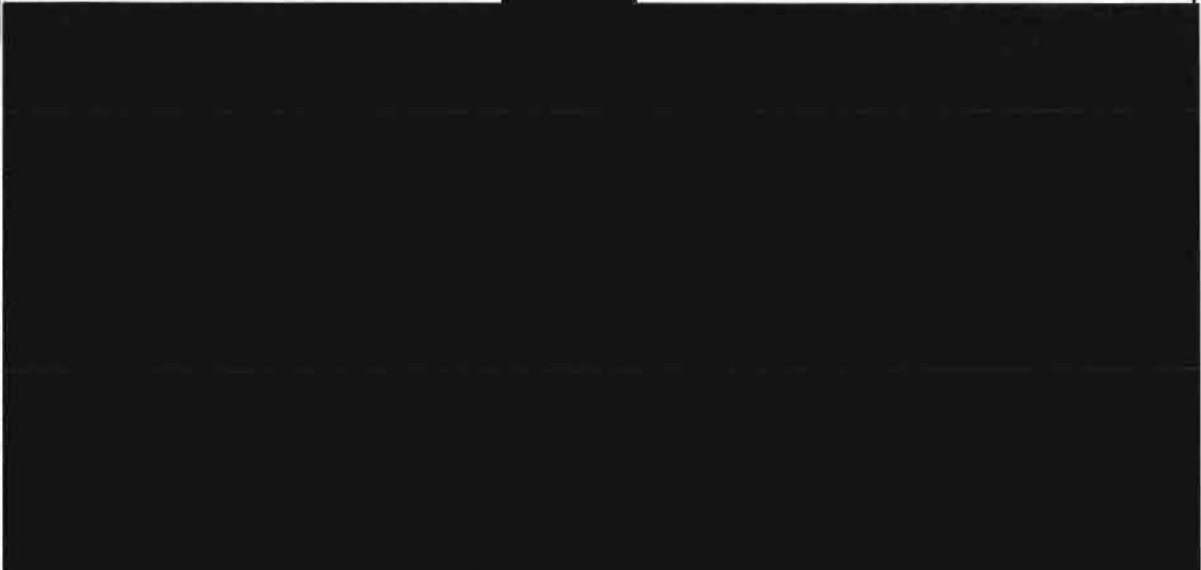
74. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~

[REDACTED]

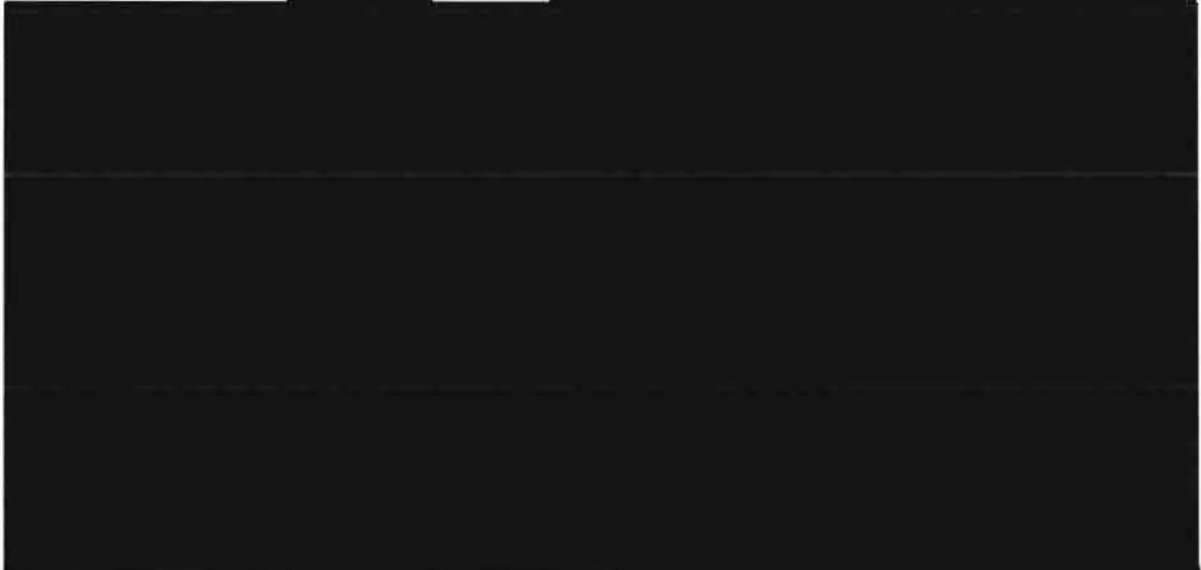
²⁶ ~~(TS//SI//OC/NF)~~

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

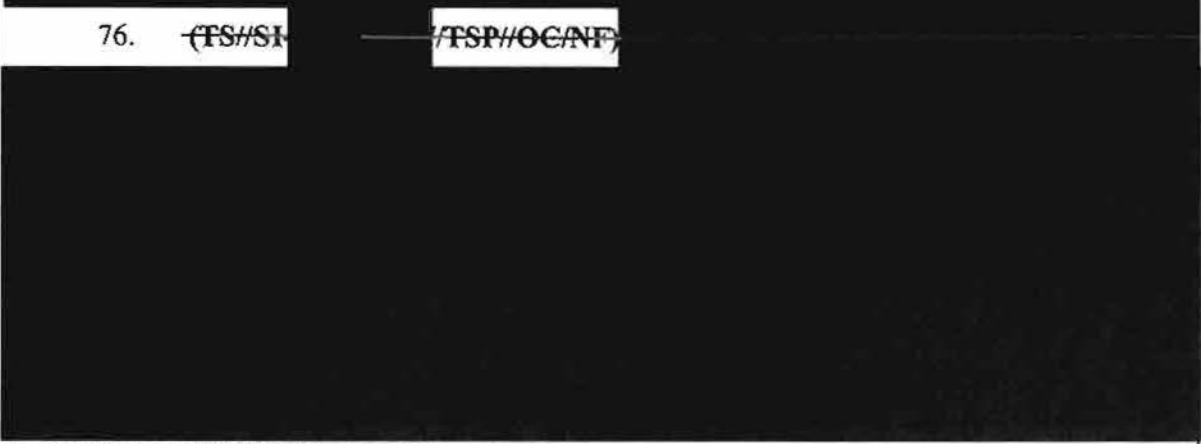
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



75. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~

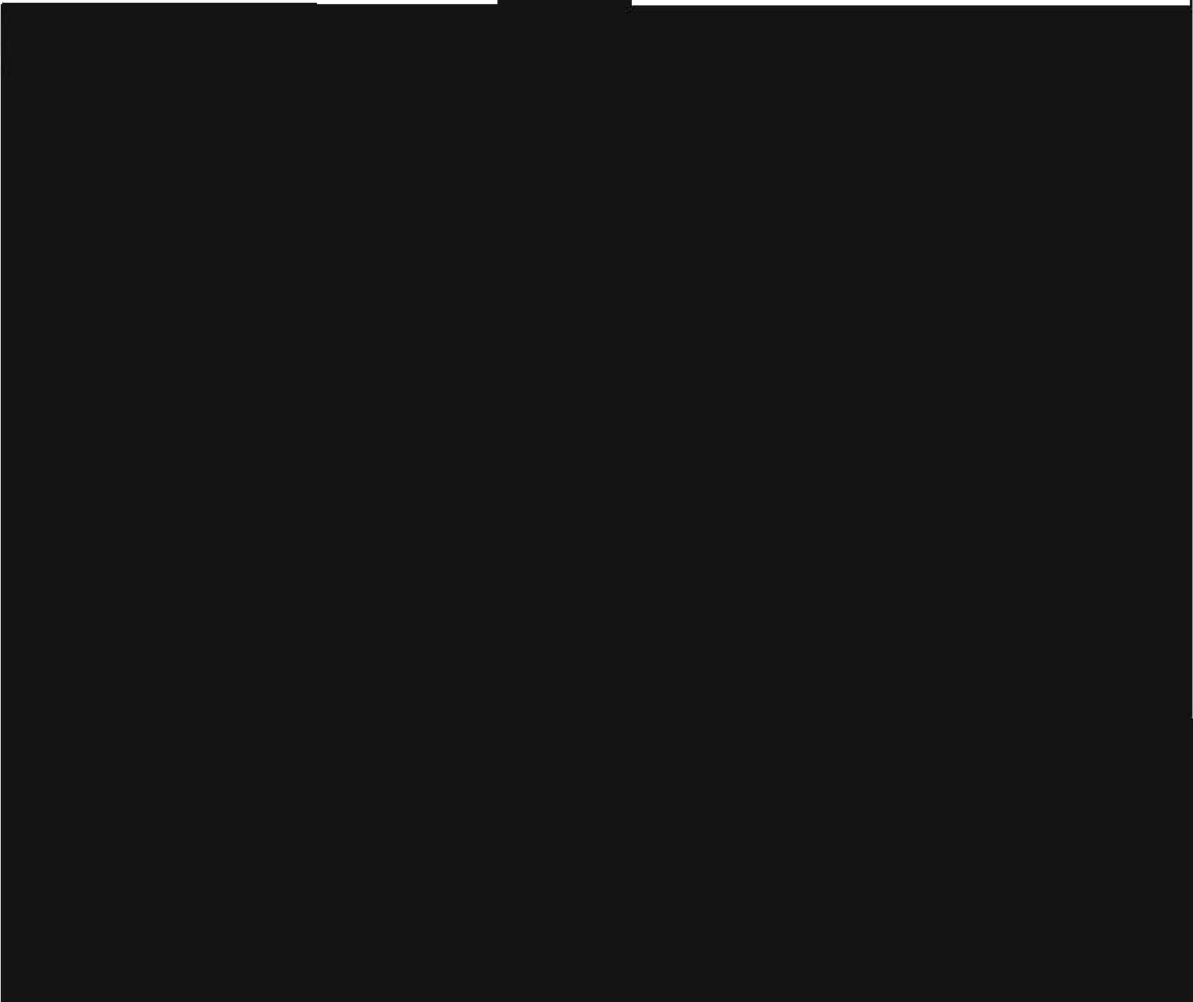


76. ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~



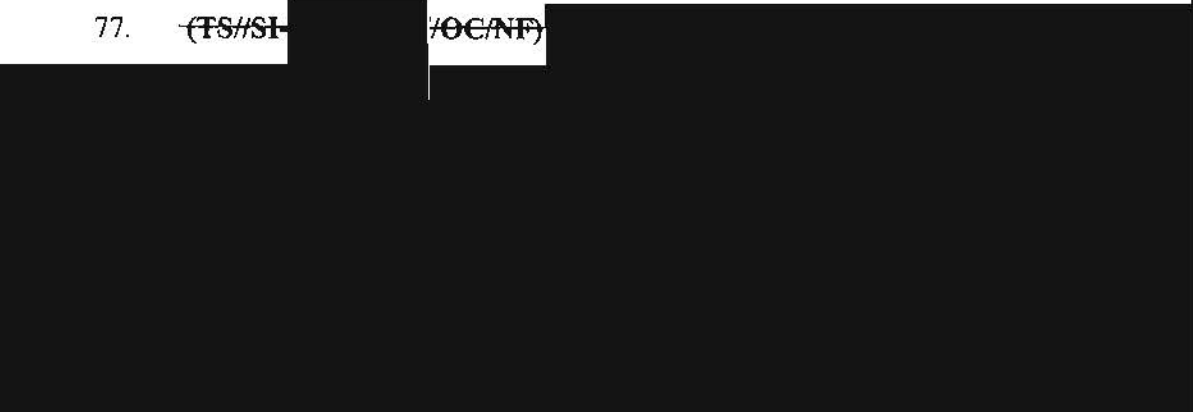
CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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



2. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~ Harm of Confirming or Denying Verizon/MCI and/or AT&T Assistance

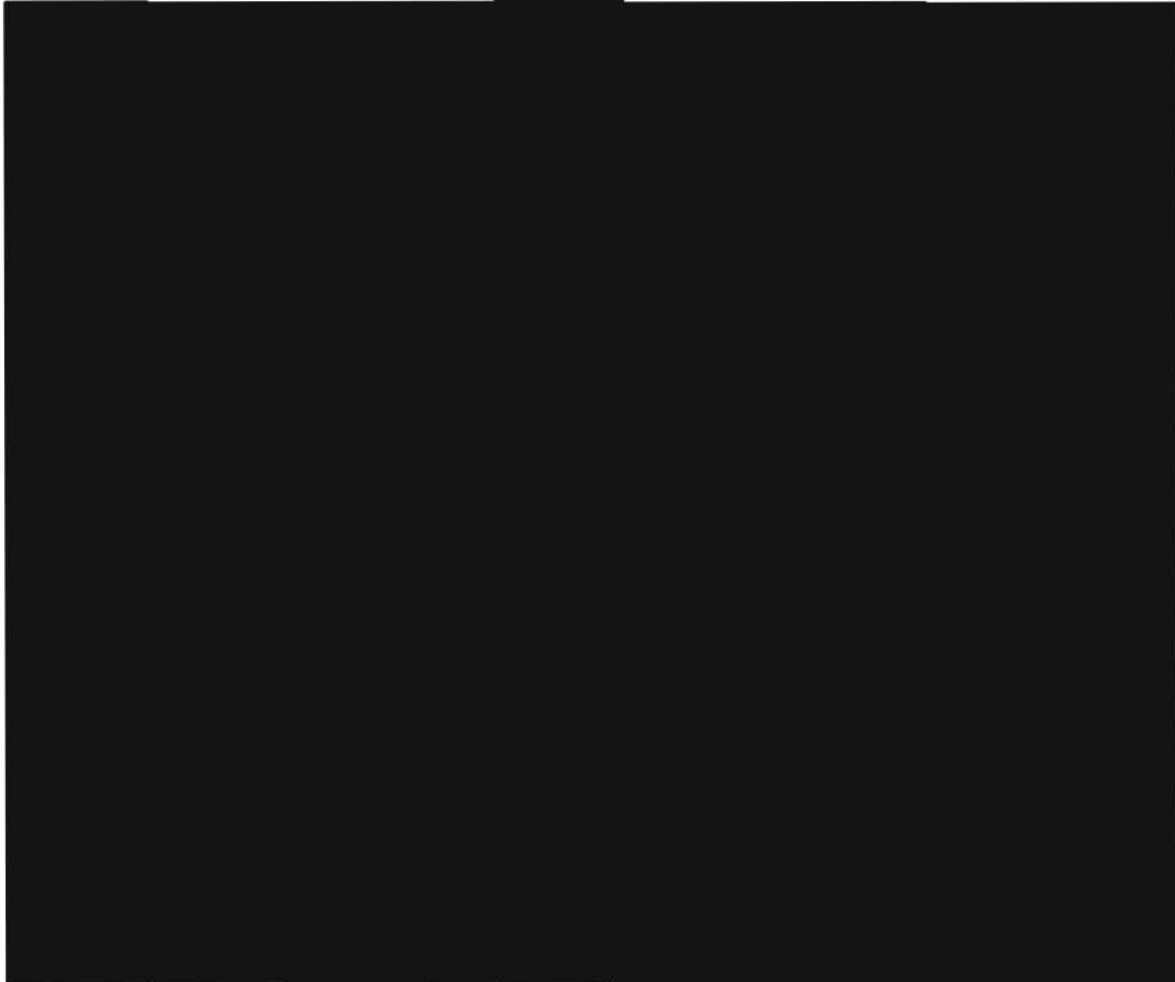
77. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~ [REDACTED]



²⁷ ~~(TS//SI~~ [REDACTED] ~~//TSP//OC/NF)~~ [REDACTED]

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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



78. ~~(TS//SI~~

~~//TSP//OC/NF)~~

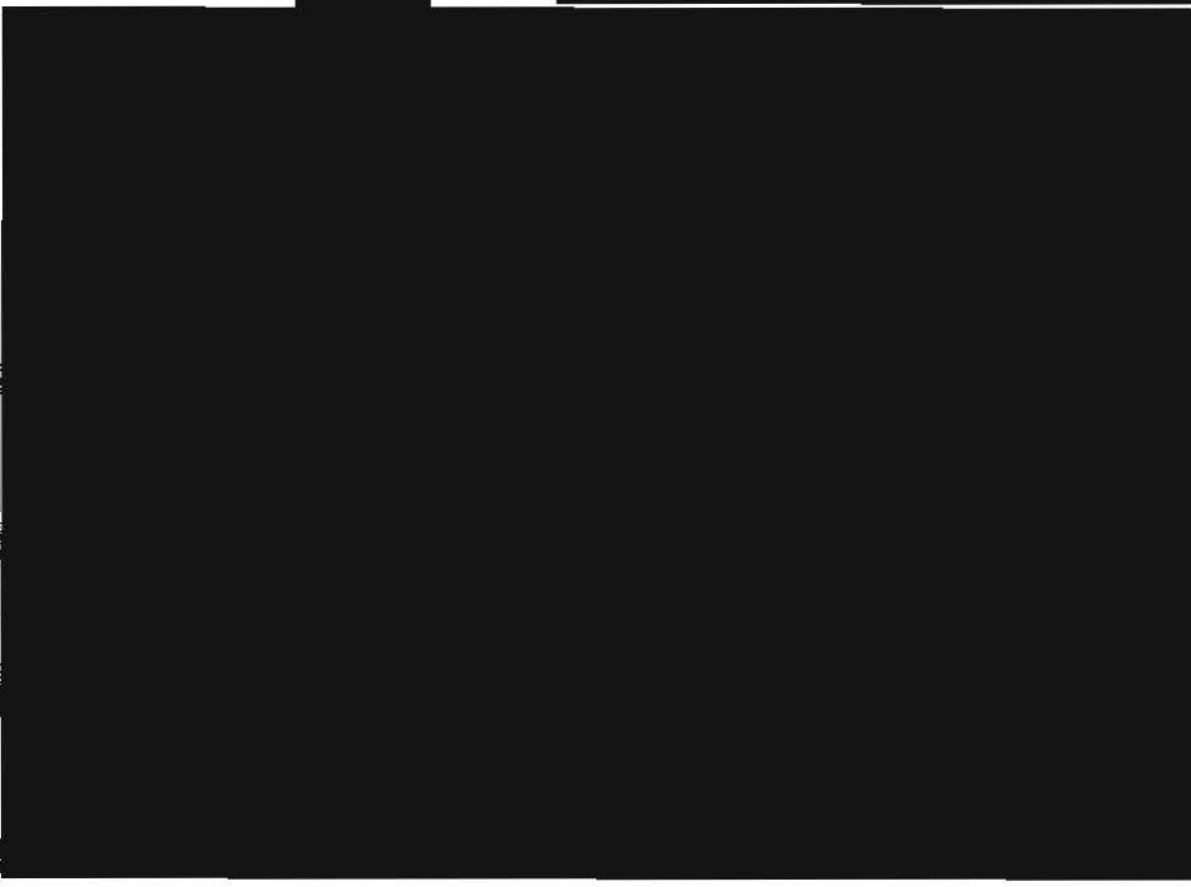
CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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



79. ~~(TS//SI)~~

~~//OC/NF)~~



CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

80. (TS//SI [REDACTED] //OC/NF) [REDACTED]

[REDACTED]

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

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

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

[REDACTED]

81. ~~(TS//SI~~ [REDACTED] ~~//NF)~~

[REDACTED]

VII. (U) Risks of Allowing Litigation to Proceed

82. ~~(TS//SI~~ [REDACTED] ~~//OC/NF)~~ Upon examination of the allegations, claims, facts, and issues raised by this case, it is my judgment that sensitive state secrets are so central to the subject matter of the litigation that any attempt to proceed will substantially risk the disclosure of the privileged state secrets described above. Although Plaintiffs challenge an alleged content surveillance dragnet that does not exist, proving why that is so, [REDACTED] would directly implicate highly classified intelligence information and activities. [REDACTED]

[REDACTED] In my judgment, any effort to probe the outer-bounds of such classified information would pose inherent and

1 significant risks of the disclosure of that information, including critically sensitive information
2 about NSA sources, methods, operations, targets, [REDACTED]

3 83. (S) Indeed, any effort merely to allude to those facts in a non-classified fashion
4 could be revealing of classified details that should not be disclosed. As noted, even seemingly
5 minor or innocuous facts, in the context of this case or other non-classified information, can tend
6 to reveal, particularly to sophisticated foreign adversaries, a much bigger picture of U.S.
7 intelligence gathering sources and methods.

8 **VIII. (U) Summary and Conclusion**

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

19 85. (TS//SI//NF) Al Qaeda seeks to use our own communications infrastructure
20 against us as they secretly attempt to infiltrate agents into the United States, waiting to attack at a
21 time of their choosing. One of the greatest challenges the United States confronts in the ongoing
22 effort to prevent another catastrophic terrorist attack against the Homeland is the critical need to
23 gather intelligence quickly and effectively. Time is of the essence in preventing terrorist attacks,

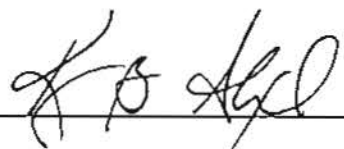
24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER
DIRECTOR, NATIONAL SECURITY AGENCY
CASE NO. 07-693; MDL NO. 06-1791

1 and the government faces significant obstacles in finding and tracking agents of al Qaeda as they
2 manipulate modern technology in an attempt to communicate while remaining undetected. The
3 NSA activities described herein are vital tools in this effort.

4 86. (S) For the foregoing reasons, in my judgment the disclosure of the information
5 discussed herein would cause exceptionally grave damage to the national security of the United
6 States. In addition to upholding the state secrets privilege and statutory privilege assertions by
7 the Director of National Intelligence in this case, I request that the Court also uphold my
8 assertion of NSA's statutory privilege to protect information about NSA activities. Finally, it is
9 my view that continued litigation of this lawsuit would risk the disclosure of sensitive classified
10 information and, accordingly, that the Court should not only protect from disclosure the
11 classified information described herein but dismiss this lawsuit.

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

14
15 DATE: 25 May 2007



16 LT. GEN. KEITH B. ALEXANDER
17 Director, National Security Agency