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

-HOP-SECRET//COMINT

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS

(1) All Actions Against the MCI and Verizon

Consolidated Complaint, Dkt. 125; (2) Bready,

Wireless (06-06570); and (4) Riordan, et al. v.

et al. v. Verizon Maryland (06-06313); (3) Chulsky

Defendants in the Master MCI and Verizon

et al. v. Cellco Partnership d/b/a Verizon

Verizon Communications (06-3574)

//TSP//ORCON/JUPOKN//MIL

1

2

3

4

LITIGATION

This Document Relates to:

5

6

7

9

10

12

11

13

14

15 16

17

18

19

20

21

22

23

24

) MDL Dkt. No. 06-1791-VRW

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY

SUBMITTED IN CAMERA, EX PARTE

Hon. Vaughn R. Walker

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

I. (U) Introduction

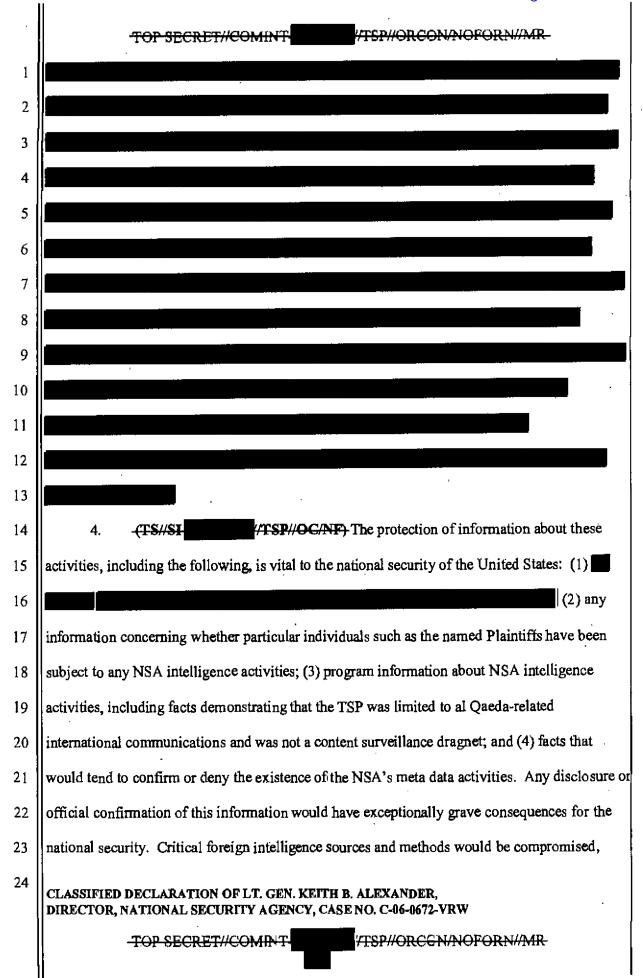
- 1. (U) I am the Director of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I am responsible for directing the NSA, overseeing the operations undertaken to carry out its mission and, by specific charge of the President and the Director of National Intelligence, 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 privilege under the National Security Act. Specifically, in the course of my official duties, I

Derived From: NSA/CSSM 1-52

Dated: 20041123 Declassify On: MR

· SECHETHCOMIN'II

TOP RECRETHEOMINT //TSP://OHCON/MOPORN//MR have been advised of this litigation and the allegations in the various complaints in this action 1 brought against the Verizon Defendants, including the MCI entities. As described herein. 2 various classified facts related to the Plaintiffs' claims are subject to the DNI's state secrets 3 privilege assertion. The disclosure of this information, which relates to NSA intelligence 4 5 information, activities, sources, and methods, reasonably could be expected to cause 6 exceptionally grave damage to the national security of the United States. In addition, it is my 7 judgment that sensitive state secrets are so central to the subject matter of the litigation that any 8 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 statements made herein are based on my personal knowledge of NSA activities and operations, 13 and on information available to me as Director of the NSA. 14 15 II. (U) Summary 16 3. **B//TSP//OC/NF)**. This lawsuit implicates several highly 17 classified and critically important NSA intelligence activities and, in particular, 18 Although Plaintiffs wrongly claim that the NSA 19 conducts a dragnet of surveillance of the content of millions of communications sent or received by people inside the United States, 20 21 22 (U) Any reference to "Verizon" in this declaration includes all Verizon Defendants in this matter. "Verizon" also specifically includes the MCI Defendants, which are now a part of 23 Verizon, even though "MCI" may at times be referenced separately. 24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW TOP SECRET//COMINT-- //TSP//ORCON/NOFORN//MR--



	TOP SECRET//COMINT
1	
2	and the ability
3	of the United States to
4	would be severely damaged.
5	5. (U) For these reasons, as set forth further below, the state secrets and statutory
6	privilege assertions that the DNI and I are making should be upheld and the information
7	described in this declaration should be protected from disclosure. I also believe that any further
8	litigation of this case poses exceptionally grave risks to the national security.
9	(U) <u>Table of Contents</u>
10	6. (TS//S) //TSP//OC/NF) To facilitate the Court's review, this
11	declaration is organized as follows:
12	I. Introduction
13	II. Summary
14	III. Classification of Declaration
15	IV. Background Information
16	A. The National Security Agency
17	B. September 11, 2001 and the Continuing al Qaeda Threat
18	V. Information Protected by Privilege
19	VI. Description of Information Subject to Privilege and the Harm of Disclosure
20	A. Information That May Tend to Confirm or Deny Whether Verizon/MCI Has Assisted the NSA with Any Alleged Intelligence Activities
21	Thas Assisted the NSA with Airy Allegen intelligence Activities
22	
23	
24	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	TOP SECRET//COMINT //TSP//ORCON/NOFORN//MR

]]		Case4	1.00-CV-04373-33VV DOCUMENT223 Filed03/03/14 Fages 01 49
			TOP SECRETI/COMINI
1			
2			
3			
4		_	The state of the Designation of the Disintiffer
5		В.	Information That May Tend to Confirm or Deny Whether or Not the Plaintiffs Have Been Subject to Any Alleged NSA Activities That May Be at Issue in This Matter
6			
7			1.
8			2.
9			3. Harm of Disclosure
10		Ċ.	Information Concerning NSA Activities, Sources, and Methods, and the Harm of Disclosure
11			1. Information Concerning Plaintiffs' Allegations of Content Surveillance
12			2. Information Concerning Meta Data Activities
13			3. Information Demonstrating the Success of TSP and Meta Data Activities
14			4. Information Concerning the FISC Orders
15	VII.	Risks	of Allowing Litigation to Proceed
16	V111.	Summ	nary and Conclusion
17			III. (U) Classification of Declaration
18		7.	(S) This declaration is classified TOP SECRET//COMINT
19			/TSP//ORCON/NOFORN//MR pursuant to the standards in Executive Order No.
20	12958	, as am	ended by Executive Order No. 13292. Under Executive Order No. 12958,
21	inform	nation i	s classified "TOP SECRET" if unauthorized disclosure of the information
22	reason	nably co	ould be expected to cause exceptionally grave damage to the national security of the
23	Unite	d States	s; "SECRET" if unauthorized disclosure of the information reasonably could be
24			DECLARATION OF LT. GEN. KEITH B. ALEXANDER, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	1		-TOP SECRET//COMINT

TOP-SECRET//COMINT ///TSP//ORCON/NOFORN//MR

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

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

² (TS//SI//NF)

CLASSIFIED DECLARATION OF LT, GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW

-TOP-SECRET//COMINT

-FOP-SECRETHEOMINT DIFFSP//ORCON/NOFORH//MR. //TSP//OC/NF) This declaration also contains information 1 9. related to or derived from the Terrorist Surveillance Program (TSP), a controlled access signals 2 3 intelligence program authorized by the President in response to the attacks of September 11, 2001. Although the President publicly acknowledged the existence of the TSP in December 4 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. 8 9 10 11 12 13 10. 14 (S) In addition to the fact that classified information contained herein may not be revealed to any person without authorization pursuant to Executive Order 12958, as amended, 15 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 ³ (S) 23 24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW

##TSP#ORCON/NOFORN//MR

TOP SECRET//COMINT-

-TOP SECRET//COMINT

#THP#ORCON/MOPORPH#MR:

1

2

3 4

5

6 7

8 9

10

11 12

13

14

15

16 17

18

19

20

21

22

23

24

IV. (U) Background Information

(U) Background on The National Security Agency

- 11. (U) The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. Under Executive Order 12333, § 1.12(b), as amended, the NSA's cryptologic mission includes three functions: (1) to collect, process, and disseminate signals intelligence (SIGINT) information, of which COMINT is a significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations; (2) to conduct information security activities; and (3) to conduct operations security training for the U.S. Government.
- 12. (TS//SI) Signals intelligence (SIGINT) consists of three subcategories: (1) communications intelligence (COMINT); (2) electronic intelligence (ELINT); and (3) foreign instrumentation signals intelligence (FISINT). Communications intelligence (COMINT) is defined as "all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients." 18 U.S.C. § 798. COMINT includes information derived from the interception of foreign and international communications, such as voice, facsimile, and computer-to-computer information conveyed via a number of means
- Electronic intelligence (ELINT) is technical intelligence information derived from foreign non-communications electromagnetic radiations except atomic detonation or radioactive sources-in essence, radar systems affiliated with military weapons platforms (e.g., anti-ship) and civilian systems (e.g., shipboard and air traffic control radars). Foreign instrumentation signals intelligence (FISINT) is derived from non-U.S. aerospace surfaces and subsurface systems which may have either military or civilian applications.

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW 1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

TOP SECRET//COMINT-[/TSP//ORCON/NOFORN//MR

- 13. (S) The NSA's SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities set forth in Executive Order No. 12333, § 1.12(b), as amended. In performing its SIGINT mission, NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications and related information. The technological infrastructure that supports the NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated collection and processing technology.
- 14. (U) There are two primary reasons for gathering and analyzing foreign intelligence information. The first, and most important, is to gain information required to direct U.S. resources as necessary to counter external threats. The second reason is to obtain information necessary to the formulation of U.S. foreign policy. Foreign intelligence information provided by the NSA is thus relevant to a wide range of important issues, including military order of battle; threat warnings and readiness; arms proliferation; international terrorism; and foreign aspects of international narcotics trafficking.
- 15. (S) The NSA's ability to produce foreign intelligence information depends on its access to foreign and international electronic communications. Foreign intelligence produced by COMINT activities is an extremely important part of the overall foreign intelligence information available to the United States and is often unobtainable by other means. Public disclosure of either the capability to collect specific communications or the substance of the information derived from such collection itself can easily alert targets to the vulnerability of their communications. Disclosure of even a single communication holds the potential of revealing intelligence collection techniques that are applied against targets around the world. Once alerted,

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW TOP SECRET//COMINT

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

I//TSP//OH.COM/NOPORN//MR-

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.

16. (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 deathsthe highest single-day death toll from hostile foreign attacks in the Nation's history. In addition, these attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars of damage to the economy.

CLASSIFIED DECLARATION OF LT. GEN, KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW

TOP SECRET//COMINT

/TSP//ORCION/MOFORN/MR

TOP SECRET//COMINT //TSP//ORCON/NOFORN//MR

1

2

3

4

5

6

7

. 8

9

10

11

12

13

14

15

16

17

- 18

19

20

21

22

23

24

- (U) On September 14, 2001, the President declared a national emergency "by 17. reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." Proclamation No. 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001). The United States also immediately began plans for a military response directed at al Qaeda's training grounds and haven in Afghanistan. On September 14, 2001, both Houses of Congress passed a Joint Resolution authorizing the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11. Authorization for Use of Military Force, Pub. L. No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept. 18, 2001) ("Cong. Auth."). Congress also expressly acknowledged that the attacks rendered it "necessary and appropriate" for the United States to exercise its right "to protect United States citizens both at home and abroad," and acknowledged in particular that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," Id. pmbl.
- (U) As the President made clear at the time, the attacks of September 11 "created 18. a state of armed conflict." Military Order, § 1(a), 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001). Indeed, shortly after the attacks, NATO took the unprecedented step of invoking article 5 of the North Atlantic Treaty, which provides that an "armed attack against one or more of [the parties] shall be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246. The President also determined that al Qaeda terrorists "possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER. DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW TOP SECRET/COMIN'F

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

б

- States found itself immediately propelled into a worldwide war against a network of terrorist groups, centered on and affiliated with al Qaeda, that possesses the evolving capability and intention of inflicting further catastrophic attacks on the United States. That war is continuing today, at home as well as abroad. Moreover, the war against al Qaeda and its allies is a very different kind of war, against a very different enemy, than any other war or enemy the Nation has previously faced. Al Qaeda and its supporters operate not as a traditional nation-state but as a diffuse, decentralized global network of individuals, cells, and loosely associated, often disparate groups, that act sometimes in concert, sometimes independently, and sometimes in the United States, but always in secret—and their mission is to destroy lives and to disrupt a way of life through terrorist acts. Al Qaeda works in the shadows; secrecy is essential to al Qaeda's success in plotting and executing its terrorist attacks.
- 20. (TS//SI//NF) The In Camera Declaration of Michael McConnell, Director of National Intelligence, details the particular facets of the continuing al Qaeda threat and, thus, the exigent need for the NSA intelligence activities described here. The NSA activities are directed at that threat

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

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW

TOP SECRET//COMINT

TSP//GRCON/NOFORN//MR

	THE SECHET//COMIN'T
1	providers, or "ISPs," and other providers of communications services offer a wide variety of
2	global communications options, often free of charge.
3	
4	
5	21. (TS//SI//NF)
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	22. (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	4 (TS//SI//OC/NF)
23	
24	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	-TOP SECRET//COMINT- ///TSP//ORCON/NOFORN//MR

TOP SECRET//COMINT

H/TSP//ORCON/NOFORN//MR-

States. Communications intelligence often is the only means we have to learn the identities of particular individuals who are involved in terrorist activities and the existence of particular terrorist threats. Second, at the same time that communications intelligence is more important than ever, the decentralized, non-hierarchical nature of the enemy and their sophistication in exploiting the agility of modern telecommunications make successful communications intelligence more difficult than ever. It is against this backdrop that the risks presented by this litigation should be assessed, in particular the risks of disclosing particular NSA sources and methods implicated by the claims,

9

10

11

12

13

14

15

16

17

18

19

20

21

22

8

1

2

3

4

5

6

7

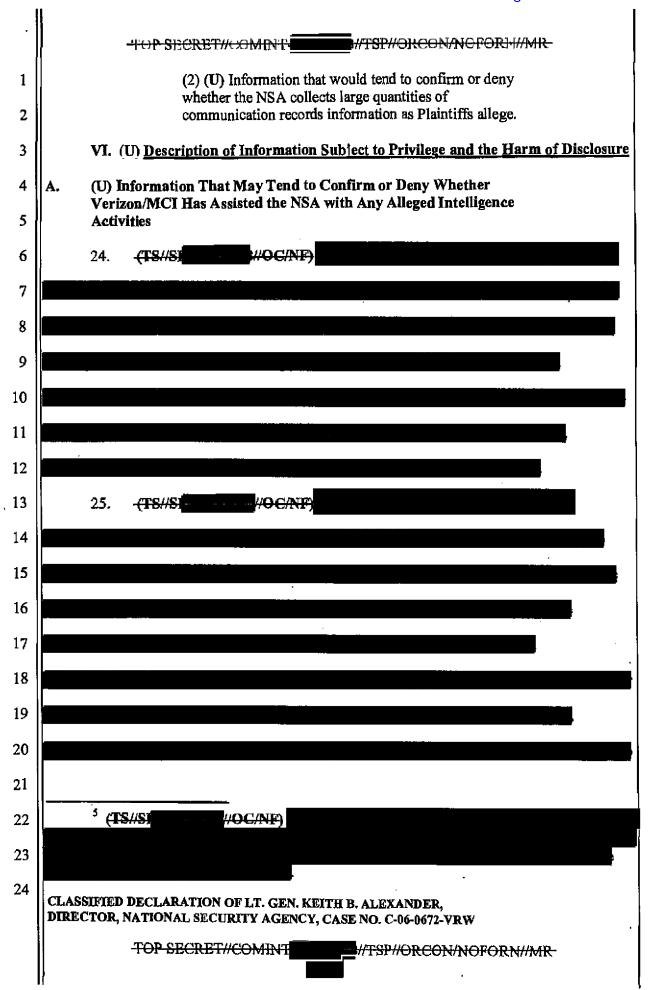
V. (U) Information Protected by Privilege

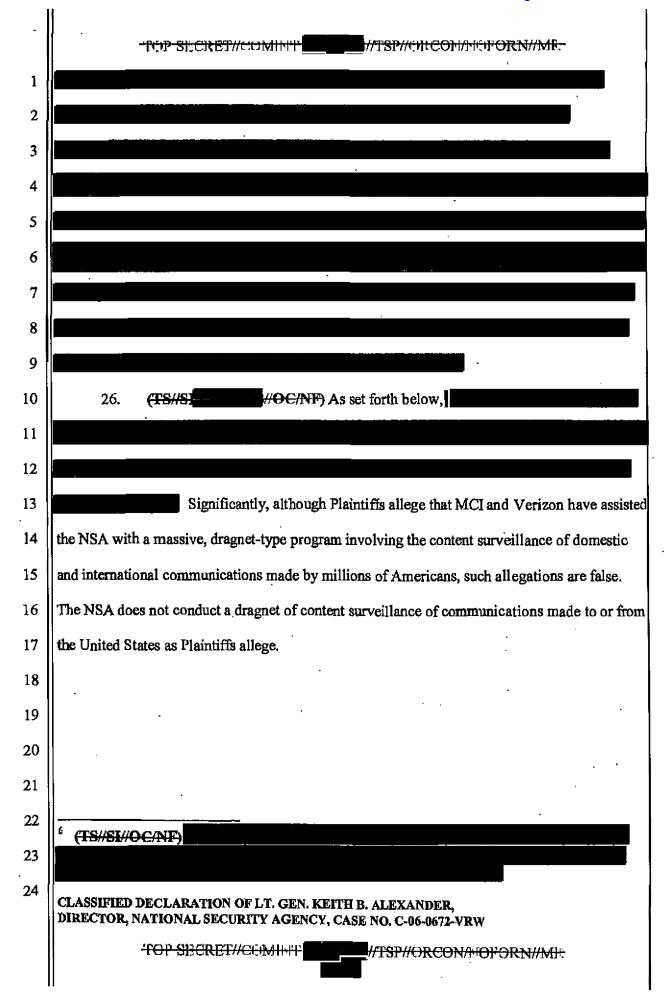
- 23. (U) As set forth further below, the following categories of information are subject to the DNI's assertion of the state secrets privilege and statutory privilege under the National Security Act, as well as my assertion of the NSA privilege:
 - A. (U) Information that may tend to confirm or deny whether Verizon/MCI has assisted the NSA with any alleged intelligence activities; and
 - B. (U) Information that may tend to confirm or deny whether the Plaintiffs have been subject to any of the alleged NSA intelligence activities that may be at issue in this matter; and
 - C. (U) Information concerning any NSA intelligence, activities, sources, or methods, including:
 - (1) (U) Information concerning the scope and operation of the Terrorist Surveillance Program, including information that may be needed to demonstrate that the TSP was limited to one-end foreign al Qaeda communications and that the NSA does not otherwise engage in the content surveillance dragnet that the Plaintiffs allege: and

23

24

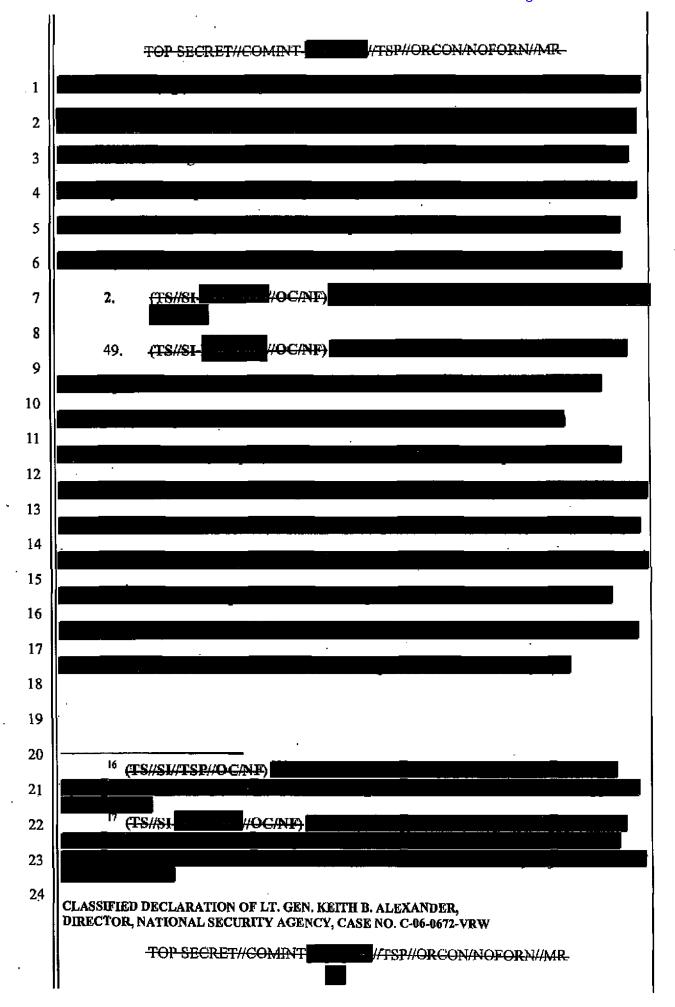
CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER. DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW



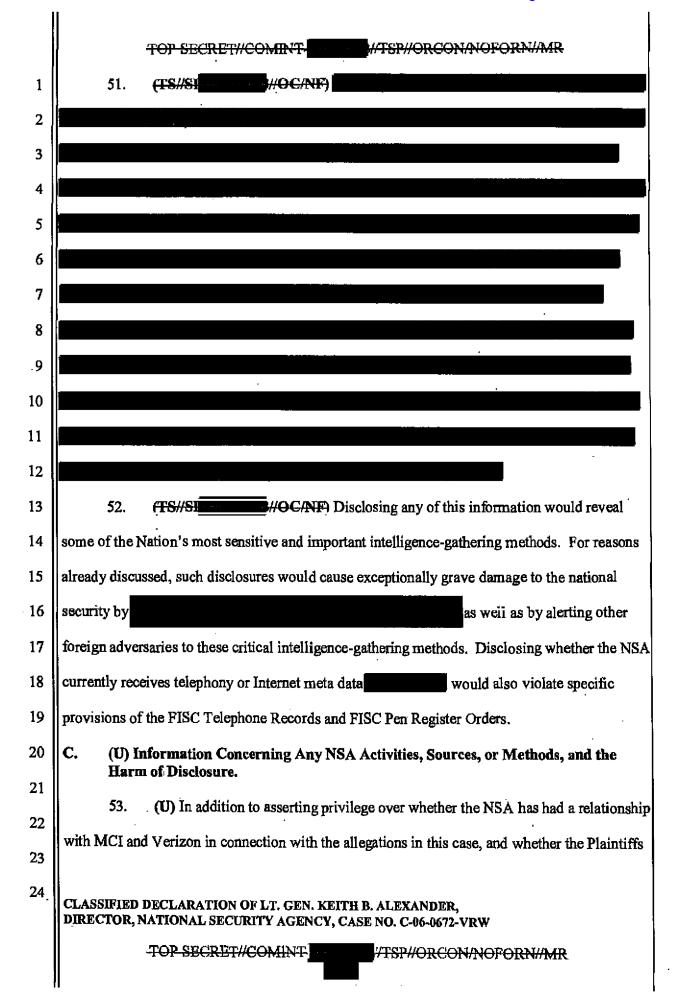


[[Page(s) Redacted]]

	-TOP SECRET//COMINT ///TSP//ORCON/NOFORN//MR
1	B. (U) Information That May Tend to Confirm or Deny Whether the Plaintiffs Have Been Subject to Any Alleged NSA Activities That May Be at Issue in This Matter
2	47. (U) The second major category of information as to which I am supporting the
4	DNI's assertion of privilege, and asserting the NSA's own statutory privilege, concerns
5	information as to whether particular individuals, including the Plaintiffs in the lawsuits against
6	Verizon, have been subject to alleged NSA intelligence activities. As set forth below,
7	confirmation or denial of such information would cause exceptionally grave harm to national
8	security.
9	1. (TS//SI//TSP//OC/NF)
10	48. (TS//SI//TSP//OC/NF) The named Plaintiffs in this action—which are those
11	listed in paragraphs 24-123 of the Master Consolidated Complaint Against MCI Defendants and
12	Verizon Defendants, as well as those named in the complaints in the <i>Bready</i> , <i>Riordan</i> , and
13	Chulsky actions—allege that the content of their telephone and Internet communications and
14	information related to those communications have been and are being intercepted, disclosed,
15	divulged, and/or used without judicial or other lawful authorization. The NSA does not engage
16	in a program of "dragnet" surveillance that captures the contents of all domestic telephone or
17	Internet communications as Plaintiffs allege,
18	
19	
20 21	
22	
23	
24	
- -	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER. DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	TOP SECRET//COMINT- /TSP//ORCON/NOFCRN//MR



TOP SECRET//COMINTY TSP//ORCON/NOFORN//MR-1 3. (U) Harm of Disclosure 2 50. (TS//SI//TSP//OC/NF) 3 First, as a matter of course, the NSA cannot publicly confirm 4 5 or deny whether any individual is subject to the surveillance activities described herein, because 6 to do so would tend to reveal actual targets. For example, if the NSA were to confirm in this 7 case and others that specific individuals are not targets of surveillance, but later refuse to comment (as it would have to) in a case involving an actual target, a person could easily deduce 8 9 by comparing such responses that the person in the latter case is a target. The harm of revealing 10 targets of foreign intelligence surveillance should be obvious. If an individual knows or suspects he is a target of U.S. intelligence activities, he would naturally tend to alter his behavior to take 11 . 12 new precautions against surveillance, 13 14 15 In addition, revealing 16 who is not a target would indicate who has avoided surveillance and who may be a secure 17 channel for communication. Such information could lead a person, secure in the knowledge that 18 he is not under surveillance, to help a hostile foreign adversary convey information; 19 alternatively, such a person may be unwittingly utilized or even forced to convey information 20 through a secure channel. Revealing which channels are free from surveillance and which are 21 not would also reveal sensitive intelligence methods and thereby could help any adversary evade detection. 22 23 24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW TOP SECRET//COMIN'I H/TSP//ORCON/NOFORN//MR



TOP SECRET//COMINT //TSP//ORCON/NOFORN//MR

have been subject to any alleged intelligence activities, I am supporting the DNI's assertion of privilege and asserting the NSA's statutory privilege over any other facts concerning NSA intelligence sources and methods that would be needed to resolve this case. This includes: (1) facts concerning the operation of the Terrorist Surveillance Program and any other NSA intelligence activities needed to demonstrate that the TSP was limited as the President stated to the interception of one-end foreign communications reasonably believed to involve a member or agent of al Qaeda or an affiliated terrorist organization and that the NSA does not otherwise conduct a dragnet of content surveillance as the Plaintiffs allege; and (2) facts that would confirm or deny whether the NSA collects large quantities of communication records information as the Plaintiffs allege. As set forth below, the disclosure of information needed to address these allegations would cause exceptionally grave harm to national security.

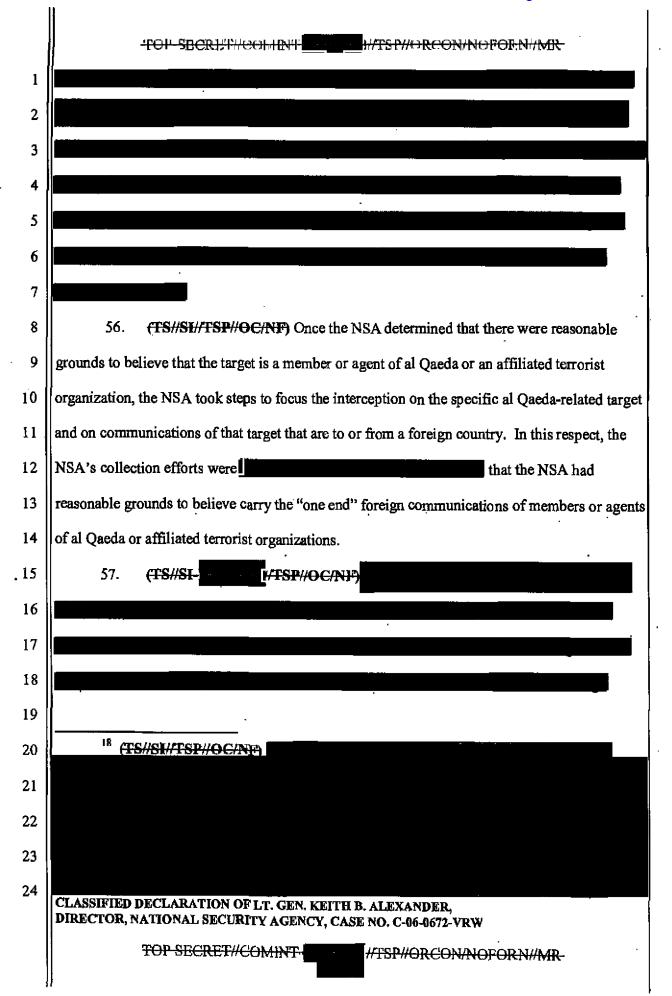
- 1. (U) Information Concerning Plaintiffs' Allegations of Content Surveillance.
- attacks, he authorized the NSA to intercept the content of certain communications for which there are reasonable grounds to believe that (1) such communication originated or terminated outside the United States, and (2) a party to such communication is a member or agent of al Qaeda or an affiliated terrorist organization. The President stated at the time that this activity, now referred to as the Terrorist Surveillance Program, did not involve the collection of purely domestic communications, or international communications with no al Qaeda connection, and these facts were reiterated publicly by the Attorney General and then-Deputy Director of National Intelligence. Nonetheless, I am advised that the Plaintiffs have alleged that the NSA "intercepts millions of communications made or received by people inside the United States, and uses powerful computers to scan their contents for particular names, numbers, words, or

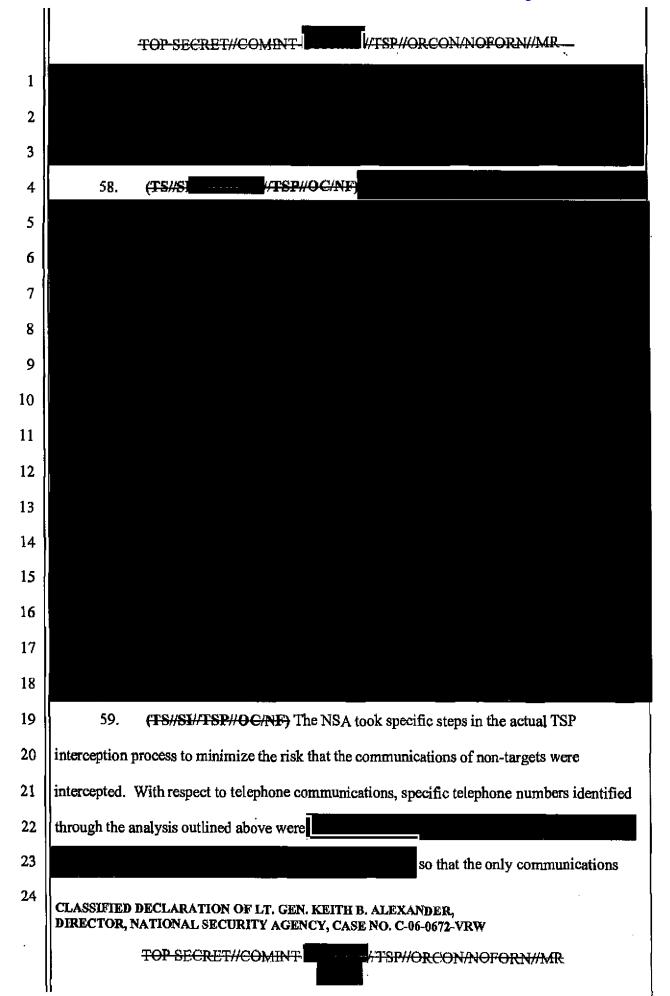
CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW

TOP-SECRET//COMIN'T

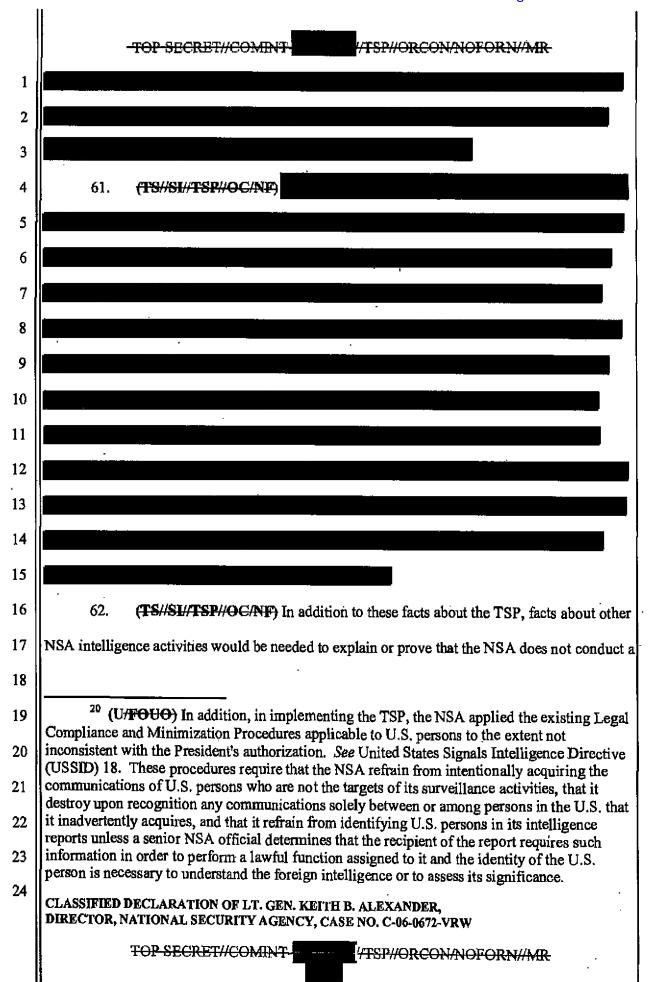
i	I
	TOP SECRET//COMINT ////TSP//ORCON/NOFORN//MR
1.	phrases." Master Verizon Complaint ¶ 165. As the President made clear in describing the
2	limited scope of the TSP, such allegations of a content surveillance dragnet are false. But if the
3	NSA had to demonstrate in this case that the TSP was limited as the President stated, and not a
4	dragnet as the Plaintiffs claim, and that the NSA does not otherwise engage in the dragnet that
5	Plaintiffs allege, sensitive and classified facts about the operation of the TSP and NSA
6	intelligence activities would have to be disclosed.
7	55. (TS//SI//TSP//OC/NF) The privileged information that must be protected from
8	disclosure includes the following classified details demonstrating the limited nature of the TSP.
9	First, interception of the content of communications under the TSP was triggered by a range of
10	information, including sensitive foreign intelligence, obtained or derived from various sources
11	indicating that a particular phone number or email address is reasonably believed by the U.S.
12	Intelligence Community to be associated with a member or agent of al Qaeda or an affiliated
13	terrorist organization. Professional intelligence officers at the NSA undertook a careful but
14	expeditious analysis of that information, and considered a number of possible factors, in
15	determining whether it would be appropriate to target a telephone number or email address unde
16	the TSP. Those factors included whether the target phone number or email address was: (1)
17	reasonably believed by the U.S. Intelligence Community, based on other authorized collection
18	activities or other law enforcement or intelligence sources, to be used by a member or agent of a
19	Qaeda or an affiliated terrorist organization;
20	
21	
22	
23	
24	

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW





1	l
	TOP SECRET//COMINT //TSP//ORCON/NOFORN/MIC
1	intercepted were those to or from the targeted number of an individual who was reasonably
2	believed to be a member or agent of al Qaeda or an affiliated terrorist organization. For Internet
3	communications, the NSA used identifying information obtained through its analysis of the
4	target, such as email addresses to target for collection the communications of
5	individuals reasonably believed to be members or agents of al Qaeda or an affiliated terrorist
6	organization. 19
7	60. (TS//SI//TSP//OC/NF) In addition to procedures designed to ensure that the TSP
8	was limited to the international communications of al Qaeda members and affiliates, the NSA
9	also took additional steps to ensure that the privacy rights of U.S. persons were protected.
10	
11	
12	
13	
14	
15	
16	
17	19 (TS//SI //TSP//OC/NF)
18	
19	At no point did the NSA search the content of the communications with "key words" other than the targeted
20	selectors themselves. Rather, the NSA targeted for collection only email addresses associated with suspected members or agents of al Qaeda or affiliated
21	terrorist organizations, or communications in which such were mentioned. In addition, due to technical limitations of the hardware and software currently used, incidental collection of non-target correspondence becomes and software currently used.
22	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 processed to disseminated.
23	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.
24	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	TOP SECRET//COMINT-

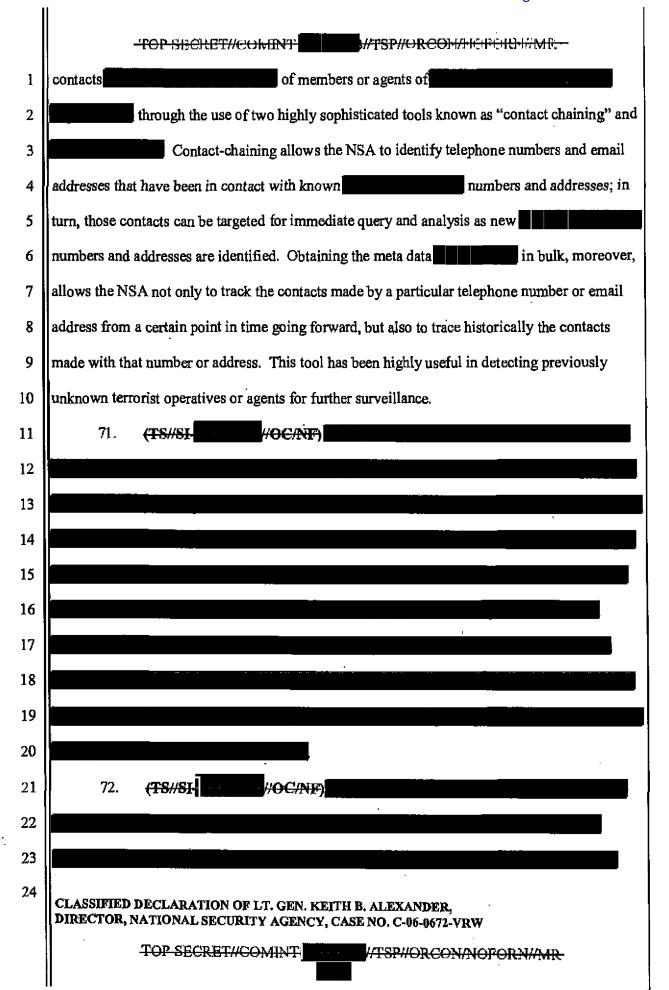


]
	TOP SECRET//COMINT //TSP//ORCON/NOFORN//MR
1	dragnet as Plaintiffs allege.
2	
3	
4	
5	
6	
7	None of these activities, however, could be
8	disclosed to address and rebut Plaintiffs' dragnet allegations without causing exceptionally grave
9	damage to the national security.
10	63. (U) Finally, to the extent the Plaintiffs in this case are challenging the lawfulness
11	of the TSP itself, facts about the operation of that program (which remain highly classified) also
12	could not be disclosed.
13	64. (TS//SI//TSP//OC/NF) For example, in conjunction with meta data analysis, the
14	TSP provided far greater operational swiftness and effectiveness for identifying the al Qaeda
15	terrorist network in the United States than the traditional procedures that had been used under the
16	Foreign Intelligence Surveillance Act. In order to ascertain as rapidly as possible the potential al
17	Qaeda terrorist threats facing the United States, the NSA must know not only what a foreign
18	terrorist target says in a particular telephone or Internet intercept, but with whom that person has
19	been communicating. To the extent individual court orders for all TSP targets could have been
20	required in advance under traditional FISA procedures, the NSA would have been unable to
21	target communications sent to and from new phone numbers or Internet accounts as quickly, and
22	valuable intelligence could have been lost.
23	
24	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	TOP SECRET//COMINT

İ	
ľ	*POP-SECRET//COMIN'P
1	65. (TS//SI//TSP//OC/NF) As noted,
2	
3	the TSP, in conjunction with meta data collection and analysis,
4	allowed the NSA to obtain rapidly not only the content of a particular communication, but
5	connections between that target and others who may form a web of al Qaeda conspirators. In
6	some cases, the NSA was able to begin collection on a target phone number in
7	to begin collection on a targeted phone number or
8	email address. In contrast, if individual applications have to be prepared and approved through
9	the traditional FISA process before the NSA can target a newly identified phone number or email
10	account associated with al Qaeda, vital information could be lost in the interim. The traditional
11	FISA process is a highly effective tool for many types of surveillance activities,
12	
13	
14	· · · · · · · · · · · · · · · · · · ·
15	
16	it would have had
17	to stop and demonstrate, through a multi-layered process involving NSA and DOJ counsel, the
18	Attorney General, and the FISA Court, that each of numerous, target numbers
19	or emails requires coverage. Where the gravest of dangers are at stake—a catastrophic mass
20	casualty terrorist attack against the U.S. Homeland and the corresponding need to track
21	thousands of potential terrorists—and where
22	21 (FIGURE / FIGURE)
23	21 (TS//SI//TSP//OC/NF)
24	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER,
•	DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	TOP SECRET//COMINT

	i · · · · · · · · · · · · · · · · · · ·
	##OP-SECRET#COMINT
1	to hide their communications and tracks, it is vital that the NSA be able to track multiple
2	communications, contacts, and as rapidly as possible to fulfill its mission to protect the
3	national security of the United States.
4	66. (TS//SL//TSP//OC/NF) None of the foregoing information about the Textorist
5	Surveillance Program could be disclosed in this case, however, without causing exceptionally
6	grave harm to the national security. Even though the President has determined not to reauthorize
7	the TSP, revealing how the program operated would provide key insights to foreign adversaries
8	as to how the NSA monitors communications. Information about the specific foreign
9	intelligence factors that triggered interception under the TSP would obviously reveal to foreign
10	adversaries the very facts that would most likely lead to their communications being intercepted,
11	even under the current FISA Court Orders, thereby giving adversaries a roadmap as to how to
12	avoid such interception.
13	
14	
14 15	
	67. (TS//SI//TSP//OC/NF) Likewise, information about the speed and agility with
15	67. (TS//SI//TSP//OC/NF) Likewise, information about the speed and agility with which the NSA can collect content on a target, and how long it might maintain surveillance,
15 16	
15 16 17	which the NSA can collect content on a target, and how long it might maintain surveillance,
15 16 17 18	which the NSA can collect content on a target, and how long it might maintain surveillance, would provide invaluable insights for an adversary to devise new and different ways to protect
15 16 17 18 19	which the NSA can collect content on a target, and how long it might maintain surveillance, would provide invaluable insights for an adversary to devise new and different ways to protect their communications. In particular, disclosure of the NSA's ability to utilize the TSP (or,
15 16 17 18 19 20	which the NSA can collect content on a target, and how long it might maintain surveillance, would provide invaluable insights for an adversary to devise new and different ways to protect their communications. In particular, disclosure of the NSA's ability to utilize the TSP (or, therefore, the current FISA Court-authorizes content collection) in conjunction with contact
15 16 17 18 19 20 21	which the NSA can collect content on a target, and how long it might maintain surveillance, would provide invaluable insights for an adversary to devise new and different ways to protect their communications. In particular, disclosure of the NSA's ability to utilize the TSP (or, therefore, the current FISA Court-authorizes content collection) in conjunction with contact chaining would severely undermine efforts to detect terrorist activities.
15 16 17 18 19 20 21 22	which the NSA can collect content on a target, and how long it might maintain surveillance, would provide invaluable insights for an adversary to devise new and different ways to protect their communications. In particular, disclosure of the NSA's ability to utilize the TSP (or, therefore, the current FISA Court-authorizes content collection) in conjunction with contact chaining would severely undermine efforts to detect terrorist activities. Armed with this knowledge, an adversary could make more robust use

	TOP SECRET//COMINT.
1	
2	Compromise of one NSA
3	method of surveillance, even no longer in use, can easily lead to evasive actions as to other
4	current methods that would deprive U.S. decision-makers of critical information needed to detect
5	al Qaeda terrorist threats.
6	2. (TS//Signal Activities
7	68. (U) I am advised that this lawsuit also puts at issue allegations concerning
8	whether the NSA has acquired large quantities of communication records. Confirmation or
9	denial of any information concerning these particular allegations, however, will cause
0	exceptionally grave damage to the national security.
.1	69. (TS#SI- #OC/NF) As noted above, starting in October 2001, and now
2	pursuant to the FISC Pen Register Order,
3	
ا 14	
5	
16	
17	pursuant to the FISC Telephone Records Order,
18	
9	Disclosure of the NSA's meta
20	data collection activities, either before or after FISC authorization, would cause exceptionally
21	grave harm to national security.
22	70. (TS//SI-WOC/NF) In particular, the bulk collection of Internet and
23	telephony meta data allows the NSA to use critical and unique analytical capabilities to track the
24	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	-TOP SECRET//COMINT



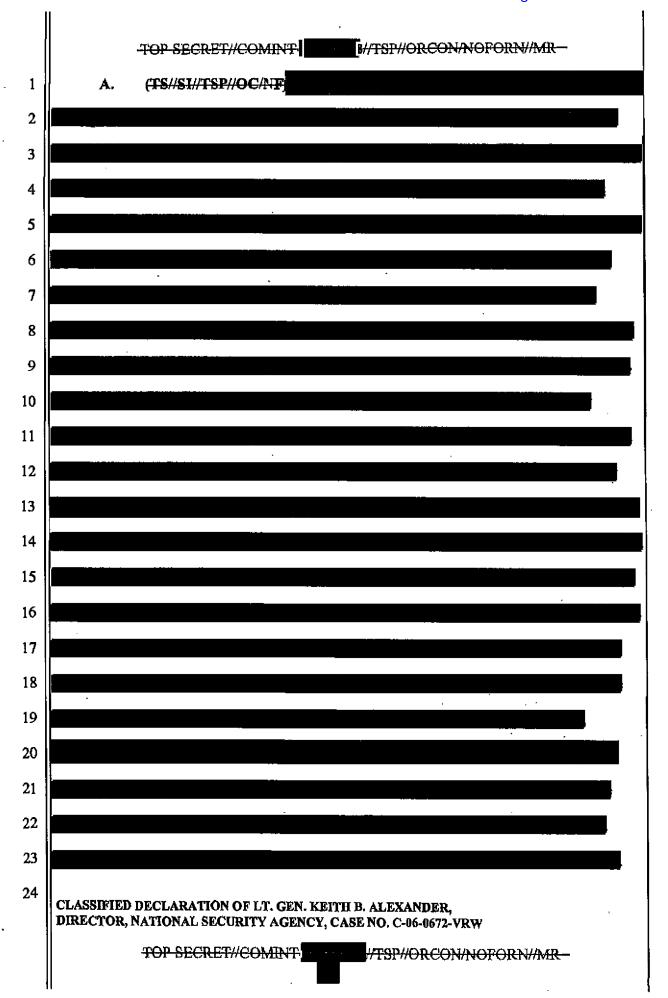
	+ FOP SECRET#COMENT # TEP#ON.COMMERCIRMAMIL
1	
2	· · · · · · · · · · · · · · · · · · ·
3	
4	
5	
6	
7	
8 9	
9 10	
11	·
12	
13	73. (TS//SI//TSP//OC//NF) The capability provided by meta data analysis may be
14	illustrated by an example of when this tool was not utilized. According to the 9/11 Commission
15	report, when Khalid al-Mihdhar, one of the 9/11 hijackers, was in the United States from January
16	2000 to June 2001, he telephoned the home of his wife's family in Yemen. The phone number
17	for this home in Yemen had well-established terrorist connections ²² and was being targeted by
18	the NSA through an overseas collection process that did not have the capability to obtain meta
19	data to help identify the location of incoming calls. At the time, there was no FISA collection on
20	this number, and neither the TSP program, under which the NSA targeted one-end foreign calls
21	The second second and the program, and of which the NBA targeted one-cha foreign cans
22	(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-ladened vehicle at the last minute.
24	,
	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	TOP SECRET//COMINT

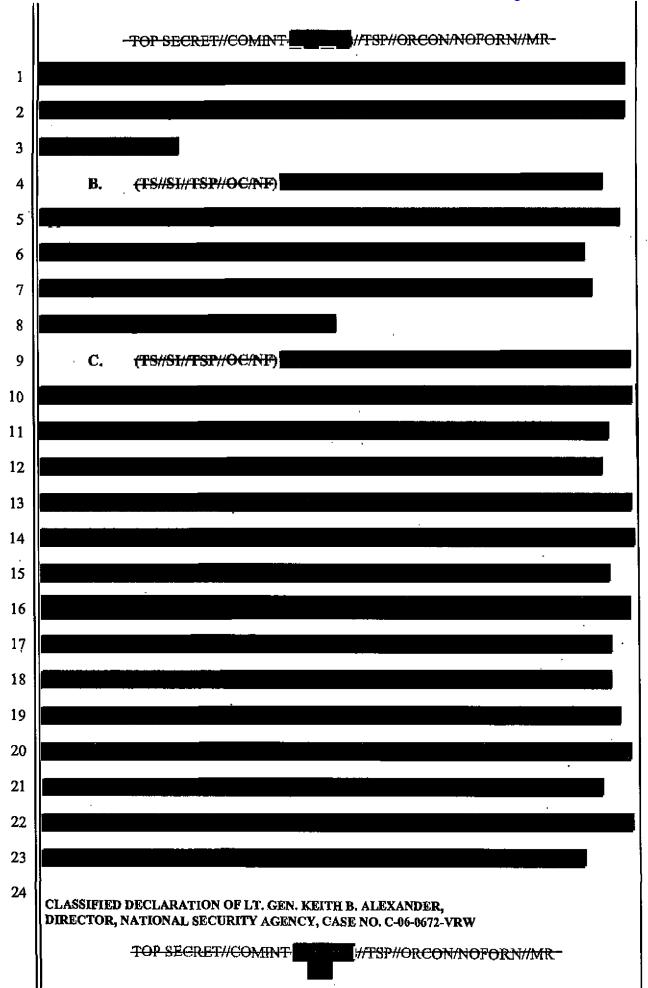
"FOP SECKET//COMIN'F MTTP//ORCON/NOPOHN/IMR 1 into the United States, nor collection of bulk meta data that would have allowed analysis of this 2 number to ascertain other contact numbers, were in place. Had the Yemeni phone number been 3 targeted using the TSP and were meta data analysis available, we should have been able to 4 identify that al-Mihdhar was in the United States when he called the number in Yemen, which 5 would have provided leads to investigate the matter further. Indeed, the 9/11 Commission report 6 noted that if the FBI had known that al Mihdhar was in the United States, "investigations or 7 interrogation of [al Mihdhar], and investigation of [his] travel and financial activities could have 8 yielded evidence of connections to other participants in the 9/11 plot. The simple fact of [his] 9 detention could have derailed the plan. In any case, the opportunity did not arise." Final Report 10 of the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission 11 Report") at 272. While there is an element of hindsight to this example, and perhaps other 12 actions could have detected al Mihdhar, the existence of the TSP and meta data activities would 13 have provided a highly significant tool that may have proved valuable in detecting the 9/11 plot. 14 74. (TS//SL//TSP//OC/NF) Based on my experience as Director of the NSA, I believe 15 that the meta data collection activities authorized by the President after 9/11 and subsequently 16 authorized by the FISC are among the most important intelligence tools available to the United 17 States for protecting the Homeland from another catastrophic terrorist attack. In my view, the 18 NSA could not have obtained certain critical intelligence in any other way. These NSA activities 19 have given the United States unparalleled ability to understand 20 If employed on a sufficient volume of raw data, contact 21 chaining can expose and contacts that were 22 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 23

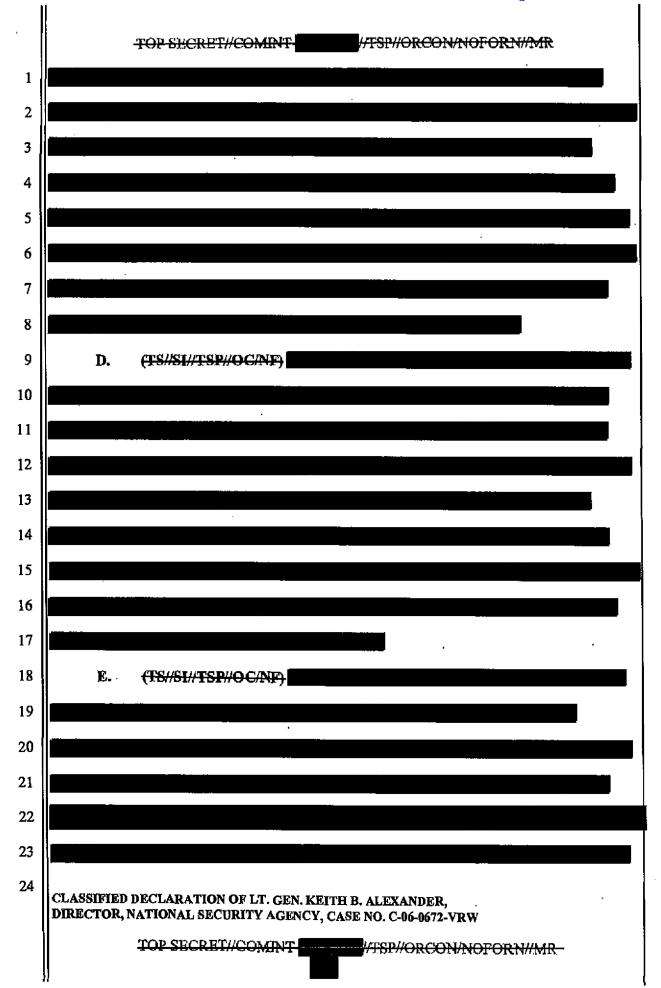
CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW

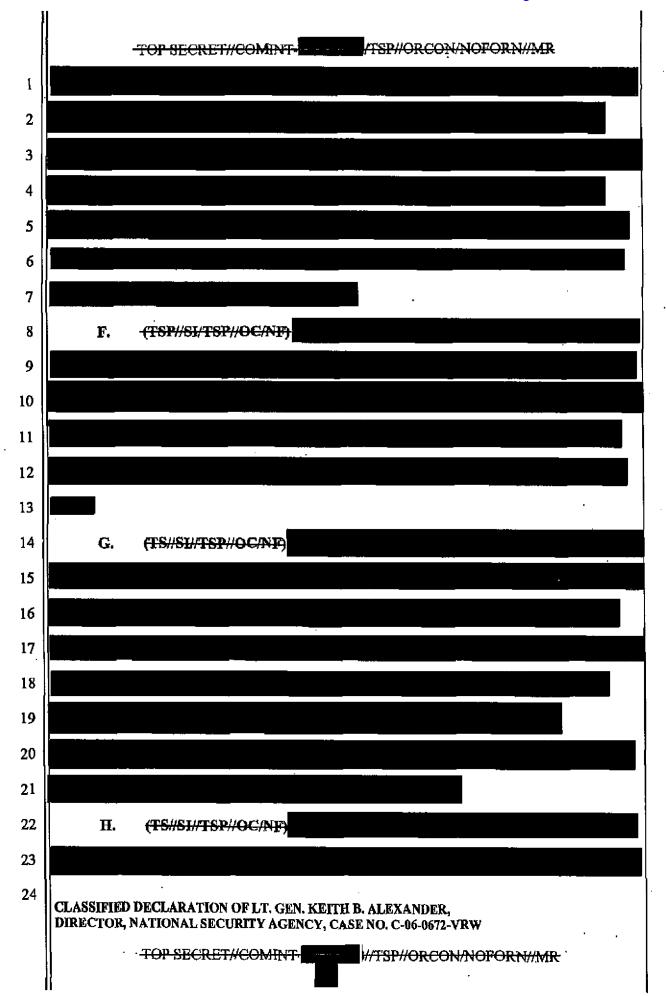
24

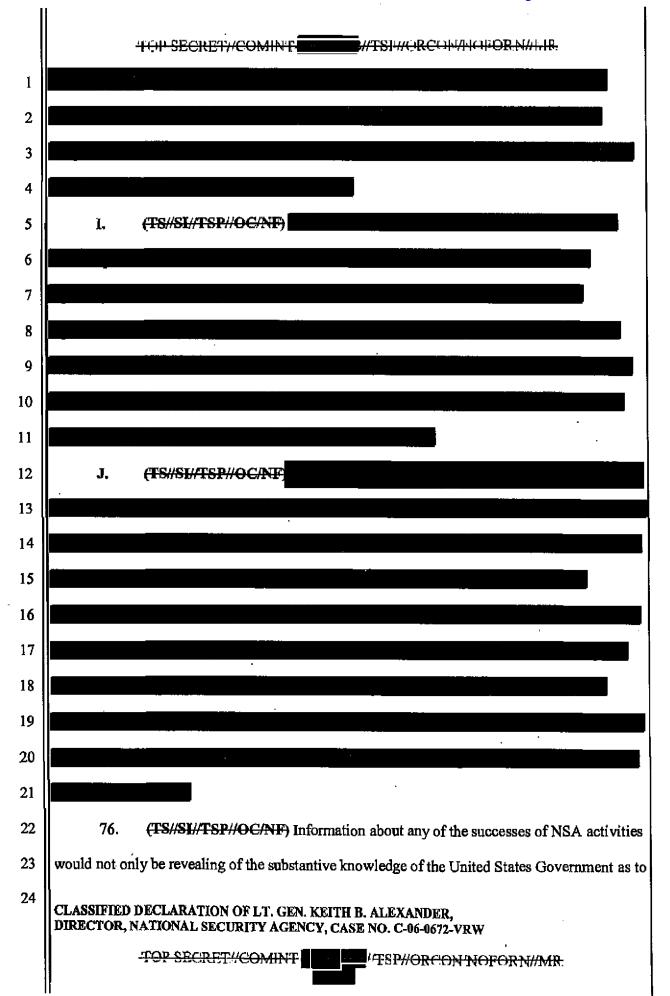
	"FOP HECKET//COMIN'S " "FIST-HORCOM/NHOPORN/WHX-
1	amount of other information that has no intelligence value whatsoever—in colloquial terms, to
2	find at least some of the needles hidden in the haystack.
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	Disclosure or confirmation of the NSA's bulk collection and targeted analysis of telephony meta
14	data would confirm to all of our foreign adversaries the
15	existence of these critical intelligence capabilities and thereby severely undermine NSA's ability
16	to gather information concerning terrorist connections.
17	3. (TS//SI//TSP//OC/NF) Information Demonstrating the Success of the TSP and Meta Data Activities.
18	
19	75. (TS//SI//TSP//OC/NF) Specific examples of how the TSP, in conjunction with
20	meta data analysis, led to the development by the NSA of actionable intelligence and important
21	counter-terrorism efforts help illustrate the effectiveness and need for the program, but could not
22	be disclosed without revealing specific NSA intelligence information, sources, and methods. For
23	example:
24	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER,
	DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	TOP SECRET//COMINT //TSP//ORCON/NOFORN//MR
ļ	











CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW

	·
	*FOR HECRET//EOMINT
1	The Order also provides that a telephone number believed to be used by a U.S.
2	person shall not be regarded as associated with
3	solely on the basis of activities that are protected by the First Amendment. The FISC Pen
4	Register Order authorizes the use of a pen register and trap and trace device to collect Internet
5	meta data on similar terms. Disclosure of these facts would reveal
6	sensitive sources and methods utilized by the NSA to obtain data utilized to track
7	and contacts of
8	79. (TS//SI//OC//NF) The intelligence activities authorized by the FISC Pen Register
9	and FISC Telephone Records Orders must not be compromised by the disclosure of other
10	information. For example, as discussed above, the disclosure of
11	
12	
13	
14	Thus, any attempt to address the lawfulness of the meta data activities under
15	Presidential authorization prior to the FISC orders could not disclose, or risk disclosure of,
16	current NSA operations under FISC Orders.
17	
18	
19	23 (TS//SI-WOC//NF) For this reason, the FISC Telephone Records Order and
20	FISC Pen Register Orders prohibit any person, to any other person that the NSA has sought or obtained the telephony meta data, other than to
21	(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
22	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
23	Order is directed in the same manner as such person.
24	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	TOP SECRET//COMINT TO TESP//ORCONOLOGORN//MP

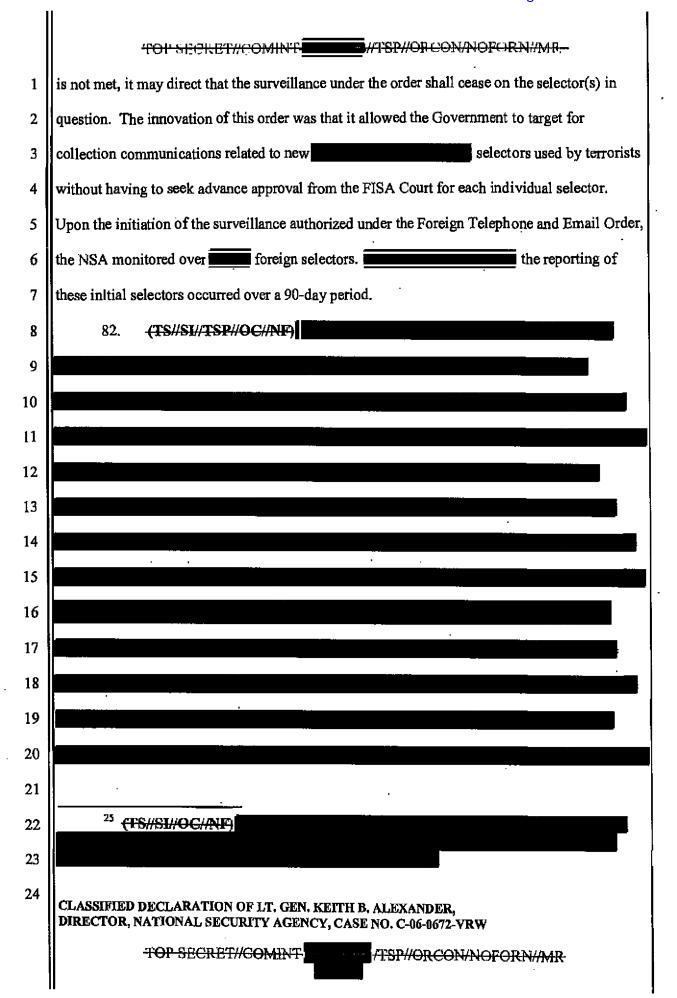
80.	(TS//SI//OC//NF)	The disclosure of inf	ormation concerning	the recent FISC
Orders authori	zing electronic surv	eillance would also h	arm national securit	y. The January 10,
2007 Foreign	relephone and Emai	1 Order authorized, a	mong other things,	electronic surveillance
of telephone ar	nd Internet commun	ications		when the
Government de	etermines that there	is probable cause to	believe that (1) one	of the communicants
is a member or	agent		an	d (2) the
communication	n is to or from a fore	eign country, i.e., a o	ne-end foreign com	nunication to or from
the United Sta	tes. ²⁴ The telephone	numbers and email	addresses to be targe	eted (i.e., "selectors")
under this orde	er were further limit	ed to those that the N	SA reasonably belie	eves are being used by
persons outsid	e the United States.	Under the order, eve	ery 30 days the Gove	ernment is required to
submit a repor	t to the FISA Court	listing new selectors	that the NSA has tar	rgeted during the
previous 30 da	ys and briefly sumn	narizing the basis for	the NSA's determin	nation that the
probable cause	standard has been i	net.	•	•

81. (TS://SI:/OC:/NF) The surveillance under this new FISA Court Foreign
Telephone and Email Order, which is subject to detailed minimization and oversight procedures,
was authorized for 90 days and indicated that it may be reauthorized by the FISA Court upon
application by the Attorney General. The order states that, with each request for reauthorization,
the Government is required to present a list of current selectors previously reported to the FISA
Court that the Government intends to continue to task for collection under the reauthorization.
The order further indicated that, at any time, the FISA Court may request additional information
regarding particular selectors, and, if the Court finds that the applicable probable cause standard

That fact, which is not relevant to this action, is, like the other details in the orders, highly classified.

CLASSIFIED DECLARATION OF LT. GEN. KETTH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW

^{24 (}TS//SI/TSP//OC//NF)



TOP SECRET//COMIN'P ##FSP#ORCOM/MCPOKN//MR 1 ⁶ While the general existence of the January 2007 orders, 2 as described publicly by the Attorney General, is not classified, the number, nature, and contents 3 of the specific orders described herein are highly classified. Among other things, disclosing to 4 5 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 б 7 to alter its communications to evade detection. 8 83. the Government filed applications (TS//SI//OC/NF) 9 with the FISA Court to renew for 90 days the surveillance authority granted by the FISA Court's 10 January 10 orders. These applications were considered by a different FISA Court Judge based 11 on the FISA Court's typical assignment practice. By order the FISA Court 12 13 14 The Court, however, did not grant the Government's application to renew the 15 surveillance authority in the Foreign Telephone and Email Order (concerning surveillance 16 targeting telephone numbers and e-mail addresses reasonably believed to be used by persons 17 outside the United States). Rather, it issued an Order and Memorandum opinion on April 3, 18 2007, declining to adopt the interpretation of the Foreign Intelligence Surveillance Act 19 underlying the Government's application for the Foreign Telephone and Email Order. The Court 20 (TS//SI//OC//NF) 21 22 23 it plans to do so by a process in which it will obtain authorization of the FISA Court for each individual selector. 24 CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW TOP SECRET/COMINT-//TSP//ORCON/NOFORN//MR

TOP SECRET//COMINT #/TSP//ORCON/NOFORN//MR

nevertheless ordered that the Government could submit an application for a single extension of the Foreign Telephone and Email Order to May 31, 2007. The Court contemplated that an extension of surveillance authority to May 31 would allow the Government to submit an application that might permit the Court "to authorize at least part of the [requested] surveillance in a manner consistent with [its] order and opinion." On the Government's application, the Court granted a separate order issued on April 5, 2007, extending the surveillance authority granted by the Foreign Telephone and Email Order to May 31, 2007.

84. (TS//SI//OC//NF) The Government is reviewing the new FISA Court orders and intends to work with the FISA Court in the hopes of developing an approach for continuing the authorized surveillance beyond May 31, 2007, in a manner consistent with the April 3, 2007, order of the FISA Court. The details of these orders, and targets implicated by the orders, like the operational details and targets of the ongoing FISA Court-approved surveillance, are highly classified. Thus, information about the nature of these recent FISC orders should not be disclosed in this case.

18

23

24

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-YRW

TOP SECRET//COMINT- //TSP//ORCON/NOFORN//MR

VII. (U) Risks of Allowing Litigation to Proceed

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. This case directly implicates the conduct of highly classified NSA intelligence activities. Those activities are not peripheral to the case: they are the very subject of this lawsuit. In my judgment, any effort to probe the outer-bounds of classified information, would pose inherent and significant risks of the disclosure of classified information,

86. (TS//SI-WOC/NF) Indeed, any effort merely to allude to those facts in a non-classified fashion could be revealing of classified details that should not be disclosed. As noted, even seemingly minor or innocuous facts, in the context of this case or other non-classified information, can tend to reveal, particularly to sophisticated foreign adversaries, a of U.S. intelligence gathering sources and methods.

VIII. (U) Summary and Conclusion

88. (TS//SI//NF) The United States has an overwhelming interest in detecting and thwarting further mass casualty attacks by al Qaeda. The United States has already suffered one attack that killed thousands, disrupted the Nation's financial center for days, and successfully

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW

TOP SECRET//COMINT

TSP/ORCON/NOFORN/MR

TOP SECRET//COMINT-

//TSP//ORCON/NOFORN//MR

struck at the command and control center for the Nation's military. Al Qaeda continues to possess the ability and clear, stated intent to carry out a massive attack in the United States that could result in a significant loss of life, as well as have a devastating impact on the U.S. economy. According to the most recent intelligence analysis, attacking the U.S. Homeland remains one of al Qaeda's top operational priorities, see In Camera Declaration of Michael McConnell, DNI, and al Qaeda will keep trying for high-impact attacks as long as its central command structure is functioning and affiliated groups are capable of furthering its interests.

- 89. (TS//SI//NF) Al Qaeda seeks to use our own communications infrastructure against us as they secretly attempt to infiltrate agents into the United States, waiting to attack at a time of their choosing. One of the greatest challenges the United States confronts in the ongoing effort to prevent another catastrophic terrorist attack against the Homeland is the critical need to gather intelligence quickly and effectively. Time is of the essence in preventing terrorist attacks, and the government faces significant obstacles in finding and tracking agents of al Qaeda as they manipulate modern technology in an attempt to communicate while remaining undetected. The NSA activities described herein are vital tools in this effort.
- 90. (TS//SI//NF) For the foregoing reasons, in my judgment the disclosure of the information at issue in this lawsuit would cause exceptionally grave damage to the national security of the United States. In addition to upholding the state secrets privilege and statutory privilege assertions by the Director of National Intelligence in this case, I request that the Court also uphold my assertion of NSA's statutory privilege to protect information about NSA activities. Finally, it is my view that continued litigation of this lawsuit, which directly puts at issue highly classified NSA intelligence activities

would risk the disclosure of sensitive classified information and.

CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW

- 1	
	TOP SECRET//COMINT
1	accordingly, that the Court should not only protect from disclosure the classified information
2	described herein but dismiss this lawsuit.
3	
4	
5	
6	
7	I declare under penalty of perjury that the foregoing is true and correct.
8	
9	DATE: 20 APR 07 & Soffel
10	LT. GEN. KEITH B. ALEXANDER
1	Director, National Security Agency
12	
13	
4	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
	CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY, CASE NO. C-06-0672-VRW
	TOP SUCH ETWOOD OF THE