

	,	では、大人・大人・大人・大人・「大人・「人)」。
2		
3		(U) Table of Contents
4	1.	(U) Introduction
5	II.	(U) Summary
6	111.	(U) Classification of Declaration
7	IV.	(U) Background Information
8 9 10		 A. (U) The National Security Agency B. (U) September 11, 2001 and the al-Qaeda Threat C. (U) Summary of NSA Activities After 9/11 to Meet al-Qaeda Threat
ti	V.	(U) Information Protected by Privilege
12	VI.	(U) Description of Information Subject to Privilege and the Harm of Disclosure
13		A. (U) Information That May Tend to Confirm or Deny Whether the Plaintiffs Rave Been Subject to Any Alleged NSA Activities
15		B. (U) Information Related to NSA Activities, Sources, or Methods implicated by the Plaintiffs' Allegations and the Harm to National Security of Disclosure
17		1. (U) Plaintiffs' Allegations of a Communications Dragnet
18		(a) (U) Information Related to the Terrorist Surveillance Program
10		(b) (U) Other Classified Information Concerning NSA Activities
20		(c) (SHSHINF) Technical Details of Analytic Capabilities
21 22 23		2. (TS://SI//OC/NF) Information Concerning Current FISA Authorized Activities and Specific FISC Orders
24		 (U) Plaintiffs' Allegations that Telecommunications Companies have Assisted the NSA with the Alleged Activities
25	VII.	(U) Risks of Allowing Litigation to Proceed
26 27 28	У ЛЦ.	(U) Conclusion
40		d In Comera, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Shubert, et al. v. United States of America et al. (No. 07-ev-693-VRW; MOL No. 06-1791)
		MACTON MCCONC

TOP SECRET TSP CONTIST

2.

 $-\Theta RCONNCHORN$

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

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

I. (U) Introduction

- 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 (Apr. 17, 1995), as amended by Executive Order No. 13292, 68 Fed. Reg. 15315 (Mar. 25, 2003) (reprinted in 3 C.F.R. 2003 Comp. at 196 and at 50 U.S.C.A. § 435 (Supp. 2009)), 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 have been advised of this litigation and the allegations in the plaintiffs' Amended Complaint. As described herein, various classified facts related to the plaintiffs' claims are subject to the DNI's state secrets privilege assertion. The disclosure of information discussed throughout this declaration, which relates to NSA intelligence information, activities, sources, methods, and relationships, reasonably could be expected to cause exceptionally grave damage to the national security of the United States. In addition, it is my judgment that sensitive state secrets are so

Classified In Camera, Ex Parie Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shuberi, et al. v. United States of America, et al. (No. 07-cv-693-VRW; MDL No. 06-1791)

MARCONNOFORN

Ġ

11 12

13

10

14 15

16

17 18

> 19 20

21 22

23 24

25 26 27

28

HOP SECRET THE COMPLE

central to the subject matter of the hitigation that any attempt to proceed in the case risks the disclosure of the secrets described herein and exceptionally grave damage to the national security of the United States. Through this declaration, I also hereby invoke and assert the NSA's statutory privilege set forth in section 6 of the National Security Agency Act of 1959, Public Law No. 86-36 (codified as a note to 50 U.S.C. § 402) ("NSA Act"), to protect the information related to NSA activities described below. The statements made herein are based on my personal knowledge of NSA activities and operations, and on information available to me as Director of the NSA.

IL (U) Summary

3. (U) I have reviewed the Amended Complaint in this case. Plaintiffs allege, in sum, that, after the 9/11 attacks, the NSA received presidential authorization to engage in surveillance activities far broader than the publicly acknowledged "Terrorist Surveillance Program" ("TSP"), which was limited to the interception of specific international communications involving persons reasonably believed to be associated with all Qaeda and affiliated terrorist organizations. Plaintiffs allege that the NSA, with the assistance of telecommunications companies, Amended Compl. 1 5-8, conducts a "dragnet" surveillance program involving the interception of "virtually every telephone, internet and/or email communication that has been sent from or received within the United States since 2001" as part of an alleged Presidentially-authorized "program" after 9/11, id. ¶¶ 1, 4. I cannot disclose on the public record the nature of any NSA information implicated by the plaintiffs' allegations. However, as described further below, the disclosure of information related to the NSA's activities, sources and methods implicated by the plaintiffs' allegations reasonably could be expected to cause exceptionally grave damage to the national security of the United States and,

Classified In Cumera, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shuhert, et al. v. United States of America, et al. (No. 07-cv-697-VRW, MDL No. 06-1791)

ŦŎ₽ŸĠĊŖĿŦŸŶŖĸĊĸ**Ŋ**ĦŶŦĸ

᠉ᡃᢕᠺ᠊ᢗ᠊ᡠ᠈ᢦᢇᡧᡝᡰᢕᠺᡮ

₹€シᡰヘ╌ᠺᡛ*ᢗ᠅ᠺ*ᡶ᠋ᠮ᠁ᡛᢝᡟᠵᢇᠸᡤᢇᠫᡳᡰᡛ╲╴ᠮ

()(()()()()()()

for this reason, are encompassed by the DNI's state secrets and statutory privilege assertions, as well as by my own statutory privilege assertion, and should be protected from disclosure in this case. In addition, it is my judgment that sensitive state secrets are so central to the subject matter of the litigation that any attempt to proceed in the case risks the disclosure of the classified privileged national security information described herein and exceptionally grave damage to the national security of the United States.

4. (PS://TSP//ST://OC/NF) The allegations in this lawsuit put at issue the disclosure of information concerning several highly classified and critically important NSA intelligence activities that commenced after the 9/11 terrorist attacks, but which are now being conducted pursuant to authority of the Foreign Intelligence Surveillance Act ("FJSA"), including ongoing activities conducted under orders approved by the Foreign Intelligence Surveillance Court ("FJSC"). Plaintiffs' allegation that the NSA undertakes indiscriminate surveillance of the content of millions of communications sent or received by people inside the United States — under the now defunct-TSP or otherwise — is false, as discussed below. Likewise, the plaintiffs' allegations that telecommunications companies assisted with the alleged dragnet program are false, because the alleged dragnet does not exist. The NSA's collection of the content of communications under the TSP was directed at international communications in which a participant was reasonably believed to be associated with al Qaeda or an affiliated organization and did not constitute the kind of dragnet collection of the content of millions of Americans' telephone or Internet communications that the plaintiffs allege. Although the existence of the TSP has been acknowledged, the details of that program remain highly classified, along with

Classified In Camera, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shuberi, et al., v. United States of America, et al. (No. 07-cv-693-VRW, MDL No. 06-1791)

TOP SECREF TSP-COMERC

ᢊᠫᠺ᠅ᡳᢕ

S

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

. Because the allegations in the complaint reference activities further references to the FISC Orders will focus solely on activities under the orders directed at

Classified In Camero, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency V. rginia Shirbert, et al. v. United Sintex of America, et al. (No. 07-cv-693-VRW, MDL No. 06-1791)

TOP SECRET: TSP/COMINT

#ORCON/NOFORN

6

٤

2

8 10

12 13

14

15

11

ļ٥ 17

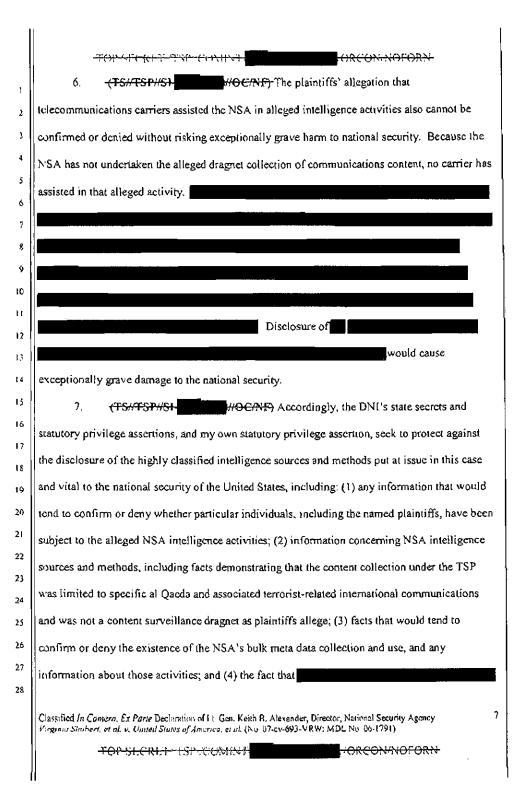
ΙŖ

19 20

> 21 22 23

24 25

> 26 27



п

12

13

14

16

17

18

19 20

21

22

2.

24 25 26

27 28 <u> चित्रा है । त्राप्त प्रकार किल्ला किल्ला</u>

about alleged NSA activities does not diminish the need to protect intelligence sources and methods from further exposure. Official confirmation and disclosure of the classified privileged national security information described herein would cause exceptionally grave damage to the national security. For these reasons, as set forth further below, I request that the Court uphold the state secrets and statutory privilege assertions that the DNI and I now make, and protect the information described in this declaration from disclosure.

III. (U) Classification of Declaration

8. (9//SV/NF) This declaration is classified TOP SECRET//TSP//SI

by Executive Order No. 13292. Under Executive Order No. 12958, information is classified "TOP SECRET" if unauthorized disclosure of the information 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 expected to cause serious damage to national security; and "CONFIDENTIAL" if unauthorized disclosure of the information reasonably could be 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.

I

(SAANTE)

Classified In Cumern, Ex Paric Declaration of Lt. Gen, Keith B. Alexander, Director, National Security Agency Pergina Student, et al. v. United States of America, et al. (No. 07-cv-693-VRW; MDL No. 06-1791)

FOM SECRETATION OCOMINAL

\ORCO\\N\OFORN

TOP SECRET 13P COMME ᠆ᢕᡑᢚᢕ᠅᠅ᢕᢪᢙᠰ 9. (SHSHINF) Additionally, this declaration also contains Sensitive Compartmented Information (SCI), which is "information that not only is classified for national security reasons 2 3 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 b information, these safeguards and access requirements exceed the access standards that are normally required for information of the same classification level. Specifically, this declaration ٤ 9 references communications intelligence (COMINT), also referred to as special intelligence (SI), 10 which is a subcategory of SCI. COMINT or SI identifies SCI that was derived from exploiting H. cryptographic systems or other protected sources by applying methods or techniques, or from 12 intercepted foreign communications. 13 #OC/NF) This declaration also contains information (TS!/TSP://SI-14 15 related to or derived from the TSP, a prior controlled access signals intelligence program that 16 operated under presidential authorization in response to the attacks of September 11, 2001, until 17 January 2007. Although the TSP was publicly acknowledged by then-President Bush in 18 December 2005, details about the program remain highly classified and strictly compartmented. 19 20 Information pertaining to this program is denoted with the special marking "TSP" and requires 2١ more restrictive handling. 22 2. 24 25 26 27 28 Classified In Camera, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shubert, et al. v. United States of America, et al. (No. 87-cv-693-VRW; MDL No. 66-1793) TOP SECRETOTSPACEMINT- ᠘᠘᠘ᢕ᠘᠘

·forsecrement contain

LIRECTIC VEHICLES (TS#SWAYF) Signals intelligence (SIGINT) consists of three subcategories: (1) communications intelligence (COMINT); (2) electronic intelligence (ELINT); and (3) foreign 2 instrumentation signals intelligence (FISINT). Communications intelligence (COMINT) is 3 ı defined as "all procedures and methods used in the interception of communications and the ŝ obtaining of information from such communications by other than the intended recipients." 18 6 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 ሄ 4 conveyed via a number of means 10 . Electronic intelligence (ELINT) is technical intelligence information derived from foreign non-communications electromagnetic radiations except atomic detonation or radioactive 12 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 15 signals intelligence (FISINT) is derived from non-U.S. aerospace surfaces and subsurface 16 systems which may have either military or civilian applications. 17 (U) The NSA's SIGINT responsibilities include establishing and operating an 18 effective unified organization to conduct SIGINT activities set forth in E.O. No. 12333, 19 20 § 1.12(b), as amended. In performing its SIGINT mission, NSA has developed a sophisticated worldwide SIGINT collection network. The technological infrastructure that supports the NSA's 22 foreign intelligence information collection network has taken years to develop at a cost of 23 billions of dollars and untold human effort. It relies on sophisticated collection and processing 24 technology. 26 signals intelligence information for foreign intelligence and counterintelligence purposes to

Classified In Camero, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency

linginia Shubert, et al. v. United States of America, et al. (No. 07-ev-693-VRW, MDL No. 06-1791)

11

;;ORCOX:NOFORN

?

11

10

21

25

27

28

support national and departmental missions."

TOP SECRETATSPACOMINA

THE STURET THE CONTROL

f 2

- 15. (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 and in support of military operations. The second reason is to obtain information necessary to the formulation of U.S. foreign policy. Foreign intelligence information provided by the NSA is thus relevant to a wide range of important issues, including military order of battle; threat warnings and readiness; arms proliferation; international terrorism; counter-intelligence; and foreign aspects of international narcotics trafficking.
- 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, 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."

Classified In Camera, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shubert, et al. v. United States of America, et al. (No. 07-cv-693-VRW, MDL No. 06-1791)

TOP SECRETATION COMIN'S

+ORCONNOFORN

THE STERFT ISP CONTICH

2

4

5

6

7

8

ŝù

п

12

13

{4 15

16

17

18

19 20

21

22

23

24

25 26

27

28

~196~(-)~~\(-)-(-)R/~

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

(U) On September 11, 2001, the al Qaeda terrorist network launched a set of £7. 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 jettiners, which they deliberately flew into the Twin Towers of the World Trade Center. Al Queda targeted the headquarters of the Nation's Armed Forces, the Pentagon, with the third jetliner. Al Qacda 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 !! resulted in approximately 3,000 deaths the highest single-day death toll from hostile foreign attacks in the Nation's history. In addition, these attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars of damage to the economy.

18. (U) On September 14, 2001, a national emergency was declared "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." Presidential Proclamation No. 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001). The United States also immediately began plans for a military response directed at al Qaeda's training grounds and havens in Afghanistan. On September 14, 2001, both Houses of Congress passed a Joint Resolution authorizing the President of the United States "to use all necessary and appropriate

Classified In Camera, Ex Parte Declaration of Lt. Gen. Kenh B. Alexander, Director, National Security Agency Laginia Student et al. v. United States of America, et al. (No. 07-ex-693-VRW, MDL No. 06-1791)

TOP SECRETATOR COMINT

ᡤ᠀ᠺᡤ᠙ᠫ᠅ᡳᢙᡏ᠐ᠺᠰ

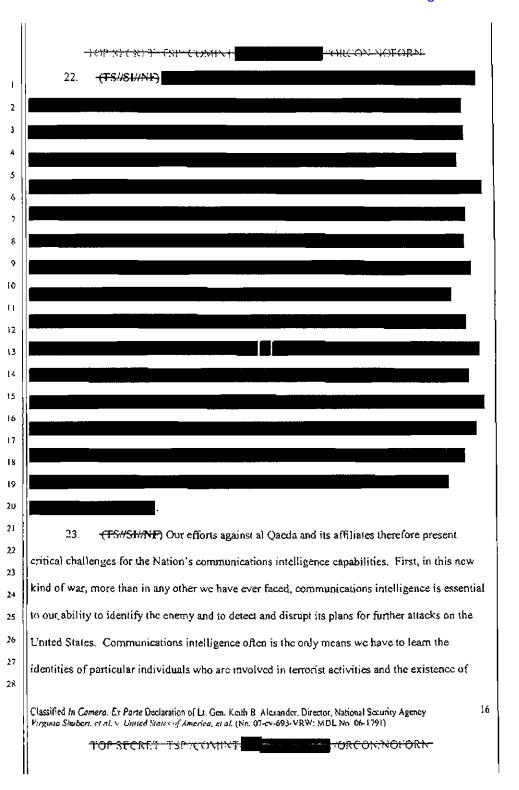
force against those nations, organizations, or persons he determines planned, authorized. committed, or aided the terrorist attacks" of September 11. Authorization for Use of Military Force, Pub. L. No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept. 18, 2001). Congress also expressly acknowledged that the 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.

- 19. (U) Also after the 9/11 attacks, a Military Order was issued stating that the attacks of September 11 "created a state of armed conflict," see Military Order by the President § 1(a), 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001), and that all Qaeda terrorists "possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the United States. Government," and concluding that "an extraordinary emergency exists for national defense purposes," id. § 1(c), (g), 66 Fed. Reg. at 57833-34. Indeed, shortly after the attacks, NATO took the unprecedented step of invoking article 5 of the North Atlantic Treaty, which provides that an "armed attack against one or more of [the parties] shall be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246.
- 20. (U) As a result of the unprecedented attacks of September 11, 2001, the United 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 affice is a very

Classified In Camera, Ex Parte Deciaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Simbert, et al. v. United States of America, et al. (No. 07-ev-693-VRW, MDL No. 06-1791)

TOP SECRETOISP COMPAN

⅌℮K℮℮ℎ℀℮



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.

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

-1()|-5,|-5,|-5,|-1-7,|-6,|-6,|-5,|-

- 24. (U) After the September 11 attacks, the NSA received presidential authorization and direction to detect and prevent further terrorist attacks within the United States by intercepting the content? of communications for which there were reasonable grounds to helieve that (1) such communications originated or terminated outside the United States and (2) a party to such communication was a member or agent of al Qaeda or an affiliated terrorist organization. The existence of this activity was disclosed by then-President Bush in December 2005 (and subsequently referred to as the "Terrorist Surveillance Program" or "TSP").8
- 25. (FS//FSP//SL//QC/NF) In more specific and classified terms, the NSA has utilized a number of critically important intelligence sources and methods to meet the threat of another mass casualty terrorist attack on the United States methods that were designed to work

Ciassified In Comera, Ex Parto Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Perginin Shubert, et al. v. United States of America, et al. (No. 07-cv-693-VRW; MDL No. 06-1791)

TOP SECRET I SPECEDMINA

HOREON/NOFORN

⁷ (U) The term "content" is used in this Declaration to refer to the substance, meaning, or purport of a communication, as defined in 18 U.S.C. § 2510(8).

^{8 (}U) On January 17, 2007, the Government made public the general facts that new orders of the Foreign Intelligence Surveillance Court had been issued that authorized the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Queda or an associated terrorist organization; that, as a result of these orders, any electronic surveillance that had been occurring as part of the TSP was then being conducted subject to the approval of the FISA Court; and that, under these circumstances, the TSP was not reauthorized.

2 3

5

6

8

9

10

11

12

13 14

15

20

21

22

23

24

25

26 27 28

in tandem and continue to this day under authority of the FISA. As noted above, one such method involved the program publicly acknowledged by then-President Bush as the TSP, in which the NSA intercepted the content of telephone and Internet communications pursuant to presidential authorization 9 As described further below, under the TSP, NSA did not engage in plaintiffs' alleged dragnet surveillance of communication content, but intercepted the content of particular communications where reasonable grounds existed to believe one party involved a member or agent of al Qaeda or affiliated terrorist organization based on particular "selectors" (phone numbers or Internet addresses) associated with that target. In addition to collecting the content of particular communications, the NSA has also collected non-content communication information known as "meta data." Specifically, after the 9/11 attacks, the NSA collected bulk meta data related to telephony communications for the purpose of conducting targeted analysis to track al Qaeda-related networks. Telephony meta data is information derived from call detail records that reflect non-content information such as, but not limited to, the date, time, and

⁹ (TS//TSP//SI- #OCANT) The first presidential authorization of the TSP was on October 4, 2001, and the TSP was reauthorized approximately every 30-60 days throughout the existence of the program. The documents authorizing the TSP also contained the authorizations for the meta data activities described herein. The authorizations, moreover, evolved over time, and during certain periods authorized other activities (this Declaration is not intended to and does not fully describe the authorizations and the differences in those authorizations over time).

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

Classified In Camera, Fr Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shubert, et al. v. United States of America, et al. (No. 07-cv-893-VRW; MDI. No. 06-1791)

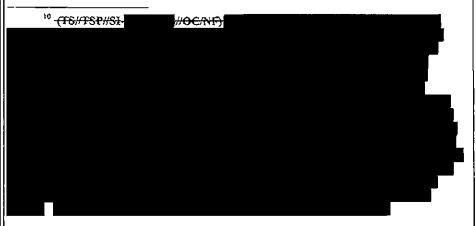
TOP SECRETATION COMMITS

Tent strike to the strike to

duration of telephone calls, as well as the phone numbers used to place and receive the calls. ¹⁰ In addition, since the 9/11 attacks, the NSA has collected bulk meta data related to *Internet* communications. Internet meta data is header/router/addressing information, such as the "to," "from," "ce," and "bee" lines, as opposed to the body or "re" lines, of a standard email.

- ()R(()N, N()] ()RN

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



11 (TS//SI//OC/NF) As also described further, see infra ¶ 63-66, the FISC extended these orders with some modifications. What is described below as the Foreign Telephone and Email Order expired in August 2007 and was supplanted by authority enacted by Congress – first under the Protect America Act and then the FISA Amendments Act of 2008 – to authorize

C assisted In Camera, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency V refine Student, et al. v. United States of America, et al. (No. 07-ov-693-VRW; MDL No. 06-1791)

ᢊᢒᠺ᠅ᢊᢒ᠀ᢋ᠐ᢢ

3

4

5

7

8

10

п

12

13

14 15 16

17

18

19

20

21

22

23

24

25

26

27

since May 2006 certain telecommunication providers have been required by an order of the FISC to produce to the NSA on a daily basis all telephony meta data that they create ("FISC Telephone Business Records Order") The FISC Telephone Business Records Order has been reauthorized approximately every 90 days since it was first issued. Although this collection is broad in scope, the NSA was authorized by the FISC to query the archived telephony data with identified telephone numbers for which there are facts giving rise to a reasonable, articulable suspicion that the number is associated with (hereafter referred to as a "RAS" determination). Historically, only a tiny fraction of telephony meta data records collected by the NSA has actually been presented to a trained professional for analysis. As discussed further below, see infra ¶ 48-56, while the vast majority of records are thus never viewed by a human at the NSA, it is still necessary to collect the meta data in bulk in order to

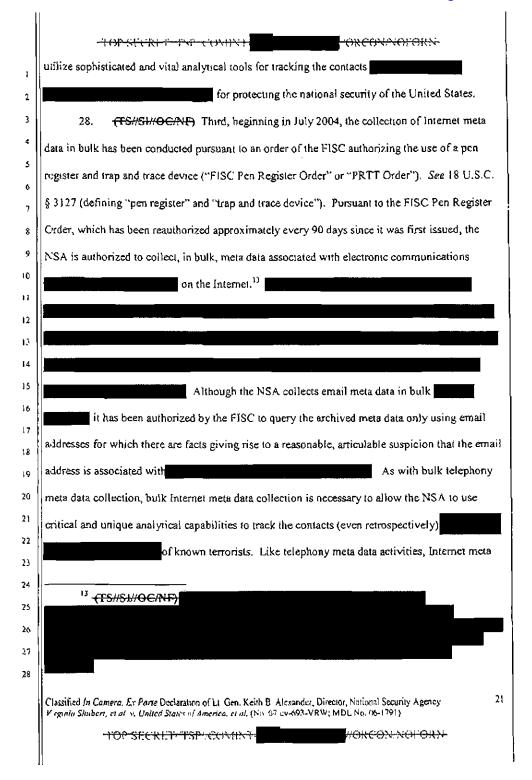
foreign intelligence surveillance of targets located overseas without individual court orders.

12 (TSHSH/OC/NF) As set forth further below, see infra \$\ 00-62, NSA's compliance with this limitation in the FISC Order has been subject to further proceedings in the FISC that commenced with a compliance report by the government on January 15, 2009, which indicated that the NSA had also been querying incoming telephony meta data with selectors for counterterrorism targets subject to NSA surveillance under Executive Order 12333, as to which the NSA had not made a "RAS" determination. On March 2, 2009, the FISC renewed the Order authorizing the bulk provision to NSA of business records containing telephony meta data from telecommunications carriers, but subjected that activity to new limitations, including that the NSA may overy the meta data only after a motion is granted on a case-by-case basis (unless otherwise necessary to protect against imminent threat to human life). The FISC also required the Government to report to the FISC on its review of revisions to the meta data collection and analysis process and to include affidavits describing the value of the collection of telephony metadata authorized by the FISC Telephone Business Records Order. The Government submitted its report to the FISC as required on August 17, 2009. The FISC subsequently renewed the Telephone Business Records Order on September 3, 2009, and, in so doing, restored to NSA the authority to make RAS determinations for selectors that NSA counterterrorism personnel (these selectors are described nominate for analysis through contact chaining as "seeds"). This renewed Order expires on October 30, 2009.

Classified In Camera, Ex Parie Declaration of Lt. Gen. Keith B., Alexander, Director, National Security Agency Progistic Shubert, et al. v. United States of America, et al. (No. 07-cv-693-VRW, MDL No. 06-1791)

-IOP SECKED ISPACOMINE

LORCON NOFORN



~(>{}(`')}~~~(`)|~(`){}?~~ data collection and analysis are vital tools for protecting the United States from attack, and, accordingly, information pertaining to those activities is highly classified.14 2 3 V. (U) Information Protected by Privilege 29. (U) In general and unclassified terms, the following categories of information are 5 subject to the DNI's assertion of the state secrets privilege and statutory privilege under the ñ National Security Act, as well as my assertion of the NSA privilege: 7 (U) Information that may tend to confirm or deny whether Α. the plaintiffs have been subject to any alleged NSA 9 intelligence activity that may be at issue in this matter, and 10 В. (U) Any information concerning NSA intelligence activities, sources, or methods that may relate to or be 11 necessary to adjudicate plaintiffs' allegations, including 12 allegations that the NSA, with the assistance of telecommunications carriers, indiscriminately intercepts the 13 content of communications and also, to the extent applicable to plaintiffs' claim, the communications records 14 of millions of Americans as part of an alleged "Program" 15 authorized by the President after 9/11. See. e.g., Amended Compl. 99 1-8, 58. 16 17 (U) The scope of this assertion includes but is not limited 10: 18 (i) (U) Information concerning the scope and 19 operation of the now inoperative "Terrorist Surveillance 20 Program" ("TSP") regarding the interception of the content of certain one-end international communications 21 reasonably believed to involve a member or agent of al-Queda or an affiliated terrorist organization, and any other 22 information related to demonstrating that the NSA does not 23 otherwise engage in the content surveillance dragnet that the plaintiffs allege; and 24 25 14 (TS//TSP//SI//OC/NF) As the NSA has previously advised the Court in related 26 proceedings, 27 See Classified In Camera, Ex Parte Declaration of LTG Keith B. Alexander ¶ 31 n.8, MDL No. 06-1791-VRW (N.D. Cal.) (submitted Apr. 20, 2007) (relating to 28 all actions against the MCI and Verizon Defendants). 22 Classified In Camera, Ex Parie Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shubert, et al. v. United States of America, et al. (No. 07-ev-692-VRW; MDL No. 06-1791) OKCONNOFORN TOP SECRETATION COMMIT

3

5

7

8

10

П

12

13

14

15

16 17

18

19

20

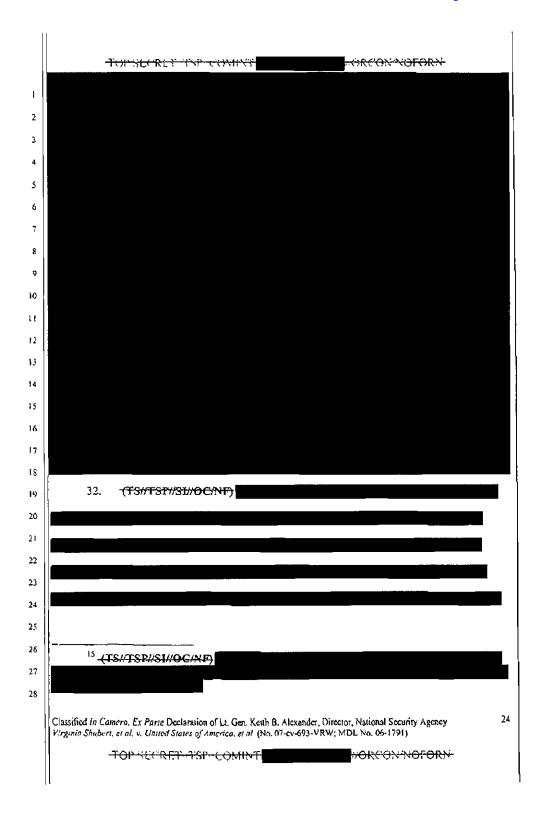
21

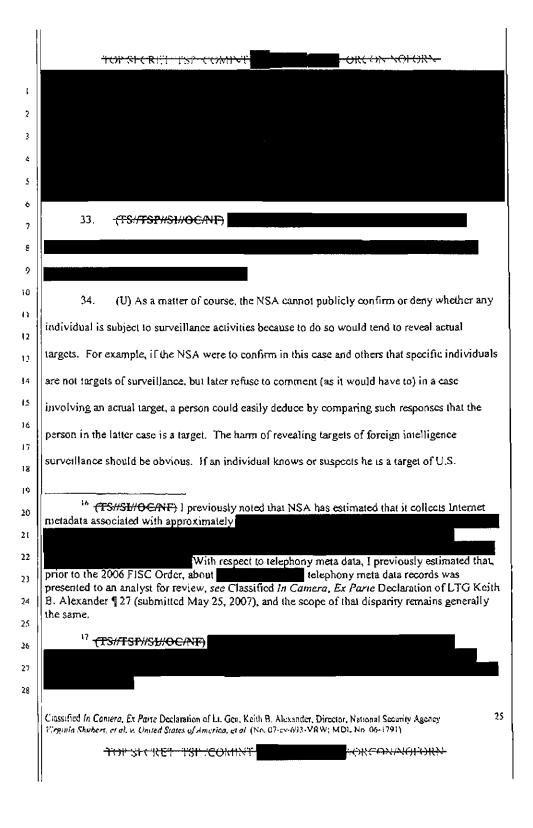
22 23

24

25

26





TOP SHORE THE TREE SHOULD BE SHOON NOTOR

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

- 1. (U) Plaintiffs' Allegations of a Communications Dragnet
- 36. (U) I am also supporting the DNI's assertion of privilege and asserting the NSA's statutory privilege over any other facts concerning NSA intelligence activities, sources, or methods that may relate to or be necessary to adjudicate the plaintiffs' claims and allegations, including that (i) the NSA is indiscriminately intercepting the content of communications of millions of ordinary Americans, see, e.g., Amended Compl. 👭 1-4, and (ii) to the extent relevant to this action, that the NSA is collecting the "call data" of people in the United States with the assistance of telecommunications carriers, presumably including information concerning the plaintiffs' communications. See, e.g., id. ¶¶ 5-8, 58. As described above, the scope of the guvernment's privilege assection includes but is not limited to: (1) facts concerning the operation of the now inoperative Terrorist Surveillance Program and any other NSA activities needed to demonstrate that the TSP was limited to the interception of the content 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) information concerning whether or not the NSA obtains transactional communications records from telecommunications companies. As set forth below, the disclosure of such information would cause exceptionally grave harm to national security.

13 (TS//S1//OCANF)

2

4

5

8

9

10

11 12

13

14

15

16 17

18

19

20

21

22 23

24

25 26

27 28

Classified In Camera, Ex Parie Decianation of Lt. Gen. Keith B. Alexander, Director, National Security Agency V rginia Shubert, et al. v. United States of America, et al. (No. 07-ev-693-VRW: MDL No. 06-1791)

TOP SECRET TWO COMINS

HORCON, NOFORN

TOW YEAR TEN TEN TOWN

2

3

5

6

7

8

10

11

12

13 14

15

16

17

18

19 20

21

22

23

24

25 26 27

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

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

- 38. (U) The privileged information that must be protected from disclosure includes the following classified details concerning content surveillance under the now inoperative TSP.
- 39. (TS//TSP//SI//OC/NF) First, interception of the content of communications under the TSP was triggered by a range of information, including sensitive foreign intelligence,

Classified In Camera, Ex Parte Declaration of L. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shubert, et al. v. Unned States of America, et al. (No. 07-cv-693-VRW; MDl. No. 06-1791)

TOP SHORET TSP-COWINT

¹⁹ (U) See, e.g., Public Declaration of LTG Keith B. Alexander, Director, National Security Agency ¶ 16 (submitted May 25, 2007).

4

5

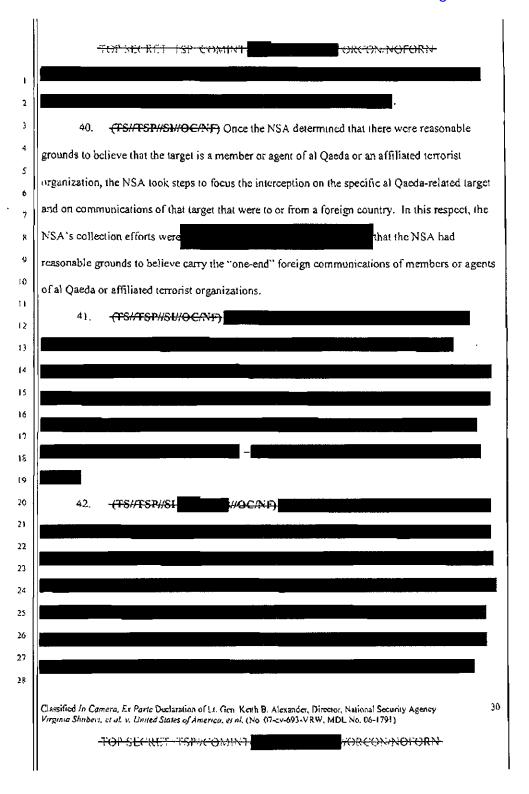
8

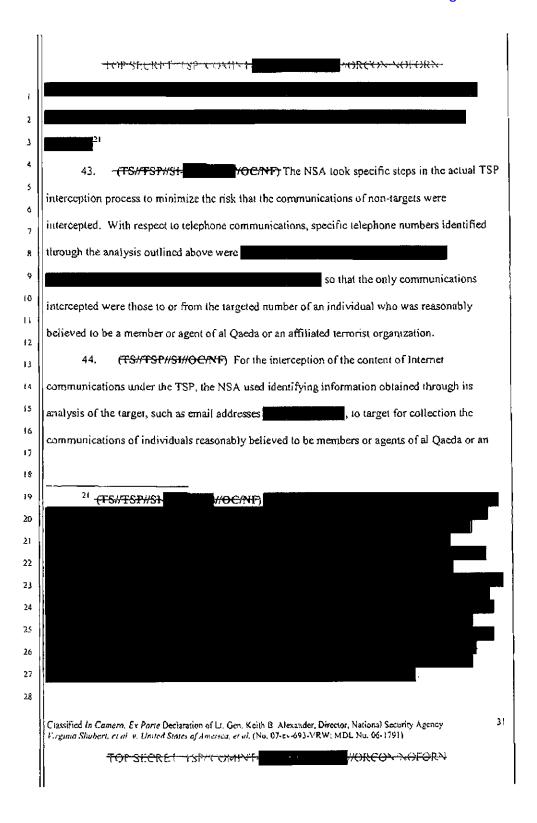
10

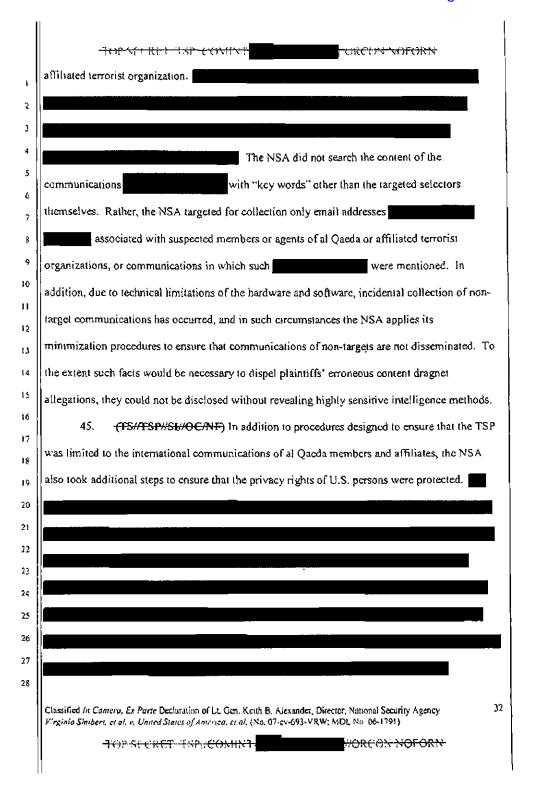
11

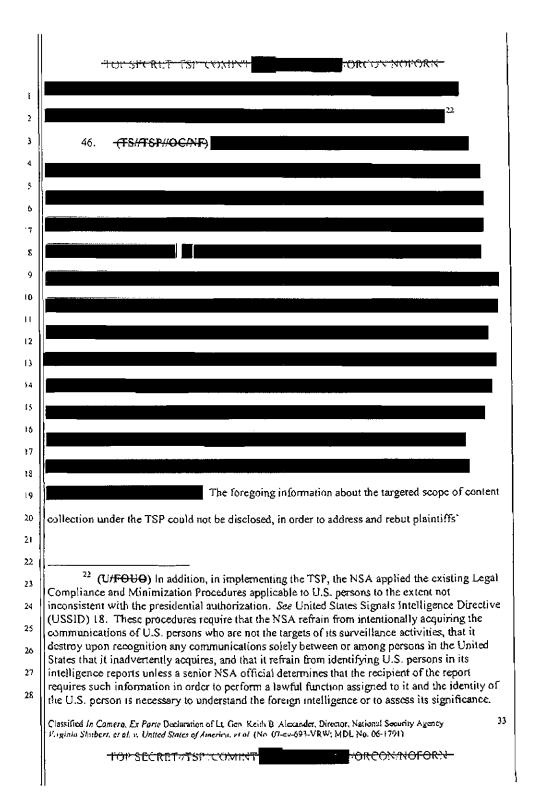
12

obtained or derived from various sources indicating that a particular phone number or email address is reasonably believed by the U.S. Intelligence Community to be associated with a member or agent of al Qacda or an affiliated terrorist organization. Professional intelligence officers at the NSA undertook a careful but expeditious analysis of that information, and considered a number of possible factors, in determining whether it would be appropriate to target a telephone number or cmail address under the TSP. Those factors included whether the target phone number or email address was: (1) reasonably believed by the U.S. Intelligence Community, based on other authorized collection activities or other law enforcement or intelligence sources, to be used by a member or agent of al Qaeda or an affiliated terrorist organization; ²⁰ (TS//TSP//SL//OC/NF) 20 Classified In Camera, Ex Pane Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shiberi, ct at v. United States of America, et al. (No. 07-cv-693-VRW; MDL No. 06-1791) TOP STURFF ISP COMINT









5

6

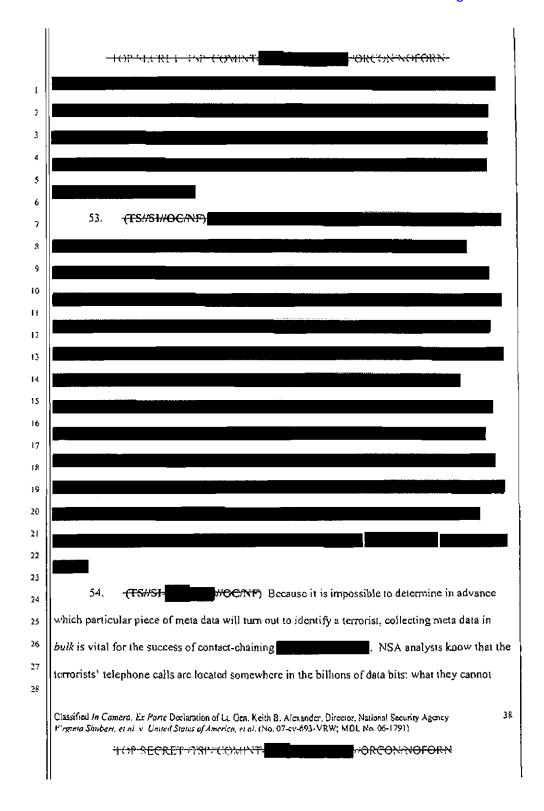
ŀΦ

11

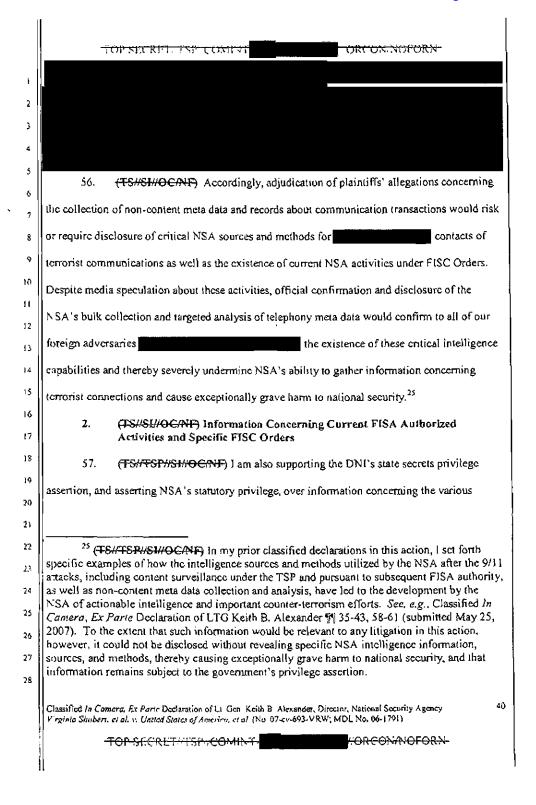
13 14

16

	HOP SPERE TO THE COMING TO THE CORCUMNOPOREN	
	. The only effective means by which NSA analysts are able contin	uously
o keep track	of such operatives is through meta data collection and analysis.	
	(S#Sh/PNF) Technical Details of Analytic Capabilities	
51.	(TS://SU/OC/PIP) In particular, the bulk collection of Internet and telephon	y meta
lata allows ti	ne NSA to use critical and unique analytical capabilities to track the contacts	
hrough the d	ise of two highly sophisticated tools known as "contact-chaining" and	
C	ontact-chaining allows the NSA to identify telephone numbers and email add	resses
liat have bee	numbers and addresses; in turn,	those
ontacts can	be targeted for immediate query and analysis as new	nbers
nd addressc	s are identified. When the NSA performs a contact-chaining query on a terro	rist-
ssociated te	lephone identifier,	
52.	(TS://SE//OC/NT)	
	mera, Ex Parte Doctetation of Lt. Gen. Keith B. Alexander, Director, National Society Agency , et al. v. United States of America, et al. (No. 07-ex-693-VRW, MDL No. 06-1791)	
_	POP SECRET - PSP+COMINT	



ŀ	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
, [know shead of time is exactly where. The ability to accumulate meta data substantially increases
2	NSA's ability to detect and identify these targets. One particular advantage of bulk meta data
3	collection is that it provides a historical perspective on past contact activity that cannot be
4	captured in the present or prospectively. Such historical links may be vital to identifying new
\$	turgets, because the meta data may contain links that are absolutely unique, pointing to potential
6	targets that otherwise would be missed.
é	
9	
10	
ш	
12	These sources and methods enable the NSA to segregate some of that very
13	small amount of otherwise undetectable but highly valuable information from the overwhelming
14	amount of other information that has no intelligence value whatsoever - in colloquial terms, to
15	find at least some of the needles hidden in the haystack. If employed on a sufficient volume of
16	row data, contact chaining and can expose and and
17	contacts that were previously unknown.
19	
20	
21	
22	55. (TS#SH/OC/NP) The foregoing discussion is not hypothetical. Since inception
23	of the first FISC Telephone Business Records Order, NSA has provided 277 reports to the FBI.
24	
25	These reports have tipped a total of 2,900 telephone identifiers as being in contact with
26	identifiers associated with
27	
~3	Classified to Common For Pure, Destaurion of L. Com Maith D. Afmander Disease, Majornal Sequiple Access
	Classified In Camera. Ex Purie Declaration of U. Gir. Keith B. Alexander, Director, National Security Agency Virginia Shubert, et al. v. Limited States of America, et al. (No. 07-ev-693-VRW, MDL No. 06-179))
	TOP SECRET ASPECUMENT



(3R(-(3)-~()F()R\

TOP MERCINET TOP WORLD

orders of the Foreign Intelligence Surveillance Court mentioned throughout this declaration that 2 3 S 6 8 10 16 12 13 14 15 orders, and of subsequent FISC orders reauthorizing these activities, remain highly classified and ١ň disclosure of this information would cause exceptionally grave harm to national security.26 In 17 addition, while the Government has acknowledged the general existence of the January 10, 2007 18 FISC Orders authorizing electronic surveillance similar to that undertaken in the TSP, the 19 20 content of those orders, and facts concerning the NSA sources and methods they authorize, 21 22 23 24 persons as permitted by the Director of the FBI or the Director's designee. The FISC Orders

26

27

28

authorize NSA intelligence collection activities, as well as NSA surveillance activities conducted pursuant to the now lapsed Protect America Act ("PAA") and current activities authorized by the FISA Amendments Act of 2008. As noted herein, the three NSA intelligence activities initiated after the September 11 attacks to detect and prevent a further at Qaeda attack - (i) content collection of targeted at Quedo and associated terrorist-related communications under what later was called the TSP; (ii) internet meta data bulk collection; and (iii) telephony meta data bulk collection - have been subject to various orders of the FISC (as well as FISA statutory authority) and are no longer being conducted under presidential authorization. The bulk collection of noncontent transactional data for Internet communications was first authorized by the FISC in the July 2004 FISC Pen Register Order, and the bulk collection of non-content telephony meta data was first authorized by the FISC in May 2006. The existence and operational details of these

26 (TS//SI//OC/NIP) For this reason, the FISC Telephone Business Records Order and FISC Pen Register Orders prohibit any person from disclosing to any other person that the NSA has sought or obtained the telephony meta data, other than to (a) those persons to whom disclosure is necessary to comply with the Order, (b) an attorney to obtain legal advice or assistance with respect to the production of meta data in response to the Order; or (c) other

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 In Camero, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shuhert, et al. v. (Inited States of America, et al. (No. 97-cv-693-VRW; MDI No. 06-1791)

-TOP SECRET TSP ('ONHH-

/ORCON/XOLOK/

2

1

5

6

8

10

11

12

13

15

16

17

16

19 20

21

22

23

24

25 26

27

28

Classified In Comero. Ex Parie Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shubert, et al. v. United States of America, et al. (No. 07-cv-693-VRW; MDL No. 06-1791)

- (3RC(3)\, \<(3F(3R\) -T()P 's1 c 't21 T - htx|P c 'c7%Htx }

2

4

6

9

10

Ħ

12

13

14 15

16

17

18

19 30

21

22 23

24

25 26

27

28

(TS//SI//OC/NF) By Order dated March 2, 2009, the FISC directed that the NSA may continue to acquire call detail records of telephony meta data in accordance with the FISC Telephone Business Record Orders, but was prohibited from accessing data acquired except in a limited manner. In particular, the Government could request through a motion that the FISC authorize querying of the telephony meta data for purposes of obtaining foreign intelligence on a case-by-case basis (unless otherwise necessary to protect against imminent threat to human life, subject to report to the FISC the next business day). In addition, following the Government's disclosures concerning compliance with the FISC Orders, the FISC imposed other obligations, including to report on its ongoing review of the matter and to file affidavits describing the continuing value of the telephony meta data collection to the national security of the United States and to certify that the information sought is relevant to an authorized investigation. The Government completed its end-to-end review and submitted its report and the required affidavits to the FISC on August 3, 2009. In that report, the Government outlined the steps NSA had taken to address and correct the instances of noncompliance with FISC Orders, as well as the remedial safeguards put in place to monitor and ensure compliance with such Orders in the future. The FISC most recently renewed the Telephone Business Records Order on September 3, 2009. This latest renewal restored to NSA the authority to make RAS determinations on telephone identifiers nominated by NSA personnel to use in conducting contact chaining

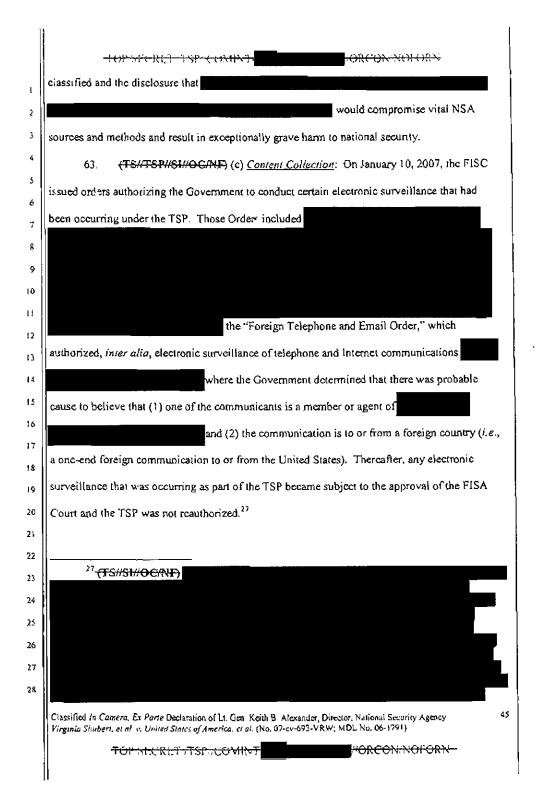
-(TS//TSP//SI WORNING WITH THE FISC on this and other compliance issues to ensure that this vital intelligence tool works appropriately and effectively. For purposes of this litigation, and the privilege assertions now made by the DNI and by the NSA, the intelligence sources and methods described herein remain highly

Classified In Camera, Ex Parte Declaration of LL Gen. Keith B. Alexander, Director, National Security Agency Virginia Simbers, et al. v. United States of America, et al. (No. 07-ex-693-VRW; MDL No. 06-1791)

TOP SECRET / ISP COMINT

44

ᡢ᠐ᠺᢗ᠊ᡃᡠᡳ᠈ᢣᢙᠮᢒᢣᢥ



- until the Protect America Act ("PAA") was enacted in August 2007. Under the PAA, the FISA's definition of "electronic surveillance" was clarified to exclude "surveillance directed at a person reasonably believed to be located outside the United States." 50 U.S.C. § 1805A. The PAA authorized the DNI and the Attorney General to jointly "authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States" for up to one year, id § 1805B(a), and to issue directives to communications service providers requiring them to "immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition" of necessary intelligence information, id. § 1805B(e). Such directives were issued to telecommunications companies and the NSA conducted content surveillance of overseas targets under the PAA through their facilities.
- 65. (TS#SH/OC/NF) Beginning in September 2008, expiring directives that had been issued under the PAA for content surveillance of overseas targets (including surveillance of specific targets overseas) were replaced by new directives for such surveillance issued pursuant to the FISA Amendments Act of 2008. Title I of the FISA Amendments Act of 2008 authorizes the targeting of persons outside of the United States without individual FISC orders but subject to directives issued to carriers by the Director of National Intelligence and the Attorney General under Section 702(h) of the FISA for the continuation of overseas surveillance

u

Classified In Comera, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginio Slubert, et al. v. United States of America, et al. (No. 07-ex-693-VRW; MDL No. 06-1791)

TOP SECRET TSP-CTMINT

᠘᠘᠙ᢗ᠊ᢙᠰᡎ᠐᠄ᢕ

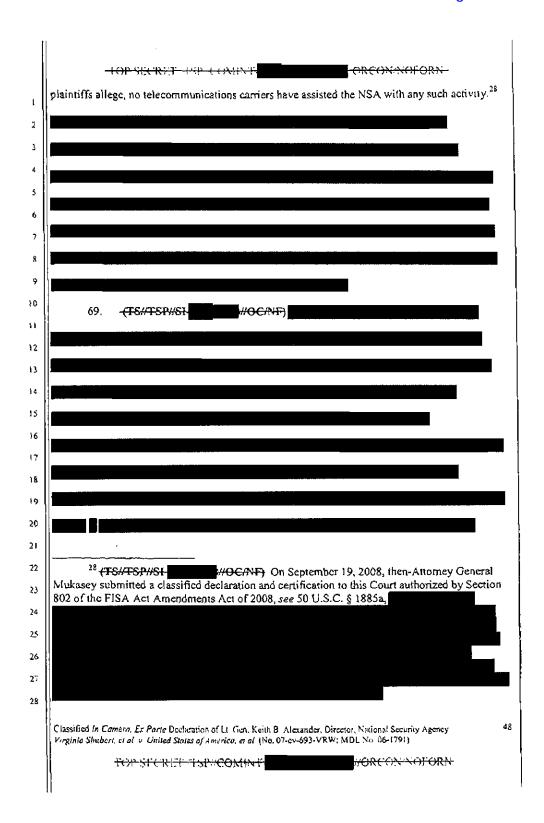
Ηt

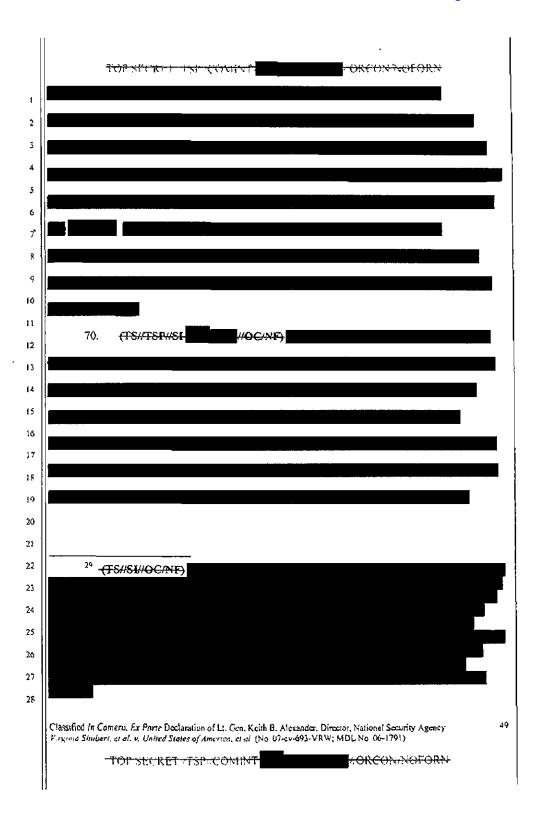
- ondertaken by the NSA evolved from the presidentially authorized TSP to the FISC Foreign Telephone and Email Order, to the directives issued under the PAA and, ultimately, to the directives that are now being issued pursuant to the FISA Amendments Act of 2008. Each authorization sought to enable the NSA to undertake surveillance on numerous multiple targets overseas without the need to obtain advance court approval for each target, but none has entailed the kind of indiscriminate content surveillance dragnet on telephone and Internet communications that the plaintiffs allege.
 - (U) Plaintiffs' Allegations that Telecommunications Companies have Assisted the NSA with the Alleged Activities
- 67. (U) The third major category of NSA intelligence sources and methods as to which I am supporting the DNI's assertion of privilege, and asserting the NSA's statutory privilege, concerns information that may tend to confirm or deny whether or not telecommunications providers have assisted the NSA with alleged intelligence activities.

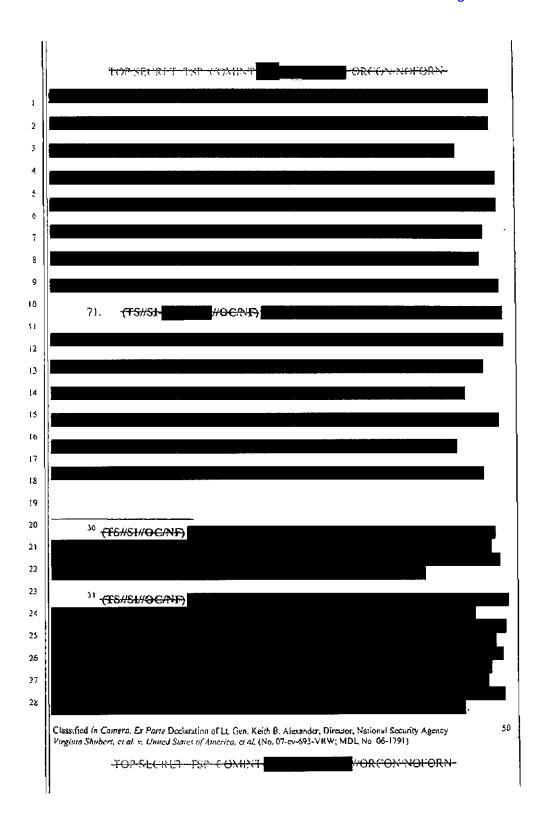
 Plaintiffs allege that they are customers of telecommunications carriers such as AT&T and Verizon, and that these companies participated in the alleged surveillance activities that the plaintiffs seek to challenge. As set forth below, confirmation or denial of a relationship between the NSA and any telecommunications carriers on alleged intelligence activities would cause exceptionally grave harm to national security.
- 68. (TS//TSP//SI- CONTENT OF CONTENT OF Because the NSA is not engaged in the indiscriminate dragnet of the content of domestic and international communications as the

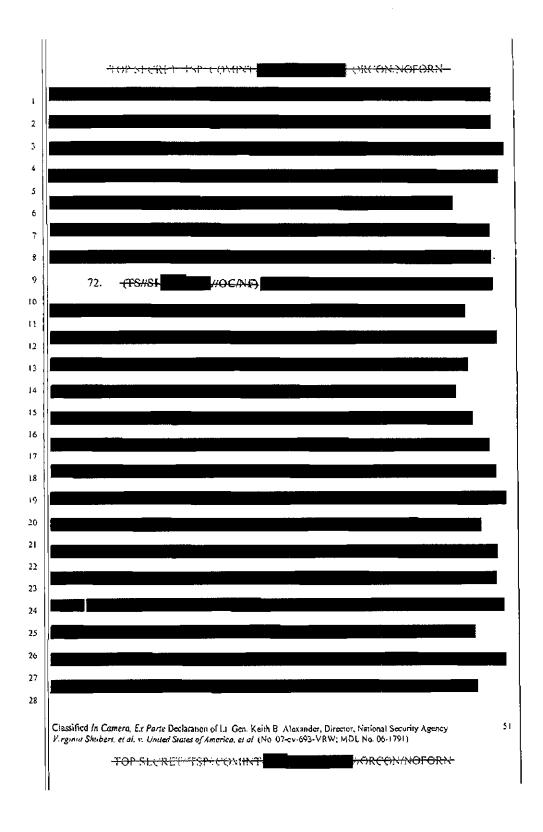
Classified In Camera, Ex Parta Declaration of Lt. Gen. Keith B. Aloxandor, Diroctor, National Society Agency Virginia Shuberi et al. v. United States of America, et al. (No. 07-cv-693-VRW; MDL No. 06-1791)

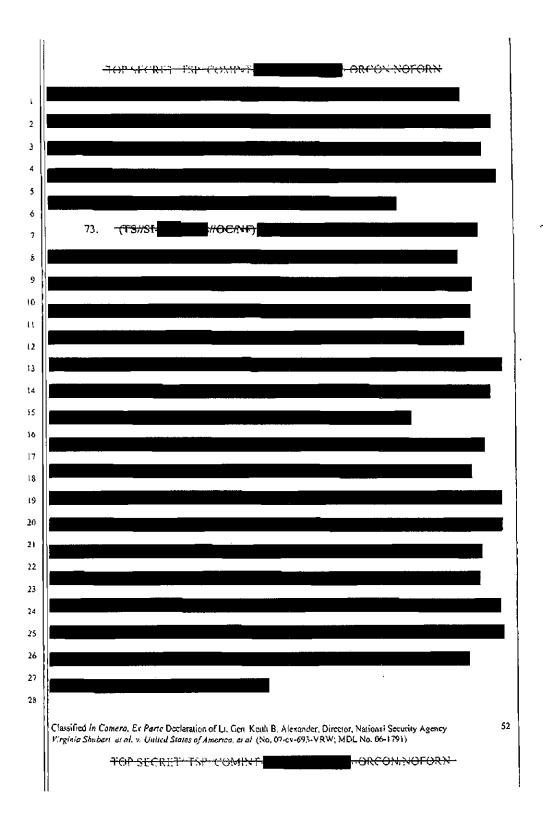
TOP SECRET TERMINE

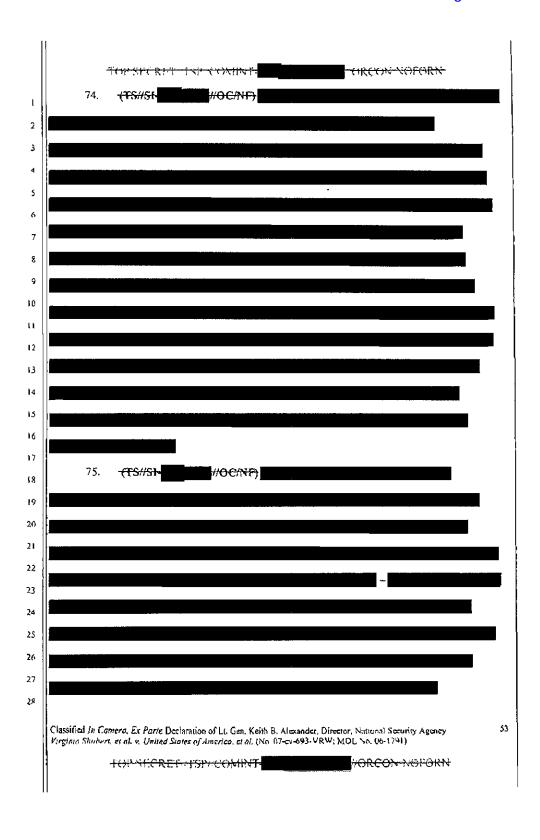


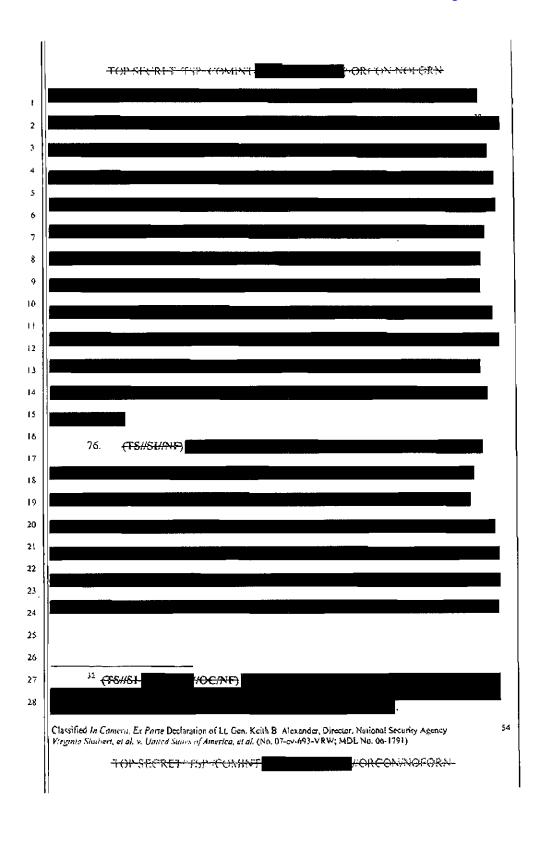












HOP STORM TISE COMING.

Indeed, any effort merely to allude to those facts in a non-classified fushion could be revealing of classified details that should not be disclosed. 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 much bigger picture of U.S. intelligence gathering sources and methods.

- 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 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 numains one of al Qaeda's top operational priorities, see Classified In Camera Ex Parte. Declaration of Admiral Dennis C. Blair, Director of National Intelligence, 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.
- 79. (FS#SHANF) All 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 all Qaeda as they

C'assified In Comera, Ex Parie Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shubert, et al. v. United States of America, et al. (No. 07-cv-893-VRW; MDL No. 06-1791)

TOP SECRET/FSP4COMINT

\`OR(`ON;NOFORN

- TOP STOWN TOWN

ŧ٥

н

{S

-ORCONNOISE ORCONNOISE ORCONNOI

manipulate modern technology in an attempt to communicate while remaining undetected. The NSA sources, methods, and activities described herein are vital tools in this effort.

VIII. (U) Conclusion

80. (U) In sum, I support the DNI's assertion of the state secrets privilege and statutory privilege to prevent the disclosure of the information described herein and detailed herein. I also assert a statutery privilege under Section 6 of the National Security Agency Act with respect to the information described herein that concerns the functions of the NSA. Public disclosure of the aforementioned intelligence sources, methods and activities could reasonably be expected to cause exceptionally grave harm to the national security of the United States.

Consequently, because proceedings in this case risk disclosure of privileged and classified intelligence-related information, I respectfully request that the Court not only protect that information from disclosure but also dismiss this case to prevent exceptionally grave harm to the national security of the United States.

Classified In Camera, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency Virginia Shubert, et al. v. United States of America, et al. (No. 07-cv-693-VRW; MDL No. 06-1791)

TOP SECRETATION COMINT

⊬ORC≔₩₩₩OFORN

	JANUARY COMPANIES CONTRACTOR OF THE STATE OF
	1 dealers and a very law of early as the sales for a size in transport
1	I declare under penalty of perjury that the foregoing is true and correct.
2	DATE: 30 OCT 09 18 B SKI
3	KEMH B. ALÉXANDER LTG. USA
4	Director
5	National Security Agency
6	· ·
7	
8	
9	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
	Classified In Camera, Ex Parte Declaration of Lt. Gen. Keith B. Alexander, Director, National Security Agency V. rginia Shubert, et al. v. United States of America, et al. (No. 07-cv-693-VRW; MDL No. 06-1791)
	TOP:SPCRESTESPTCOMINE