TOP SECRET//SI//NF [redacted] //ORCON,NOFORN

STUART F. DELERY
Acting Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
BRYAN DEARINGER
RODNEY PATTON
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782
Fax: (202) 616-8460
Attorneys for the Government Defendants

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	No. 08-cv-4373-JSW
VIRGINIA SHUBERT, *et al.*, Plaintiffs, v. BARACK OBAMA, *et al.*, Defendants	No. 07-cv-693-JSW **CLASSIFIED DECLARATION OF JAMES R. CLAPPER, DIRECTOR OF NATIONAL INTELLIGENCE** No Hearing Scheduled Courtroom 11, 19th Floor Judge Jeffrey S. White

TOP SECRET//SI//NF [redacted] //ORCON,NOFORN

TOP SECRET//SI//[redacted]//NOFORN

I, James R. Clapper, do hereby state and declare as follows:

(U) INTRODUCTION

1. (U) I am the Director of National Intelligence (DNI) of the United States. I have held this position since August 9, 2010. In my capacity as the DNI, I oversee the U.S. Intelligence Community (IC) and serve as the principal intelligence adviser to the President. Prior to serving as the DNI, I served as the Director of the Defense Intelligence Agency from 1992 to 1995, the Director of the National Geospatial-Intelligence Agency from 2001 to 2006, and the Under Secretary of Defense for Intelligence from 2007 to 2010, where I served as the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense on intelligence, counterintelligence, and security matters for the Department of Defense. In my capacity as the Under Secretary of Defense for Intelligence, I simultaneously served as the Director of Defense Intelligence for the Office of the Director of National Intelligence (ODNI).

2. (U) The purpose of this declaration is to formally assert, in my capacity as the DNI and head of the IC, the state secrets privilege and a statutory privilege under the National Security Act of 1947, as amended, *see* 50 U.S.C. § 3024(i)(1), in order to protect intelligence sources and methods that are at risk of disclosure in the above-captioned case as well as in *Shubert v. Obama* (07-cv-00693) (M: 06-cv-1791). This assertion of privilege updates and modifies my prior assertions of privilege in this litigation. As discussed below, I am no longer asserting privilege over the existence of various presidentially authorized National Security Agency (NSA) intelligence activities, later transitioned to authority under the Foreign Intelligence Surveillance Act (FISA). I continue to assert privilege over still-classified information concerning the scope and operational details of these intelligence activities, including but not limited to information that would tend to confirm or deny that particular

persons were targets of or subject to NSA intelligence activities or that particular telecommunications service providers assisted NSA in conducting intelligence activities. Disclosure of this still-classified information regarding the scope and operational details of NSA intelligence activities implicated by plaintiffs' allegations could be expected to cause extremely grave damage to the national security of the United States. The statements made herein are based on my personal knowledge as well as on information provided to me in my official capacity as the DNI.

(U) SUMMARY

3. (U) In the course of my official duties, I have been advised of this lawsuit and the allegations at issue in the plaintiffs' complaints in the *Jewel* and *Shubert* actions. In personally considering this matter, I have executed a separate unclassified declaration dated December 20, 2013. Moreover, I have read and personally considered the information contained in the Public and the *In Camera, Ex Parte* Declaration of Frances J. Fleisch, National Security Agency (NSA), executed on December 20, 2013 (hereafter "Classified NSA Declaration"). Disclosure of the information covered by my and NSA's privilege assertions reasonably could be expected to cause exceptionally grave damage to the national security of the United States and, therefore, the information should be excluded from any use in this case.

4. (U) I reach this conclusion, and make these assertions of privilege, mindful of the public disclosures of information about classified NSA intelligence programs, both authorized and unauthorized, that have taken place since June 2013. The wave of unauthorized public disclosures of classified information regarding NSA intelligence activities that began in June 2013 has been extremely damaging to the national security of the United States, threatening the ability of the IC to conduct operations effectively and keep our country safe. At the same time,

these disclosures have generated great public interest in how the NSA uses its special tools and authorities to gather intelligence, and whether they have been used appropriately. At the President's direction, I have therefore declassified and publicly released numerous documents disclosing the existence of, and a number of details about, the NSA's collection of bulk telephony and Internet metadata under sections 402 and 501 of FISA, and the content of communications of non-U.S. persons located abroad under FISA section 702. I did this to facilitate informed public debate about the value and appropriateness of these programs with full understanding of what they allow, the oversight mechanisms in place, and the contribution these programs have made to the Nation's security and safety. These documents were properly classified and the decision to declassify and release them was not taken lightly. But I concluded, in consultation with elements of the IC, that in light of the unauthorized disclosures, the public interest in the documents outweighed the potential for additional damage to national security.

5. (U) On December 20, 2013, under authority of the President, the existence of collection activities authorized by President George W. Bush in October 2001 was also declassified. Specifically, starting on October 4, 2001, President Bush authorized the Secretary of Defense to employ the capabilities of the Department of Defense, including the NSA, to collect foreign intelligence by electronic surveillance in order to detect and prevent acts of terrorism within the United States. President Bush authorized the NSA to collect: (1) the contents of certain international communications, a program that was later referred to and publicly acknowledged by President Bush as the Terrorist Surveillance Program (TSP), and (2) telephony and Internet non-content information (referred to as "metadata") in bulk, subject to various conditions.

6. (U) President Bush issued authorizations approximately every 30-60 days.

Although the precise terms changed over time, each presidential authorization required the minimization of information collected concerning American citizens to the extent consistent with the effective accomplishment of the mission of detection and prevention of acts of terrorism within the United States. The NSA also applied additional internal constraints on the presidentially authorized activities.

7. (U) Over time, the presidentially authorized activities transitioned to the authority of the FISA. The collection of communications content pursuant to presidential authorization ended in January 2007 when the U.S. Government transitioned TSP to the authority of FISA under orders of the FISC. In August 2007, Congress enacted the Protect America Act (PAA) as a temporary measure. The PAA expired in February 2008 and was replaced by the FISA Amendments Act of 2008, which was enacted in 2008 and remains in effect today. Today, content collection is conducted pursuant to section 702 of FISA. The metadata activities also were transitioned to orders of the FISC. The bulk collection of telephony metadata transitioned to the authority of FISA in May 2006 and is collected pursuant to section 501 of FISA. The bulk collection of Internet metadata was transitioned to the authority of FISA in July 2004 and was collected pursuant to section 402 of FISA. In December 2011, the U.S. Government decided not to seek re-authorization of the bulk collection of Internet metadata under section 402.

8. (U) As a result of the declassification of the information described above, the U.S. Government is no longer asserting privilege over the existence of these programs, whether conducted under presidential authority or FISC authorization. It has remained necessary, however, to withhold certain information about these programs, even from the publicly released documents, to protect sensitive sources and methods, such as particular targets of surveillance, and methods of collecting and analyzing intelligence information, because public disclosure of

this information would likely cause even graver damage to national security than has already been done by the unauthorized disclosures that have occurred since June 2013. As explained in great detail herein, and in the accompanying Classified NSA Declaration, the same is true with respect to the highly sensitive and still classified information that is implicated by the plaintiffs' allegations in this litigation.

9. (TS//SI//OC/NF) For example, litigating plaintiffs' claims would likely risk or require

10. (U) Accordingly, notwithstanding the unauthorized disclosures and the official declassification and release of information about NSA intelligence programs that have taken place since June of this year, it is my judgment that disclosure of the classified, privileged national security information described herein, and in greater detail in the NSA classified declaration, will risk further and exceptionally grave damage to the national security of the United States.

11. (U) As the NSA states, the allegations in this lawsuit implicate information concerning several highly classified and important NSA intelligence activities that commenced under presidential authorization after the 9/11 terrorist attacks. These activities subsequently

~~TOP SECRET//STLW//SI//~~[redacted]~~//ORCON,NOFORN~~

transitioned to the authority of FISA, and involve (or involved) sources or methods of intelligence gathering that continue to be relied on by the NSA. *See* Classified NSA Declaration.

12. ~~(TS//STLW//SI//~~[redacted]~~OC/NF)~~ In order to address plaintiffs' allegation that the NSA, with the assistance of telecommunication providers, including AT&T and Verizon companies, have indiscriminately intercepted the content and obtained the communications records of millions of ordinary Americans as part of an alleged presidentially authorized "Program" after 9/11, *see, e.g.*, *Jewel* Complaint at ¶¶ 2-13, 39-97; *Shubert* Second Amended Complaint (SAC) ¶¶ 1-9, 57-58, 62-91,102 further litigation would require or risk disclosure of information concerning several classified NSA intelligence activities, sources and methods. This would include [redacted] NSA's (1) targeted content surveillance aimed at [redacted] terrorist organizations, pursuant to the TSP and later pursuant to FISA authority; (2) the bulk collection and targeted analysis of non-content information about telephone and Internet communications—important and sensitive activities that have been or continue to be conducted pursuant to FISC orders [redacted] and that have enabled the NSA to uncover the contacts [redacted] of members or agents of [redacted] terrorist organizations; [redacted] This lawsuit therefore implicates information concerning foreign intelligence-gathering activities utilized to meet the extremely serious threat of another terrorist attack on the U.S. Homeland, a threat which I describe further below.

13. (U) Accordingly, as set forth further below, I am asserting the state secrets

privilege and the DNI's authority to protect intelligence sources and methods pursuant to 50 U.S.C. § 3024(i)(1) to protect against the disclosure of highly classified and important intelligence information, sources and methods put at issue in this case, many of which are vital to the national security of the United States, including: (a) information concerning the specific nature of the terrorist threat posed by al-Qa'ida and its affiliates and other foreign terrorist organizations to the United States; (b) information that would tend to confirm or deny whether particular individuals, including the named plaintiffs, have been subject to any NSA intelligence activities; (c) information concerning the scope or operational details of NSA intelligence activities that may relate to or be necessary to adjudicate plaintiffs' allegations, including plaintiffs' claims that the NSA indiscriminately intercepts the content of communications, and their claims regarding the NSA's bulk collection of telephony and Internet communications records ("metadata"); and (d) information that may tend to confirm or deny whether AT&T or Verizon (and to the extent relevant or necessary, any other telecommunications carrier) has provided assistance to the NSA in connection with any intelligence activity.

14. (U) I specifically concur with the NSA that public speculation about alleged NSA activities above and beyond what has been officially disclosed does not diminish the need to protect intelligence sources and methods from further exposure, and that official confirmation and disclosure of the classified, privileged national security information described herein can be expected to 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 I make herein, as well as the statutory privilege assertion made by the NSA pursuant to Section 6 of the National Security Agency Act, *see* 50 U.S.C. § 3605 (note), and protect the information described in this declaration from disclosure.

~~TOP SECRET//STLW/SI//ORCON/NOFORN~~

(U) CLASSIFICATION OF DECLARATION

15. ~~(S//SI//NF)~~ Pursuant to the standards in Executive Order (E.O.) 13526, this declaration is classified as: ~~TOP SECRET//STLW/SI//ORCON/NOFORN.~~ The details concerning these classification markings are set forth in the Classified NSA Declaration and are briefly summarized here. Under E.O. 13526, 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 identifiable damage to national security. At the beginning of each paragraph of this declaration, the letters "U," "C," "S," and "TS" indicate respectively that the information is either UNCLASSIFIED, or is classified CONFIDENTIAL, SECRET, or TOP SECRET.

16. (U) Additionally, this declaration also contains Sensitive Compartmented Information (SCI), which is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods. This declaration references communications intelligence, also referred to as special intelligence (SI), which is a subcategory of SCI that identifies information that was derived from exploiting cryptographic systems or other protected sources by applying methods or techniques, or from intercepted foreign communications. This declaration also references human intelligence control system (HCS), another subcategory of SCI that identifies information derived from individuals who provide intelligence information.

17. ~~(TS//STLW/SI//OC/NF)~~ This declaration also contains information related to or

derived from the STELLARWIND program, a controlled access signals intelligence program under presidential authorization in response to the attacks of September 11, 2001. In this declaration, information pertaining to the STELLARWIND program is denoted with the special marking "STLW" and requires more restrictive handling. Despite the December 2005 public acknowledgement of the TSP, and the recent public acknowledgment of NSA bulk telephony and Internet metadata collection activities that were also part of the STELLARWIND program, certain details about the STELLARWIND program (including the TSP) remain highly classified and strictly compartmented, [redacted]

[redacted]

18. (U) Finally, information labeled "NOFORN" may not be released to foreign governments, foreign nationals, or non-U.S. citizens without permission of the originator and in accordance with DNI policy. The "ORCON" designator means that the originator of the information controls to whom it is released.

(U) BACKGROUND ON DIRECTOR OF NATIONAL INTELLIGENCE

19. (U) The position of DNI was created by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, §§ 1011(a) and 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending sections 102 through 104 of Title I of the National Security Act of 1947). Subject to the authority, direction, and control of the President, the DNI serves as the head of the IC and as the principal adviser to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security. *See* 50 U.S.C. § 3023(b)(1), (2).

20. (U) The IC includes the ODNI; the Central Intelligence Agency; the NSA; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the military services, the Federal Bureau of Investigation, the Department of the Treasury, the Department of Energy, the Drug Enforcement Administration, and the Coast Guard; the Bureau of Intelligence and Research of the Department of State; the elements of the Department of Homeland Security concerned with the analysis of intelligence information; and such other elements of any other department or agency as may be designated by the President, or jointly designated by the DNI and heads of the department or agency concerned, as an element of the IC. *See* 50 U.S.C. § 3003(4).

21. (U) The responsibilities and authorities of the DNI are set forth in the National Security Act of 1947, as amended. *See* 50 U.S.C. § 3024. These responsibilities include ensuring that national intelligence is provided to the President, the heads of the departments and agencies of the Executive Branch, the Chairman of the Joint Chiefs of Staff and senior military commanders, and the Senate and House of Representatives and committees thereof. *See* 50 U.S.C. § 3024(a)(1). The DNI is also charged with establishing the objectives of, determining the requirements and priorities for, and managing and directing the tasking, collection, analysis, production, and dissemination of national intelligence by elements of the IC. *Id.* § 3024(f)(1)(A)(i) and (ii).

22. (U) In addition, the National Security Act of 1947, as amended, provides that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 3024(i)(1). Consistent with this responsibility, the DNI

establishes and implements guidelines for the IC for the classification of information under applicable law, Executive orders, or other Presidential directives, and access to and dissemination of intelligence. *Id.* § 3024(i)(2)(A), (B). In particular, the DNI is responsible for the establishment of uniform standards and procedures for the grant of access to SCI to any officer or employee of any agency or department of the United States, and for ensuring the consistent implementation of those standards throughout such departments and agencies. *Id.* § 3024(j)(1), (2).

23. (U) By virtue of my position as the DNI, and unless otherwise directed by the President, I have access to all intelligence related to the national security that is collected by any department, agency, or other entity of the United States. *See* 50 U.S.C. § 3024(b); section 1.3(a) of E.O. 12333, as amended. Pursuant to E.O. 13526, the President has authorized me to exercise original TOP SECRET classification authority.

(U) ASSERTION OF STATE SECRETS PRIVILEGE

24. (U) After careful and actual personal consideration of the matter, based upon my own knowledge and information obtained in the course of my official duties, including the information contained in the public and classified *In Camera, Ex Parte* Declarations of Frances J. Fleisch, NSA, I have determined that sensitive state secrets concerning NSA sources, methods, and activities are implicated by allegations that lie at the core of plaintiffs' claims, and that the disclosure of this information—as set forth herein and described in more detail in the Classified NSA Declaration—can be expected to cause exceptionally grave damage to the national security of the United States, and therefore that information must be protected from disclosure and excluded from this case. Thus, as to this information, I formally assert the state secrets privilege.

(U) ASSERTION OF STATUTORY PRIVILEGE UNDER NATIONAL SECURITY ACT

25. (U) Through this declaration, I also hereby invoke and assert a statutory privilege held by the DNI under the National Security Act of 1947, as amended, to protect the information described herein, *see* 50 U.S.C. § 3024(i)(l). My assertion of this statutory privilege for intelligence sources and methods is coextensive with my state secrets privilege assertion.

(U) INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE

26. (U) In general and unclassified terms, the following categories of still-classified information are subject to my state secrets and statutory privilege assertions:

A. (U) *Threat Information*: information concerning the specific nature of the terrorist threat posed by al-Qa'ida and its affiliates and other foreign terrorist organizations to the United States, including actual intelligence information collected from intelligence collection activities;

B. (U) *Persons Subject to Intelligence Activities*: information that would tend to confirm or deny whether particular individuals, including the named plaintiffs, have been subject to any NSA intelligence activities;

C. (U) *Operational Information Concerning NSA Intelligence Activities:* information concerning the scope and operational details of NSA intelligence activities that may relate to or be necessary to adjudicate plaintiffs' allegations, including:

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

a) *TSP information:* information concerning the scope and operation of the now inoperative TSP regarding the interception of the content of certain one-end-international communications reasonably believed to involve a member or agent of al-Qa'ida or an affiliated terrorist organization;

b) *FISA section 702:* information concerning operational details related to the collection of communications under

FISA section 702; and

c) any other information related to demonstrating that the NSA has not otherwise engaged in the content-surveillance dragnet that the plaintiffs allege, and

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

and

D. (U) *Telecommunications Provider Identities:* Information that may tend to confirm or deny whether AT&T or Verizon (and to the extent relevant or necessary, any other telecommunications carrier), has provided assistance to the NSA in connection with any intelligence activity, including the collection of communications content or non-content transactional records alleged to be at issue in this litigation.

(U) DESCRIPTION OF INFORMATION SUBJECT TO PRIVILEGE AND HARM OF DISCLOSURE

A. (U) Information Concerning the Threat Posed by al-Qa'ida, It's Affiliates, and Other Foreign Terrorist Organizations

27. (U) The intelligence activities, sources, and methods that are implicated by this lawsuit, and put at risk of disclosure in further proceedings, must be viewed and understood in the context of the threat faced by the United States. In unclassified terms, more than a decade after the September 11, 2001 attacks, we remain in a global conflict with al-Qa'ida and face an evolving threat from its affiliates and adherents. America's campaign against terrorism did not end with the mission at Bin Ladin's compound in May 2011. Indeed, the threats we face have become more diverse.

28. (U) In addition, to the extent classified information about the al-Qa'ida threat

from September 11, 2001 to the present, or the many other threats facing the United States, would be at issue in attempting to litigate this case (for example, to demonstrate the reasonableness of the intelligence-gathering activities initiated in the wake of the September 11, 2001, attacks, and those that remain in place today), such information could not be disclosed without revealing intelligence sources, methods, and information of the United States and thereby causing exceptionally grave damage to the national security. Therefore, I assert the state secrets and DNI statutory privilege to protect such information from disclosure. By way of illustration, set forth below is a largely unclassified discussion of al-Qa'ida and several of its principal affiliates, followed by a discussion of some of the classified threat information pertaining to these terrorist organizations that is subject to this assertion of privilege.

1. (U) Al-Qa'ida and Its Affiliated Groups

29. (TS/[redacted]/NF) As al-Qa'ida's core leadership struggles to remain relevant, the group has turned to its affiliates and adherents to carry out attacks and to advance its ideology. These groups are from an array of countries, including Yemen, Somalia, Nigeria, Iraq, and Syria. To varying degrees, these groups coordinate their activities with and follow the direction of al-Qa'ida leaders in Pakistan. Many of the extremist groups themselves are multidimensional, blurring the lines between terrorist groups, insurgency, and criminal gangs.

30. (U) For example, al-Qa'ida in the Arabian Peninsula (AQAP) remains of particular concern to the United States. The National Counterterrorism Center (NCTC) assesses that this is the most likely entity to attempt attacks in the West. Even in the wake of Anwar al-Aulaqi's death in September 2011, this group maintains the intent and capability to conduct anti-United States attacks with little to no warning. In its three attempted attacks against the U.S. Homeland -- the airliner plot of December 2009, an attempted attack against U.S.-bound cargo

planes in October 2010, and an airliner plot in May 2012 similar to the 2009 attempt -- AQAP has shown an awareness of the capabilities of Western security procedures and demonstrated its efforts to adapt. AQAP continues to exploit Yemen's inability to disrupt its operations on a consistent basis to secure safe havens in the country and mount attacks against the U.S. Embassy in Sanaa.

31. (U) AQAP has also continued to publish the English-language *Inspire* magazine—previously spearheaded by now-deceased al-Aulaqi and Samir Khan—in order to mobilize Western-based individuals for violent action, and the publication continues to reach a wide global audience of extremists.

32. (U) Al-Qa'ida's affiliate in Iraq has demonstrated its capacity to mount coordinated, country-wide terrorist attacks is growing, as it continues at an increasing pace to kill Iraqi civilians by the scores, even hundreds, with near-daily car and suicide bombs over the past year, while also publicly acknowledging the group had established an affiliate in Syria, the al-Nusrah Front, with resources diverted from its operations in Iraq. In April, AQI declared its merger with al-Nusrah Front to form the "Islamic State of Iraq and the Levant." However, al-Nusrah Front's leader rejected the merger and pledged allegiance directly to al-Qa'ida leader Ayman al-Zawahiri. Zawahiri in June 2013 recognized al-Nusrah Front as an al-Qa'ida affiliate, independent of AQI/ISIL and primarily responsible for operations in Syria. Despite his differences with al-Qa'ida leadership over roles insides Syria, AQI/ISIL's leader last year espoused support for violence against the United States, and continues to support al-Qa'ida's global ideology.

33. (U) While al-Nusrah Front and AQI/ISIL at times openly have fought, both groups share the near-term goals of removing the Syrian regime from power, and creating a

government, favorable to them, based on a strict interpretation of Sharia law. Al-Nusrah Front and AQI/ISIL subscribe to a global jihadist ideology, and each group probably has ambitions beyond the conflict in Syria. The groups potentially have access to thousands of foreign fighters, including some Americans, who since 2012 have traveled to Syria to participate in the conflict for a variety of reasons. Additionally, the groups probably have established training camps, familiarizing recruits with combat tactics, as well as the handling of firearms and explosives. Al-Nusrah Front and AQI/ISIL's access to foreign fighters, and the permissive operating environment in Syria, raise the IC's concerns that such individuals, Americans among them, could be leveraged and trained to conduct terrorist attacks in their home countries.

34. (U) AQI/ISIL leadership also continues to make public statements inciting violence against governments outside of Iraq and Syria. In an August 2013 statement, the group's spokesman called on Egyptians to attack the Egyptian military and follow the example of extremists in Iraq and Syria. Both the group's spokesman and its overall leader last year threatened future efforts to target Americans.

35. (U) For the first time, AQI/ISIL in 2013 began releasing propaganda openly recruiting Westerners, including Belgian and French speakers, highlighting its intent to build a capability to mount attacks against the West. AQI/ISIL's spokesman in mid-2013 publicly stated the group plans to conduct attacks from eastern Iraq to western Lebanon, and the group's vitriolic rhetoric and hard-line agenda suggest the group poses a broader threat outside the region than at any time since it was pushed into decline by U.S. coalition forces during the Iraq conflict.

36. (U) During the past two-to-four years, American and Canadian authorities have arrested several North America-based AQI/ISIL associates, highlighting the potential threat posed to the United States. In May 2011, the FBI arrested Kentucky-based Iraqi nationals Waad

Alwan and Shareef Hamadi for attempting to send weapons and explosives from Kentucky to Iraq and conspiring to commit terrorism while in Iraq. Alwan pled guilty to supporting terrorism in December 2011. In January 2010, Canadian authorities arrested dual Iraqi-Canadian citizen Faruq 'Isa who is accused of vetting individuals on the Internet for suicide operations in Iraq.

37. (U) The IC continues to monitor al-Shabaab and its foreign fighter cadre as a potential threat to the U.S. Homeland, although the group is mainly focused on combating African Union Mission in Somalia (AMISOM) forces battling the group in Somalia. The group, which formally merged with al-Qa'ida in February 2012, also remains intent on conducting attacks against regional and Western targets in East Africa, especially in countries contributing to the AMISOM mission. Al-Shabaab associated militants in September 2013 conducted an attack on a shopping mall in Nairobi, Kenya. Al-Shabaab leaders in the past have publicly called for transnational attacks, including threatening to avenge the January 2012 death of British national and al-Shabaab senior foreign fighter Bilal Berjawi.

38. (U) Al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) and Boko Haram have shown minimal interest in targeting the U.S. Homeland, but remain focused on local and regional attack plotting, including targeting Western interests through kidnap-for-ransom operations and other means. AQIM is actively working with local extremists in northern Mali to establish a safe haven from which to advance future operational activities. Al-Murabitun, the extremist group formed in August 2013 through the merger of two AQIM offshoots – Mohtar Belmokhtar's al-Mulathamun Battalion and Tawhid wal Jihad in West Africa (TWJWA) – likewise appears focused on plotting against Western interests in North and West Africa. Boko Haram probably has an emerging awareness of U.S. persons or entities in the United States with connections to Nigeria. The group's spokesman publicly threatened to find a way to attack a

U.S.-based news organization if its coverage of Islam did not change.

39. (U) In addition, while most Pakistani and Afghan militant groups pose a more direct threat to U.S. interests and our allies in that region, the IC continues to watch for indicators that any of these groups, networks, or individuals are actively pursuing or have decided to incorporate operations outside of South Asia as a strategy to achieve their objectives. Tehrik-e Taliban Pakistan (TTP) leaders have repeatedly threatened attacks against the United States, including after the death of Bin Ladin. NCTC assesses that TTP's claim of responsibility for the failed New York Times Square bombing in May 2010 demonstrates its willingness to act on this intent.

40. ~~(S//OC/NF)~~ The NCTC's current classified threat assessment underscores the continuing threat posed by al-Qa'ida and its affiliates. While NCTC assess that "core" al-Qa'ida, due to leadership losses and other setbacks in recent years, is probably currently unable to carry out complex, coordinated, large-scale attacks in the West, it remains intent on doing so. At the same time, the terrorist threat to the United States has diversified to include groups affiliated or allied with al-Qa'ida. NCTC assesses that these terrorist adversaries remain determined to strike against U.S. and Western interests, including via smaller and simpler plots that may be more difficult to detect. Preventing attacks remains the IC's highest priority. In this evolving threat landscape, the agencies of the IC continue to work together to disrupt terrorist plots against the United States at home and overseas, to degrade al-Qa'ida significantly through relentless counterterrorism pressure in key global safe havens, and to share key information with domestic and international partners.

(2) ~~(S//NF)~~ Counterterrorism Successes Against al-Qa'ida

41. ~~(S//NF)~~ Major counterterrorism successes and momentous global events in recent

years have altered the terrorist threat landscape in a way that lessens the direct threat of a large-scale, operationally complex, mass-casualty attack against the U.S. Homeland in the near-term. [redacted]

42. (S//NF) The deaths of Pakistan-based al-Qa'ida leader Usama Bin Ladin and Yemen-based AQAP planner Anwar al-Aulaqi in 2011 removed two of the most influential drivers of the terrorist threat against the Homeland. These two leaders provided strategic oversight and operational guidance for the majority of the most notable large-scale attacks and attempted attacks against the United States since 2001. Additionally, they were responsible for providing inspiration to a global audience of al-Qa'ida members, allies, and adherents about the necessity of attacking the "far" enemy in order to achieve the longstanding goal of the global jihad. [redacted]

43. (TS//HCS [redacted] OC/NF) [redacted]

[redacted]

44. ~~(S//NF)~~ Al-Qa'ida has not conducted a successful attack in the West since 2005, and [redacted]

(3) ~~(S//NF)~~ The Continuing Threat of al-Qa'ida and its Global Affiliates.

45. ~~(TS//HCS/[redacted]/OC/NF)~~ Notwithstanding the successes described above, al-Qa'ida and its global affiliates continue to pose a threat to the Nation's security. Pakistan-based al-Qa'ida continues to demonstrate persistent intent to conduct attacks against the United States. Intelligence reporting indicates that [redacted] NCTC assesses that the group almost certainly would attempt to attack the United States if resources, including viable operatives, were available. Zawahiri [redacted]

[redacted] Al-Qa'ida's prospects for rebounding from its weakened state are low and depend on its ability to protect its Pakistan-based cadre and global influence, while addressing deficiencies in leadership and operational capabilities. Despite its shrinking leadership cadre, persistent unrest in places such as Yemen, Libya, Syria, and Egypt, and the impending withdrawal of U.S. forces from Afghanistan, may provide core al-Qa'ida a propaganda opportunity to claim victories over the United States and reinvigorate its image as the leader of the global movement.

46. (TS//HCS [redacted] /OC/NF) [redacted]

47 (S//NF) In addition, against this backdrop of a weakened core al-Qa'ida, NCTC assesses that in the coming years the United States will be facing a more interdependent and diverse terrorist threat than we have experienced to date, which will likely be more difficult to detect. An expanded set of terrorist adversaries [redacted] in recent years have carried on al-Qa'ida's mantle and attempted to strike in and against the U.S. Homeland. Al-Qa'ida's affiliate groups are likely to remain committed to al-Qa'ida's ideology and to seek opportunities to strike U.S. interests in their operating areas or in the West. The intent and capability of each affiliate to conduct transnational attacks varies

~~TOP SECRET//HCS//SI//NOFORN~~

widely, however, in large part because of their focus on achieving local and regional goals. However, increasing collaboration between al-Qa'ida's affiliates will further shift the focal point of the global jihad away from South Asia, in particular, as the groups share expertise, advice and inspiration in ways that improve their attack capabilities and/or understanding of our counterterrorism capabilities and tactics.

48. ~~(TS//HCS//OC/NF)~~ AQAP continues its efforts to conduct attacks against Americans in the region and in the West. AQAP remains committed to its regional agenda,

Additionally, periodic reporting reveals AQAP's intentions to conduct attacks in neighboring Gulf States

49. ~~(TS//HCS//OC/NF)~~ AQAP as of early planned to conduct major operations that were disrupted by U.S. Government actions. The increased security and counterterrorism pressure mounted in response to the AQAP threat initially caused the group to decrease its operational tempo for internal attacks and limited its movements. However, with fewer counterterrorism operations conducted the IC has observed a recent spike in attacks that reflects AQAP's return to a more aggressive operational approach as they continue to pursue multiple plots

[redacted]

[redacted]

(4) ~~(S//NF)~~ Al-Qa'ida's Weapons and Tactics

53. ~~(S//NF)~~ The types of weapons and tactics al-Qa'ida employs characterize the group's continuing threat. [redacted] In its propaganda, al-Qa'ida has encouraged "lone-wolf" extremists to conduct U.S. Homeland small arms attacks because firearms are easy to acquire and use effectively in the United States, an assertion borne out by a number of small-arms attacks and disrupted plots over the past three years involving homegrown violent extremists. [redacted] Al-Qa'ida-inspired extremists can be expected to attempt to exploit emerging consumer off the shelf technologies for building, concealing and triggering IEDs, and leverage online resources to provide the know-how for new attack methods.

54. ~~(S//NF)~~ [redacted]

[redacted]

[redacted]

57. (U) In sum, a variety of entities continue to pose a significant threat to the nation's security. The U.S. Government is utilizing all lawful intelligence gathering capabilities, including those set forth in the Classified NSA Declaration, to meet these threats and to protect

the American people. I set forth this information not only to provide the Court with background information necessary to understand why the intelligence activities implicated by or directly at issue in this case are being undertaken, but also to assert a claim of privilege over classified threat information. The U.S. Government cannot disclose classified threat information in addressing plaintiffs' allegations or other issues in this case, or even in publicly supporting its assertion of privilege, because to do so would disclose to our adversaries what we know of their plans and how we may be obtaining information about them. Such disclosures would lead our adversaries not only to alter their plans, but also to implement greater security for their communications, thereby increasing the risk of non-detection. In addition, disclosure of threat information might reveal human sources for the United States, compromise those sources, and put their or their families' lives in danger. Accordingly, because I believe that classified threat information is crucial to understanding the importance to our national security of the U.S. Government's intelligence activities, sources, and methods implicated by the plaintiffs' allegations, I must assert the state secrets privilege and the DNI's statutory privilege over this classified threat information because of the exceptionally grave danger to national security that could reasonably be expected to result from its disclosure.

B. (U) Information That May Tend To Confirm or Deny Whether Particular Individuals, Including the Named Plaintiffs, Have Been Subject to NSA Intelligence Activities.

58. (U) Next, I am also asserting privilege over information that would tend to reveal whether particular individuals, including the named plaintiffs in this lawsuit, have been subject to NSA intelligence activities implicated by plaintiffs' allegations. Disclosure of such information can be expected to cause exceptionally grave damage to the national security.

59. ~~(TS//SI//NF)~~ I understand from the Classified NSA Declaration that the NSA has

[redacted] *See* Classified NSA Declaration. [redacted] I concur with the NSA's conclusion that disclosure of these facts can be expected to cause substantial harm to the national security because [redacted] would require the disclosure of sensitive and classified details about NSA intelligence-gathering methods. Accordingly, I assert the state secrets and DNI statutory privilege as to this information.

60. (U) The NSA cannot publicly confirm or deny whether any particular individual is subject to intelligence-gathering activities, no matter how likely or unlikely it might appear that the individual would be subject to surveillance. If the NSA were to reveal that an individual is the target or a subject of intelligence-gathering, the collection capability relating to that individual would certainly be compromised. On the other hand, if the NSA were to reveal that an individual is not the target or subject of intelligence-gathering, adversaries would know that a particular individual has avoided scrutiny and is a secure source for communicating. Moreover, providing assurances to those individuals who are not targets or subjects quickly becomes unworkable when faced with a situation in which an individual has in fact been a target or subject. If the NSA were to confirm that any specific individual is not a target or subject of intelligence-gathering, but later refuse to confirm or deny that fact in a situation involving an actual target or subject, it would be apparent that intelligence-gathering was occurring in the latter case. The only recourse for the NSA is to neither confirm nor deny whether someone has been targeted by or subject to NSA intelligence-gathering activities, regardless of whether the

individual has been a target or subject or not. To say otherwise when challenged in litigation would result in the frequent, routine exposure of NSA information, sources, and methods, and would severely undermine surveillance activities in general.

C. (U) Information Concerning the Scope or Operational Details of NSA Intelligence Activities, Including NSA Sources or Methods.

61. (U) Furthermore, I am asserting privilege over any other still-classified facts concerning the scope or operational details of any NSA intelligence activities that may relate to or be necessary to adjudicate plaintiffs' allegations. As noted above, my privilege assertion includes, but is not limited to, (1) facts concerning the operation of the now-defunct TSP, including any facts needed to demonstrate that the TSP was limited to the interception of the content[1] of one-end foreign communications reasonably believed to involve a member or agent of al-Qa'ida or an affiliated terrorist organization, (2) facts concerning the operation of the collection of communications under FISA Section 702; (3) any other information related to demonstrating that the NSA has not otherwise engaged in the content-surveillance dragnet that the plaintiffs allege, and (4) still classified information concerning the scope or operational details of NSA intelligence activities involving the collection of bulk communications metadata, as discussed in greater detail in the Classified NSA Declaration.

62. (U) As the NSA indicates, *see* Public NSA Declaration, 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-Qa'ida or an affiliated organization. Thus, as the U.S. Government has previously stated, plaintiffs' allegation that the NSA has indiscriminately collected the content of millions of communications sent or received

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

[redacted]

by people inside the United States after September 11, 2001, under the TSP is false. I concur with the NSA that to the extent it must demonstrate in this case that the TSP was not the content dragnet plaintiffs allege, or demonstrate that the NSA has not otherwise engaged in the alleged content dragnet, highly classified details about the scope and operation of the TSP and other NSA intelligence activities would be disclosed, including NSA intelligence sources and methods, thus risking exceptional harm to national security.

63. (U) In particular, as set forth in the Classified NSA Declaration, the United States faced urgent and immediate intelligence challenges after the September 11, 2001, attacks, and undertook signals intelligence activities pursuant to presidential authorization that were designed to meet those challenges and to detect and prevent future terrorist attacks by al-Qa'ida and its affiliates. Those activities include the TSP and similar sources and methods of content surveillance that later became subject to FISA authority, as well as the bulk collection of telephony and Internet non-content metadata that was also later transitioned to FISA authority, and used to discover contacts and communications patterns of members and affiliates of al-Qa'ida. *See* Classified NSA Declaration.

64. (U) Based on my personal consideration and judgment as to the harm disclosure can be expected to cause to national security, my privilege assertion includes, but is not limited to, the following information discussed in the Classified NSA Declaration.

65. ~~(TS//STLW//SI//OC/NF)~~ I assert privilege over still-classified facts concerning: the scope and operation of the TSP and any other NSA intelligence activities needed to demonstrate that the TSP was limited to the interception of certain one-end communications (*i.e.*, to or from the United States) reasonably believed to involve a member or agent of al-Qa'ida or an affiliated terrorist organization; the collection of communications content under FISA section

[redacted]

702; and the fact that the NSA does not otherwise conduct a dragnet of content surveillance as the plaintiffs allege. Such facts include those concerning (a) how targets were selected under the TSP; (b) the specific methods used under the TSP to intercept telephone and Internet communications; (c) the nature and identity of the targets under the TSP [redacted] (d) any additional classified details about the operation of the TSP that would be necessary to litigate the plaintiffs' allegations (to the extent relevant) including facts concerning the operational swiftness and agility of the TSP, particularly in conjunction with metadata analysis; [redacted] and the effectiveness and success of the TSP; and (e) other NSA surveillance activities, including collection of communications content under FISA section 702, that may be needed to address and disprove the content dragnet allegations, [redacted] *See* Classified NSA Declaration. In my judgment, revealing or risking disclosure of the foregoing NSA intelligence activities, sources, and methods in order to show that the NSA is not conducting the "dragnet" on the content of communications that plaintiffs allege can be expected to cause exceptionally grave harm to national security by disclosing to our adversaries the ability of the United States to monitor and track their activities and communications.

66. (U) I also assert privilege over still-classified facts that would describe the scope or operational details of other NSA intelligence activities, including but not necessarily limited to metadata collection activities, that may relate to or be necessary to adjudicate plaintiffs' claims. *See* Classified NSA Declaration. In my judgment, the NSA is unable to disclose information about the scope or operation of the NSA's bulk collection or targeted analysis of Internet or telephony metadata (whether conducted under presidential or FISC authority), beyond that which

has already been officially acknowledged by the U.S. Government, without risking exceptionally grave harm to national security. Disclosing or confirming further details about those activities could seriously undermine an important tool—telephony metadata collection and analysis—for tracking possible terrorist plots; and could reveal methods by which NSA has targeted and continues to target its intelligence-gathering activities, thus helping foreign adversaries evade detection, and otherwise undermining ongoing intelligence operations conducted under E.O. 12333 and FISC authorization.

67. (S) In my judgment, disclosure of these still-classified details regarding these intelligence-gathering activities, either directly or indirectly, would seriously compromise, if not destroy, important and vital ongoing intelligence operations. I concur with the NSA that the activities discussed herein and described further in the Classified NSA Declaration have given the United States unparalleled ability to understand the interconnected groups and agents that al-Qa'ida has become, by allowing the NSA to identify and track terrorists as they move around the world and [redacted] After personal consideration of the matter, it is my judgment that disclosing the information described herein and by the NSA would compromise important and critical activities, sources, and methods, thereby helping our adversaries evade detection and causing exceptionally grave damage to the national security of the United States.

D. (U) Information That May Tend To Confirm or Deny Whether AT&T, Verizon, or any Other Telecommunications Carrier Has Provided Assistance To the NSA In Connection With Any Intelligence Activity.

68. (U) In addition, I am asserting privilege over information that may tend to confirm or deny whether or not AT&T, Verizon, or to the extent necessary, any other particular telecommunications provider, has assisted any NSA intelligence activity, including but not

necessarily limited to the alleged intelligence activities. The disclosure of any information that would tend to confirm or deny allegations of such assistance can be expected to cause exceptionally grave harm to the national security, for a variety of reasons.

69. (U) First, confirming or denying such allegations would reveal to foreign adversaries whether or not the NSA utilizes particular intelligence sources and methods and, thus, either compromise actual sources and methods or disclose that the NSA does not utilize a particular source or method. For example, revealing that a particular company assists the NSA would compromise a range of intelligence activities by providing confirmation that certain channels of communications are vulnerable to NSA interception. Confirmation or denial of a carrier's assistance would replace speculation with certainty for hostile foreign adversaries who are balancing the risk that a particular channel of communication may not be secure against the need to communicate efficiently.

70. (TS//STLW//SI OC/NF) Second,

~~TOP SECRET//STLW//SI//ORCON/NOFORN~~ [redacted] ~~HCS//TALENT KEYHOLE//~~

Classified NSA Declaration.[2]

71. ~~(TS//SI//NF)~~ [redacted]

72. ~~(TS//SI//NF)~~ I concur, therefore, with the NSA's conclusion that [redacted]

[2] ~~(TS//STLW/SI [redacted] OC/NF)~~ In addition, I have reviewed the classified certification of then-Attorney General Mukasey submitted to the Court pursuant to Section 802 of the FISA Act Amendments Act of 2008 and assert privilege over specific information described therein, including [redacted]

[redacted] And this, in turn, would seriously undermine the NSA's very ability to perform its mission effectively.

73. (TS/SI) All of this remains so, in my judgment, notwithstanding [redacted]

74. (TS//SI [redacted] OC/NF) For the foregoing reasons, in my judgment, [redacted]

[redacted] can be expected to cause exceptionally grave harm to the national security of the United States, and any information that would tend to [redacted] must be protected from disclosure in this case. Accordingly, I assert the state secrets and DNI statutory privilege over such information, including the information about [redacted] described in the Classified NSA Declaration.

(U) CONCLUSION

75. (U) In sum, I am asserting the state secrets privilege and the DNI's statutory privilege set forth in 50 U.S.C. § 3024(i)(1) to protect the classified national security information described herein and in the Classified NSA Declaration. I respectfully request that the Court not only protect that information from disclosure, but take all steps necessary to protect the intelligence information, sources, and methods described herein in order to prevent exceptionally grave damage to the national security of the United States.

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

Executed on: December 20, 2013

JAMES R. CLAPPER
Director of National Intelligence