

1 CINDY COHN (SBN 145997)
cindy@eff.org
2 LEE TIEN (SBN 148216)
3 KURT OPSAHL (SBN 191303)
4 JAMES S. TYRE (SBN 083117)
5 MARK RUMOLD (SBN 279060)
6 ANDREW CROCKER (SBN 291596)
7 ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
PAULA L. BLIZZARD (SBN 207920)
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Fax: (415) 397-7188

8 RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
9 LAW OFFICE OF RICHARD R. WIEBE
10 One California Street, Suite 900
11 San Francisco, CA 94111
12 Telephone: (415) 433-3200
13 Fax: (415) 433-6382

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
aram@eff.org
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

16 Attorneys for Plaintiffs

17 **UNITED STATES DISTRICT COURT**
18 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
19 **SAN FRANCISCO DIVISION**

20 CAROLYN JEWEL, TASH HEPTING,)
21 YOUNG BOON HICKS, as executrix of the)
22 estate of GREGORY HICKS, ERIK KNUTZEN)
23 and JOICE WALTON, on behalf of themselves)
24 and all others similarly situated,)
Plaintiffs,)
25 v.)
26 NATIONAL SECURITY AGENCY, *et al.*,)
27 Defendants.)

Case No.: 08-cv-4373-JSW

**DECLARATION OF MARK RUMOLD
FILED IN SUPPORT OF PLAINTIFFS'
RESPONSE TO DEFENDANTS' PUBLIC
FILINGS**

Courtroom 11, 19th Floor
The Honorable Jeffrey S. White

1 I, MARK RUMOLD, hereby declare,

2 1. I am an attorney of record for plaintiffs in this action and a member in good standing of
3 the California State Bar. I am admitted to practice before this Court. I have personal knowledge of
4 the matters stated in this declaration and if called upon to do so I am competent to testify to all
5 matters set forth herein.

6 2. Attached hereto as Exhibit 1 is a true and correct copy of the following document: Mem.
7 Op., *Redacted*, No. [Redacted] (FISC Sep. 25, 2012), *available at*
8 [http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.](http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf)
9 pdf.

10 3. The following is a true and correct transcription of an excerpt of a statement made by
11 Senator Diane Feinstein on September 26, 2013 during a hearing:

12 “Upstream collection . . . comprises about 10 percent of all collection that takes
13 place under 702, and occurs when NSA obtains Internet communications, such as e-
14 mails, from certain U.S. companies that operate the Internet backbone [*sic*]; *i.e.*,
15 the companies that own and operate the domestic telecommunication lines over
which Internet traffic flows.”

16 Hearing on FISA legislation before the S. Select Comm. on Intelligence, 113th Cong. (Sep. 26,
17 2013). Video available at C-SPAN: <http://www.c-spanvideo.org/clip/4466341>.

18 4. Attached hereto as Exhibit 2 is a true and correct copy of the following document:
19 Siobhan Gorman & Jennifer Valentino-Devries, *New Details Show Broader NSA Surveillance*
20 *Reach*, Wall. St. J. (Aug. 20, 2013), *available at*
21 <http://online.wsj.com/news/articles/SB10001424127887324108204579022874091732470>.

22 5. Attached hereto as Exhibit 3 is a true and correct copy of the following document: Joint
23 Statement From the Office of the Director of National Intelligence and the National Security
24 Agency (Aug. 21, 2013), *available at*
25 [http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_21_Joint_Statement_ODNI_](http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_21_Joint_Statement_ODNI_NSA.pdf)
26 NSA.pdf.

27 6. Attached hereto as Exhibit 4 is a true and correct copy of the following document:
28 Charlie Savage, *NSA Said to Search Content of Messages To and From U.S.*, N.Y. Times (Aug. 8,

1 2013), *available at* www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html.

3 7. Attached hereto as Exhibit 5 is a true and correct copy of the following document:
4 *Procedures Used by the National Security Agency for Targeting Non-United States Persons* (July
5 28, 2009). This document was obtained from the website of the Guardian newspaper, which
6 published it on June 20, 2013: [http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-](http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document)
7 [a-procedures-nsa-document](http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document).

8 8. Attached hereto as Exhibit 6 is a true and correct copy of the following document:
9 Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of*
10 *the Foreign Intelligence Surveillance Act* (June 8, 2013), *available at*
11 [http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20](http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf)
12 [Pursuant%20to%20Section%20702.pdf](http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf).

13 9. The following is a true and correct transcription of an excerpt of a statement made by
14 General Keith Alexander on September 26, 2013 during a hearing of the Senate Select Committee
15 on Intelligence: “NSA’s programs have contributed to understanding and disrupting 54 terror-
16 related events, 25 in Europe, 11 in Asia and five in Africa, and 13 in the United States.” Hearing on
17 FISA legislation before the S. Select Comm. on Intelligence, 113th Cong. (Sep. 26, 2013).
18 Transcript *available at* [http://icontherecord.tumblr.com/post/62359076197/remarks-as-delivered-](http://icontherecord.tumblr.com/post/62359076197/remarks-as-delivered-by-general-keith-alexander)
19 [by-general-keith-alexander](http://icontherecord.tumblr.com/post/62359076197/remarks-as-delivered-by-general-keith-alexander).

20 10. The following is a true and correct transcription of an excerpt of an exchange between
21 Senator Leahy and General Keith Alexander on October 2, 2013 during a hearing of the Senate
22 Select Committee on Judiciary:

23 SEN. LEAHY: [W]e’ve heard over and over again the assertion that 54 terrorist plots were
24 thwarted by the use of Section 215 and-or Section 702 authorities. That’s plainly wrong, but
25 we still get it in letters to members of Congress, we get it in statements. These weren’t all
26 plots and they weren’t all thwarted. The American people are getting left with the inaccurate
impression of the effectiveness of NSA programs.

27 Would you agree that the 54 cases that keep getting cited by the administration were not all
28 plots, and of the 54, only 13 had some nexus to the U.S., would you agree with that, yes or
no?

1 GEN. ALEXANDER: Yes.

2 SEN. LEAHY: OK. At our last hearing, Deputy Director Inglis' testimony stated that there's
3 only really one example of a case where "but for" the use of Section 215, both phone records
4 collection, terrorist activity was stopped. Is Mr. Inglis right?

5 GEN. ALEXANDER: He's right. I believe he said two, Chairman. I may have that wrong,
6 but I think he said two. And I would like to point out that it could only have applied in 13 of
7 the cases, because of the 54 terrorist plots or events, only 13 occurred in the U.S. Business
8 record FISA was only used in 12.

9 SEN. LEAHY: I understand that, but what I worry about is that some of the statements that
10 all is well, and we have these overstatements of what's going on. We're talking about
11 massive, massive, massive collection. We're told we have to do that to protect us, and then
12 statistics are rolled out. If they are not accurate, it doesn't help with the credibility here in the
13 Congress, doesn't help the credibility with this chairman, and doesn't help with the credibility
14 with the country.

15 Hearing on FISA oversight before the S. Comm. on the Judiciary, 113th Cong. (Oct 2, 2013).

16 Video *available at* [http://www.c-span.org/Events/Intel-Chiefs-Testify-at-Senate-FISA-Oversight-
17 Hearing/10737441809-1](http://www.c-span.org/Events/Intel-Chiefs-Testify-at-Senate-FISA-Oversight-Hearing/10737441809-1) (exchange occurs at approximately 42 minutes).

18 11. Attached hereto as Exhibit 7 is a true and correct copy of an excerpt of the following
19 document: President's Review Grp. on Intelligence and Commc'ns Tech., Liberty and Security in a
20 Changing World (Dec. 12, 2013) (pages 1-7, 94-104), *available at*
21 http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

22 12. The following is a true and correct transcription of an excerpt of a statement made by
23 General Keith Alexander on June 18, 2013 during a hearing of the House Permanent Select
24 Committee on Intelligence: "We couldn't connect the dots because we didn't have the dots."
25 Hearing on disclosure of National Security Agency surveillance programs before the H. Permanent
26 Select Comm. on Intelligence, 113th Cong. (Jun. 18, 2013). Transcript *available at*
27 [http://icontherecord.tumblr.com/post/57812486681/hearing-of-the-house-permanent-select-
28 committee-on](http://icontherecord.tumblr.com/post/57812486681/hearing-of-the-house-permanent-select-committee-on).

13. Attached hereto as Exhibit 8 is a true and correct copy of an excerpt of the following
document: Peter Bergen, *Would NSA Surveillance Have Stopped 9/11 Plot?*, CNN (Dec. 30, 2013),
available at <http://us.cnn.com/2013/12/30/opinion/bergen-nsa-surveillance-september-11>.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

14. Attached hereto as Exhibit 9 is a true and correct copy of an excerpt of the following document: Justin Elliot, *Judge on NSA Case Cites 9/11 Report, But It Doesn't Actually Support His Ruling*, ProPublica (Dec. 28, 2013), available at <http://www.propublica.org/article/fact-check-the-nsa-and-sept-11>.

15. Attached hereto as Exhibit 10 is a true and correct copy of an excerpt of the following document: Michael German, *No NSA Poster Child: The Real Story of 9/11 Hijacker Khalid al-Mihdhar*, Defense One (Oct. 16, 2013), available at <http://www.defenseone.com/ideas/2013/10/no-nsa-poster-child-real-story-911-hijacker-khalid-al-mihdhar>.

DATE: January 10, 2014

Respectfully submitted,

/s/ Mark Rumold

MARK RUMOLD

CINDY COHN

LEE TIEN

KURT OPSAHL

JAMES S. TYRE

ANDREW CROCKER

ELECTRONIC FRONTIER FOUNDATION

RICHARD R. WIEBE

LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III

ROYSE LAW FIRM, PC

RACHAEL E. MENY

PAULA L. BLIZZARD

MICHAEL S. KWUN

AUDREY WALTON-HADLOCK

BENJAMIN W. BERKOWITZ

KEKER & VAN NEST LLP

ARAM ANTARAMIAN

LAW OFFICE OF ARAM ANTARAMIAN

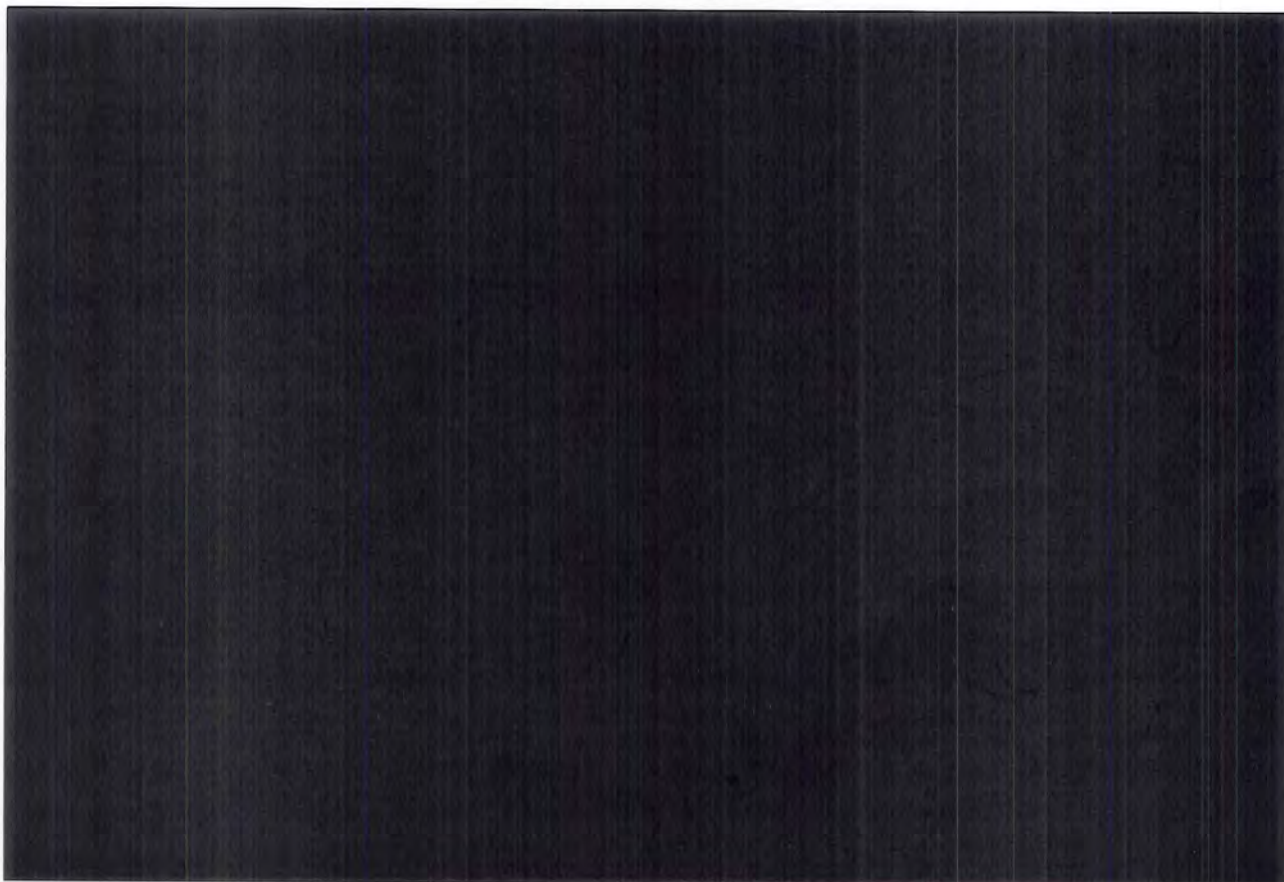
Attorneys for Plaintiffs

Exhibit 1

Exhibit 1

~~TOP SECRET//SI//ORCON,NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.



MEMORANDUM OPINION

This matter is before the Foreign Intelligence Surveillance Court (“FISC” or “Court”) on the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications,” which was filed on August 24, 2012

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

a. *The Scope of NSA's Upstream Collection.*

Last year, following the submission of Certifications [REDACTED] for renewal, the government made a series of submissions to the Court disclosing that it had materially misrepresented the scope of NSA's "upstream collection" under Section 702 (and prior authorities including the Protect America Act). The term "upstream collection" refers to the acquisition of Internet communications as they transit the "internet backbone" facilities of [REDACTED] as opposed to the collection of communications directly from Internet service providers like [REDACTED]. See Docket Nos. [REDACTED] [REDACTED] Oct. 3, 2011 Memorandum Opinion ("Oct. 3 Op.") at 5 n.3. Since 2006, the government had represented that NSA's upstream collection only acquired discrete communications to or from a facility tasked for acquisition and communications that referenced the tasked facility (so-called "about" communications). See *id.* at 15-16. With regard to the latter category, the government had repeatedly assured the Court that NSA only acquired [REDACTED] specific categories of "about" communications. *Id.*

The government's 2011 submissions made clear, however, that NSA's upstream collection was much broader than the government had previously represented. For the first time, the government explained that NSA's upstream collection results in the acquisition of "Internet transactions" instead of discrete communications to, from or about a tasked selector. See *id.* at 15. Internet transactions, the government would ultimately acknowledge, could and often do contain multiple discrete communications, including wholly domestic non-target communications and other non-target communications to, from, or concerning U.S. persons. *Id.*

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

While the government was able to show that the percentage of wholly domestic non-target communications and other non-target communications to, from, or concerning U.S. persons being acquired was small relative to the total volume of Internet communications acquired by the NSA pursuant to section 702, the acquisition of such communications nonetheless presented a significant issue for the Court in reviewing the procedures. In fact, it appeared that NSA was annually acquiring tens of thousands of Internet transactions containing at least one wholly domestic communication; that many of these wholly domestic communications were not to, from, or about a targeted facility; and that NSA was also likely annually acquiring tens of thousands of additional Internet transactions containing one or more non-target communications to or from U.S. persons or persons in the United States. Id. at 33, 37.

In the October 3 Opinion, the Court approved in large part Certifications [REDACTED] and the accompanying targeting and minimization procedures. The Court concluded, however, that one aspect of the proposed collection – NSA’s upstream collection of Internet transactions containing multiple communications, or “MCTs” – was, in some respects, deficient on statutory and constitutional grounds. The Court concluded that although NSA’s targeting procedures met the statutory requirements, the NSA minimization procedures, as the government proposed to apply them to MCTs, did not satisfy the statutory definition of “minimization procedures” with respect to retention. Oct. 3 Op. at 59-63. As applied to the upstream collection of Internet transactions, the Court found that the procedures were not reasonably designed to minimize the retention of U.S. person information consistent with the government’s national security needs. Id. at 62-63. The Court explained that the net effect of the

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

procedures would have been that thousands of wholly domestic communications, and thousands of other discrete communications that are not to or from a targeted selector but that are to, from, or concerning United States persons, would be retained by NSA for at least five years, despite the fact that they have no direct connection to a targeted selector and, therefore, were unlikely to contain foreign intelligence information. Id. at 60-61. For the same reason, the Court concluded that NSA's procedures, as the government proposed to apply then to MCTs, failed to satisfy the requirements of the Fourth Amendment. Id. at 78-79. The Court noted that the government might be able to remedy the deficiencies that it had identified, either by tailoring its upstream acquisition or by adopting more stringent post-acquisition safeguards. Id. at 61-62, 79.

By operation of the statute, the government was permitted to continue the problematic portion of its collection for 30 days while taking steps to remedy the deficiencies identified in the October 3 order and opinion. See 50 U.S.C. § 1881a(i)(3)(B). In late October of 2011, the government timely submitted amended NSA minimization procedures that included additional provisions regarding NSA's upstream collection. The amended procedures, which took effect on October 31, 2011 ("Oct. 31, 2011 NSA Minimization Procedures"), require NSA to restrict access to the portions of its ongoing upstream collection that are most likely to contain wholly domestic communications and non-target information that is subject to statutory or Fourth Amendment protection. See Nov. 30 Op. at 7-9. Segregated Internet transactions can be moved to NSA's general repositories only after having been determined by a specially trained analyst not to contain a wholly domestic communication. Id. at 8. Any transaction containing a wholly domestic communication (whether segregated or not) would be purged upon recognition. Id. at

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

8, 9. Any transaction moved from segregation to NSA's general repositories would be permanently marked as having previously been segregated. Id. at 8. On the non-segregated side, any discrete communication within an Internet transaction that an analyst wishes to use is subject to additional checks. Id. at 8-10. NSA is not permitted to use any discrete, non-target communication that is determined to be to or from a U.S. person or a person who appears to be in the United States, other than to protect against an immediate threat to human life. Id. at 9. Finally, all upstream acquisitions are retained for a default maximum period of two, rather than five, years. Id. at 10-11.

The Court concluded in the November 30 Opinion that the October 31, 2011 NSA Minimization Procedures adequately remedied the deficiencies that had been identified in the October 3 opinion. Id. at 14-15. Accordingly, NSA was able to continue its upstream collection of Internet transactions (including MCTs) without interruption, but pursuant to amended procedures that are consistent with statutory and constitutional requirements.

However, issues remained with respect to the past upstream collection residing in NSA's databases. Because NSA's upstream collection almost certainly included at least some acquisitions constituting "electronic surveillance" within the meaning of 50 U.S.C. § 1801(f), any overcollection resulting from the government's misrepresentation of the scope of that collection implicates 50 U.S.C. § 1809(a)(2). Section 1809(a)(2) makes it a crime to "disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. The Court therefore directed the government to make a written submission addressing

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

the applicability of Section 1809(a), which the government did on November 22, 2011. See [REDACTED], Oct. 13, 2011 Briefing Order, and Government's Response to the Court's Briefing Order of Oct. 13, 2011 (arguing that Section 1809(a)(2) does not apply).

Beginning late in 2011, the government began taking steps that had the effect of mitigating any Section 1809(a)(2) problem, including the risk that information subject to the statutory criminal prohibition might be used or disclosed in an application filed before this Court. The government informed the Court in October 2011 that although the amended NSA procedures do not by their terms apply to information acquired before October 31, NSA would apply portions of the procedures to the past upstream collection, including certain limitations on the use or disclosure of such information. See Nov. 30 Opinion at 20-21. Although it was not technically feasible for NSA to segregate the past upstream collection in the same way it is now segregating the incoming upstream acquisitions, the government explained that it would apply the remaining components of the amended procedures approved by the Court to the previously-collected data, including (1) the prohibition on using discrete, non-target communications determined to be to or from a U.S. person or a person in the United States, and (2) the two-year age-off requirement. See id. at 21.

Thereafter, in April 2012, the government orally informed the Court that NSA had made a "corporate decision" to purge all data in its repositories that can be identified as having been acquired through upstream collection before the October 31, 2011 effective date of the amended NSA minimization procedures approved by the Court in the November 30 Opinion. NSA's

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

effort to purge that information, to the extent it is reasonably feasible to do so, is now complete. See Aug. 24 Submission at 9-10.¹⁷

Finally, NSA has adopted measures to deal with the possibility that it has issued reports based on upstream collection that was unauthorized. NSA has identified [REDACTED] reports that were issued from the inception of its collection under Section 702 to October 31, 2011, that rely at least in part on information derived from NSA's upstream acquisitions from that period. See Sept. 12, 2012 Supplement to the Government's Ex Parte Submission of Reauthorization Certifications at 2 ("Sept. 12 Submission"). The government advises that, of the [REDACTED] reports, [REDACTED] have been confirmed to be based entirely upon communications that are to, from or about persons properly targeted under Section 702 and therefore present no issue under Section 1809(a)(2). See id. The government is unable to make similar assurances, however, regarding the remaining [REDACTED] reports. Accordingly, NSA will direct the recipients of those [REDACTED] reports (both within NSA and outside the agency) not to further use or disseminate information contained therein without first obtaining NSA's express approval. Id. at 3-4. Upon receipt of such a request, NSA will review the relevant report to determine whether continued use thereof is

¹⁷ The government has informed the Court that NSA stores some of the past upstream collection in repositories in which it may no longer be identifiable as such. [REDACTED]

[REDACTED] See Aug. 24 Submission at 14-16. Assuming that NSA cannot with reasonable effort identify information in its repositories as the fruit of an unauthorized electronic surveillance, such information falls outside the scope of Section 1809(a)(2), which by its terms applies only when there is knowledge or "reason to know that the information was obtained through electronic surveillance not authorized" by statute.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

appropriate. Id. at 4.¹⁸ Finally, the government has informed the Court that it will not use any report that cites to upstream collection acquired prior to October 31, 2011 in an application to this Court absent express notice to, and approval of, the Court. Aug. 24 Submission at 24.

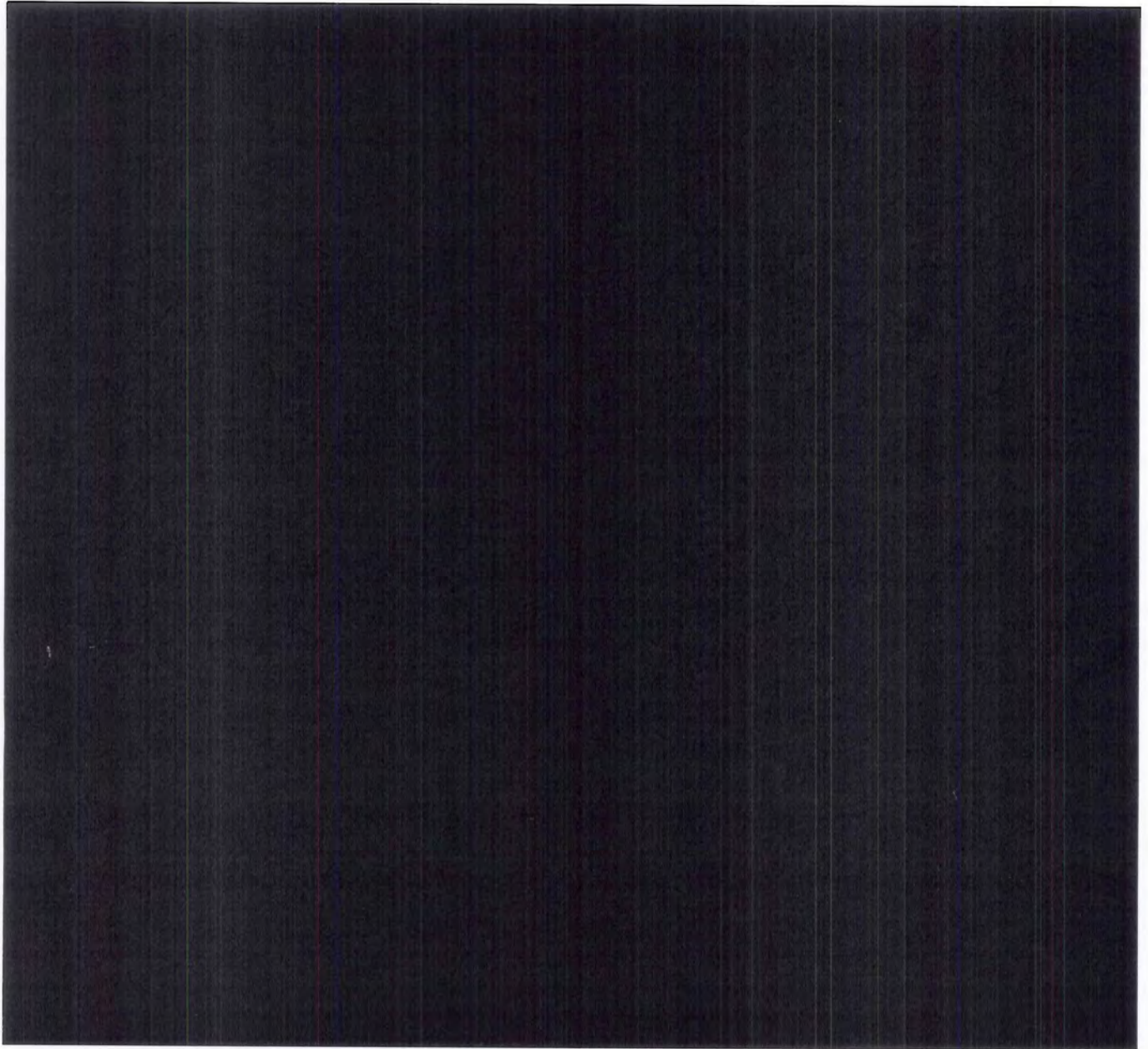
Taken together, the remedial steps taken by the government since October 2011 greatly reduce the risk that NSA will run afoul of Section 1809(a)(2) in its handling of the past upstream acquisitions made under color of Section 702. NSA's self-imposed prohibition on using non-target communications to or from a U.S. person or a person in the United States helped to ensure that the fruits of unauthorized electronic surveillance were not used or disclosed while it was working to purge the pre-October 31, 2011 upstream collection. And NSA's subsequent purge of that collection from its repositories and the above-described measures it has taken with respect to derivative reports further reduce the risk of a problem under Section 1809(a)(2). Finally, the amended NSA minimization procedures provide that in the event, despite NSA's effort to purge the prior upstream collection, the agency discovers an Internet transaction acquired before October 31, 2011, such transaction must be purged upon recognition. See Amended NSA Minimization Procedures at 8 § 3(c)(3). In light of the foregoing, it appears to the Court that the outstanding issues raised by NSA's upstream collection of Internet transactions have been resolved, subject to the discussion of changes to the minimization procedures that appears

¹⁸ For instance, NSA may determine that the report is fully supported by cited communications other than the ones obtained through upstream communication. Sept. 12 Submission at 4. In other instances, NSA may revise the report so that it no longer relies upon upstream communications and reissue it. Id. If such steps are not feasible because the report cannot be supported without the upstream communication, NSA will cancel the report. Id.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

below.¹⁹



¹⁹ Under the circumstances, the Court finds it unnecessary to further address the arguments advanced by the government in its November 22, 2011 response to the Court's October 13, 2011 briefing order regarding Section 1809(a), particularly those regarding the scope of prior Section 702 authorizations.

~~TOP SECRET//SI//ORCON,NOFORN~~

Exhibit 2

Exhibit 2

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

- [See a sample reprint in PDF format:](#)
- [Order a reprint of this article now](#)

U.S. NEWS

New Details Show Broader NSA Surveillance Reach

Programs Cover 75% of Nation's Traffic, Can Snare Emails

By SIOBHAN GORMAN and JENNIFER VALENTINO-DEVRIES

Updated Aug. 20, 2013 11:31 p.m. ET

WASHINGTON—The National Security Agency—which possesses only limited legal authority to spy on U.S. citizens—has built a surveillance network that covers more Americans' Internet communications than officials have publicly disclosed, current and former officials say.

The system has the capacity to reach roughly 75% of all U.S. Internet traffic in the hunt for foreign intelligence, including a wide array of communications by foreigners and Americans. In some cases, it retains the written content of emails sent between citizens within the U.S. and also filters domestic phone calls made with Internet technology, these people say.

The NSA's filtering, carried out with telecom companies, is designed to look for communications that either originate or end abroad, or are entirely foreign but happen to be passing through the U.S. But officials say the system's broad reach makes it more likely that purely domestic communications will be incidentally intercepted and collected in the hunt for foreign ones.

The NSA's surveillance network covers more Americans' Internet communications than officials have publicly disclosed, reaching roughly 75 percent of all U.S. internet traffic. Siobhan Gorman reports on the News Hub. Photo: Getty Images.

The programs, code-named Blarney, Fairview, Oakstar, Lithium and Stormbrew, among others, filter and gather information at major telecommunications companies. Blarney, for instance, was established with AT&T Inc., former officials say. AT&T declined to comment.

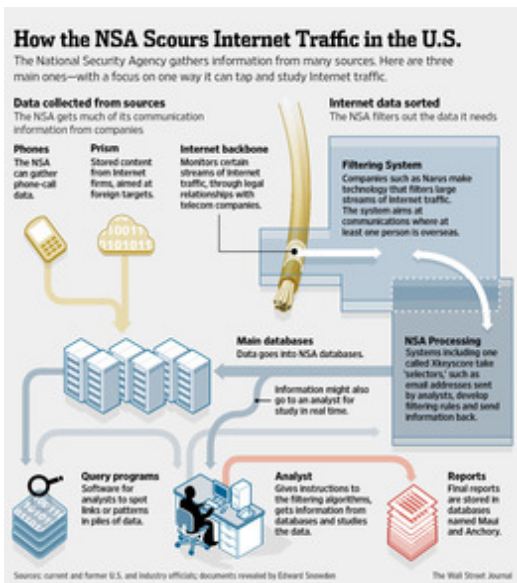
Q&A

[What You Need to Know on the New Details of NSA Spying](#)

How the NSA Scours Internet Traffic in the U.S.

This filtering takes place at more than a dozen locations at major Internet junctions in the U.S., officials say. Previously, any NSA filtering of this kind was largely believed to be happening near points where undersea or other foreign cables enter the country.

Details of these surveillance programs were gathered from interviews with current and former intelligence and government officials and people from companies that help



build or operate the systems, or provide data. Most have direct knowledge of the work.

The NSA defends its practices as legal and respectful of Americans' privacy. According to NSA spokeswoman Vanee Vines, if American communications are "incidentally collected during NSA's lawful signals intelligence activities," the agency follows "minimization procedures that are approved by the U.S. attorney general and designed to protect the privacy of United States persons."

As another U.S. official puts it, the NSA is "not wallowing willy-nilly" through Americans' idle online chatter. "We want high-grade ore."

To achieve that, the programs use complex algorithms that, in effect, operate like filters placed over a stream with holes designed to let certain pieces of information flow through. After the 2001 terrorist attacks, NSA widened the holes to capture more information when the government broadened its definition of what constitutes "reasonable" collection, according to a former top intelligence official.

The NSA's U.S. programs have been described in narrower terms in the documents released by former NSA contractor [Edward Snowden](#). One, for instance, acquires Americans' phone records; another, called Prism, makes requests for stored data to Internet companies. By contrast, this set of programs shows the NSA has the capability to track almost anything that happens online, so long as it is covered by a broad court order.

The NSA programs are approved and overseen by the secret Foreign Intelligence Surveillance Court. NSA is required to destroy information on Americans that doesn't fall under exceptions to the rule, including information that is relevant to foreign intelligence, encrypted, or evidence of a crime.

The NSA is focused on collecting foreign intelligence, but the streams of data it monitors include both foreign and domestic communications. Inevitably, officials say, some U.S. Internet communications are scanned and intercepted, including both "metadata" about communications, such as the "to" and "from" lines in an email, and the contents of the communications themselves.

Much, but not all, of the data is discarded, meaning some communications between Americans are stored in the NSA's databases, officials say. Some lawmakers and civil

WSJ: Privacy Insights >

The Wall Street Journal is conducting a long-running investigation into the profound transformation of personal privacy in America.

Selected findings:

The Wall Street Journal **reconstructs the clash over the counterterrorism program** within the administration of President Barack Obama. (10/13/12)

Companies today are **increasingly tying people's real-life identities** to their online browsing habits. (12/7/12)

Two students are outed as gay—provoking a crisis within their families—by **a Facebook privacy loophole**. (10/12/12)

Suspicious spouses are **taking investigations into their own hands** as snooping technologies become cheaper and easier to use. (10/6/12)

Americans' license plates are now being tracked **not only by the government, but also by repo men** who hope to profit from the information. (10/2/12)

Google bypassed the privacy settings on millions of Web browsers on Apple iPhones and computers—**tracking the online activities** of people who intended that kind of monitoring to be blocked. (2/17/12)

The government follows the movements of thousands of Americans a year by **secretly monitoring their cellphone records**. (9/9/11)

iPhone and Android apps **secretly shared data** about their users, a Journal investigation found. (12/10/10)

Top apps on Facebook **transmit personal identifying details** to tracking companies, a Journal investigation found. (10/18/10)

Plus, the global **surveillance bazaar**, a secretive **phone-tracking "stingray"** and RapLeaf's clever way of figuring out Web surfers' **real names**.

[See full privacy coverage](#)

Audio

Siobhan Gorman has more with The Wall Street Journal This Morning.

00:00 |
05:06

libertarians say that, given the volumes of data NSA is examining, privacy protections are insufficient.

Sen. Ron Wyden, an Oregon Democrat, in 2012 sought but failed to prohibit the agency from searching its databases for information on Americans without a warrant. He has also pushed intelligence agencies to detail how many Americans' communications have been collected and to explain whether purely domestic communications are retained in NSA's databanks. They have declined.

"Technology is moving us swiftly into a world where the only barriers to this kind of dragnet surveillance are the protections enshrined into law," Mr. Wyden says.

This month President Barack Obama proposed changes to NSA surveillance to improve oversight. Those proposed changes wouldn't alter the systems in the U.S. that NSA relies upon for some of its most sensitive surveillance.

The systems operate like this: The NSA asks telecom companies to send it various streams of Internet traffic it believes most likely to contain foreign intelligence. This is the first cut of the data.

These requests don't ask for all Internet traffic. Rather, they focus on certain areas of interest, according to a person familiar with the legal process. "It's still a large amount of data, but not everything in the world," this person says.

The second cut is done by NSA. It briefly copies the traffic and decides which communications to keep based on what it calls "strong selectors"—say, an email address, or a large block of computer addresses that correspond to an organization it is interested in. In making these decisions, the NSA can look at content of communications as well as information about who is sending the data.

One U.S. official says the agency doesn't itself "access" all the traffic within the surveillance system. The agency defines access as "things we actually touch," this person says, pointing out that the telecom companies do the first stage of filtering.

The surveillance system is built on relationships with telecommunications carriers that together cover about 75% of U.S. Internet communications. They must hand over what the NSA asks for under orders from the secret Foreign Intelligence Surveillance Court. The firms search Internet traffic based on the NSA's criteria, current and former officials say.

Verizon Communications Inc., for example, has placed intercepts in the largest U.S. metropolitan areas, according to one person familiar with the technology. It isn't clear how much information these intercepts send to the NSA. A Verizon spokesman declined to comment.

Not all telecommunications providers handle the government demands the same way, says the person familiar with the legal process. According to a U.S. official, lawyers at telecom companies serve as checks on what the NSA receives. "The providers are independently deciding what would be responsive," the official says.

Lawyers for at least one major provider have taken the view that they will provide access only to "clearly foreign" streams of data—for example, ones involving connections to ISPs in, say, Mexico, according to the

person familiar with the legal process. The complexities of Internet routing mean it isn't always easy to isolate foreign traffic, but the goal is "to prevent traffic from Kansas City to San Francisco from ending up" with the NSA, the person says.

At times, the NSA has asked for access to data streams that are more likely to include domestic communications, this person says, and "it has caused friction." This person added that government officials have said some providers do indeed comply with requests like this.

The person says talks between the government and different telecoms about what constitutes foreign communications have "been going on for some years," and that some in the industry believe the law is unclear on Internet traffic. "Somebody should enunciate a rule," this person says.

Intelligence officials and the White House argue NSA's surveillance provides early warnings of terror threats that don't respect geographic boundaries. "It's true we have significant capabilities," Mr. Obama said in his NSA remarks last week. "What's also true is we show a restraint that many governments around the world don't even think to do."

Mr. Obama and top intelligence officials say NSA's programs are overseen by all three branches of government, citing procedures approved by the secret surveillance court that require the NSA to eliminate "incidentally acquired" data on Americans. "If you say, 'We don't want the NSA to be scanning large amounts of traffic,' you're saying you don't want it to do its job," says one former official.

Blarney, Fairview, Oakstar, Lithium and Stormbrew were mentioned, but not fully explained, in documents released by Mr. Snowden. An NSA paper released this month mentioned several but didn't describe them beyond saying, "The government compels one or more providers to assist NSA with the collection of information responsive to the foreign intelligence need."

The system is built with gear made by Boeing Co. 's Narus subsidiary, which makes filtering technology, and Internet hardware manufacturers Cisco Systems Inc. and Juniper Networks Inc., among other companies, according to former intelligence officials and industry figures familiar with the equipment.

Narus didn't respond to requests for comment. Cisco and Juniper declined to comment.

The NSA started setting up Internet intercepts well before 2001, former intelligence officials say. Run by NSA's secretive Special Services Office, these types of programs were at first designed to intercept communications overseas through arrangements with foreign Internet providers, the former officials say. NSA still has such arrangements in many countries, particularly in the Middle East and Europe, the former officials say.

Within NSA, former officials say, intelligence officers joked that the Blarney intercept program with AT&T was named in homage to the NSA program Shamrock, which intercepted telegraphic messages into and out of the U.S. and was an inspiration for the 1978 Foreign Intelligence Surveillance Act, which created the secret national-security court and placed intelligence activities under its supervision.

Blarney was in use before the 2001 terror attacks, operating at or near key fiber-optic landing points in the U.S. to capture foreign communications coming in and out of the country. One example is an AT&T facility in San Francisco that was revealed in 2006 during the debate over warrantless wiretapping. A similar facility was built at an AT&T site in New Jersey, former officials say.

After the 2001 attacks, a former official says, these intercept systems were expanded to include key Internet

networks within the U.S. through partnerships with U.S. Internet backbone providers. Amid fears of terrorist "sleeper cells" inside the U.S., the government under President George W. Bush also began redefining how much domestic data it could collect.

For the 2002 Winter Olympics in Salt Lake City, officials say, the Federal Bureau of Investigation and NSA arranged with Qwest Communications International Inc. to use intercept equipment for a period of less than six months around the time of the event. It monitored the content of all email and text communications in the Salt Lake City area.

At that point, the systems fed into the Bush administration's program of warrantless wiretapping, which circumvented the surveillance court on the authority of the president's power as commander in chief. The Bush administration came under criticism from lawmakers and civil libertarians for sidestepping court supervision.

The current legal backing for Blarney and its related programs stems from a section of a 2008 surveillance law. It permits the government, for foreign intelligence investigations, to snoop on foreigners "reasonably believed" to be outside the U.S.

Previously, the law had tighter standards. It allowed the government to spy on people if there were "probable cause" to believe they were an "agent of a foreign power."

NSA has discretion on setting its filters, and the system relies significantly on self-policing. This can result in improper collection that continues for years.

For example, a recent Snowden document showed that the surveillance court ruled that the NSA had set up an unconstitutional collection effort. Officials say it was an unintentional mistake made in 2008 when it set filters on programs like these that monitor Internet traffic; NSA uncovered the inappropriate filtering in 2011 and reported it.

"NSA's foreign intelligence collection activities are continually audited and overseen internally and externally," Ms. Vines says. "When we make a mistake in carrying out our foreign intelligence mission, we report the issue internally and to federal overseers and aggressively get to the bottom of it."

Another Snowden document describes the procedures NSA uses to protect American information that is retained. Any such information is "minimized," meaning that it is destroyed. The document highlights several exceptions, including encrypted communications and information of foreign intelligence significance.

Officials acknowledged some purely domestic communications are incidentally swept into the system. "We don't keep track of numbers of U.S. persons," a U.S. official says. "What we try to do is minimize any exposure."

When searching the data, intelligence officials say they are permitted to look only for information related to a "foreign intelligence interest." In practice, the NSA has latitude under that standard, and an American's communication could be read without a warrant, another U.S. official says.

Paul Kouroupas, a former executive at Global Crossing Ltd. and other telecom companies responsible for security and government affairs, says the checks and balances in the NSA programs depend on telecommunications companies and the government policing the system themselves. "There's technically and physically nothing preventing a much broader surveillance," he says.

An official at Global Crossing's parent, Level 3 Communications Inc., says the company complies with laws requiring it to assist government investigations and declined to disclose the assistance provided.

It is difficult to know how much domestic data NSA is inadvertently retaining. The filtering technology relies on algorithms to seek out valuable communications. A U.S. official says analysts guide the use of these algorithms to make them as precise as possible.

—Devlin Barrett contributed to this article.

Write to Siobhan Gorman at siobhan.gorman@wsj.com and Jennifer Valentino-DeVries at Jennifer.Valentino-DeVries@wsj.com

Copyright 2013 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

Exhibit 3

Exhibit 3

Joint Statement from the Office of the Director of National Intelligence and the National Security Agency

21 August 2013

Press reports based on an article published in today's Wall Street Journal mischaracterize aspects of NSA's data collection activities conducted under Section 702 of the Foreign Intelligence Surveillance Act. The NSA does not sift through and have unfettered access to 75% of the United States' online communications.

The following are the facts:

- Media reports based upon the recent Wall Street Journal (WSJ) article regarding NSA's foreign intelligence activities provide an inaccurate and misleading picture of NSA's collection programs, but especially with respect to NSA's use of Section 702 of the Foreign Intelligence Surveillance Act (FISA).
- The reports leave readers with the impression that NSA is sifting through as much as 75% of the United States' online communications, which is simply not true.
- In its foreign intelligence mission, and using all its authorities, NSA "touches" about 1.6%, and analysts only look at 0.00004%, of the world's internet traffic.
- The assistance from the providers, which is compelled by the law, is the same activity that has been previously revealed as part of Section 702 collection and PRISM.
- FISA is designed to allow the U.S. Government to acquire foreign intelligence while protecting the civil liberties and privacy of Americans.
 - Section 702 specifically prohibits the intentional acquisition of any communications when all parties are known to be inside the U.S.
 - The law specifically prohibits targeting a U.S. citizen without an individual court order based on a showing of probable cause.
 - The law only permits NSA to obtain information pursuant to Section 702 in accordance with orders and procedures approved by the Foreign Intelligence Surveillance Court.
- When conducting 702 FISA surveillance, the only information NSA obtains results from the use of specific identifiers (for example email addresses and telephone numbers) used by non-U.S. persons overseas who are believed to possess or receive foreign intelligence information.
 - Foreign terrorists sometimes communicate with persons in the U.S. or Americans overseas. In targeting a terrorist overseas who is not a U.S. person, NSA may get both sides of a communication. If that communication involves a U.S. person, NSA must follow Attorney General

and FISA Court approved “minimization procedures” to ensure the Agency protects the privacy of U.S. persons.

- The collection under FISA section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world.

Exhibit 4

Exhibit 4

The New York Times

August 8, 2013

N.S.A. Said to Search Content of Messages to and From U.S.

By CHARLIE SAVAGE

WASHINGTON — The [National Security Agency](#) is searching the contents of vast amounts of Americans' e-mail and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance, according to intelligence officials.

The N.S.A. is not just intercepting the communications of Americans who are in direct contact with foreigners targeted overseas, a practice that government officials have openly acknowledged. It is also casting a far wider net for people who cite information linked to those foreigners, like a little used e-mail address, according to a senior intelligence official.

While it has long been known that the agency conducts extensive computer searches of data it vacuums up overseas, that it is systematically searching — without warrants — through the contents of Americans' communications that cross the border reveals more about the scale of its secret operations.

It also adds another element to the unfolding debate, provoked by the disclosures of Edward J. Snowden, the former N.S.A. contractor, about whether the agency has infringed on Americans' privacy as it scoops up e-mails and phone data in its quest to ferret out foreign intelligence.

Government officials say the cross-border surveillance was authorized by a 2008 law, the FISA Amendments Act, in which Congress approved eavesdropping on domestic soil without warrants as long as the "target" was a noncitizen abroad. Voice communications are not included in that surveillance, the senior official said.

Asked to comment, Judith A. Emmel, an N.S.A. spokeswoman, did not directly address surveillance of cross-border communications. But she said the agency's activities were lawful and intended to gather intelligence not about Americans but about "foreign powers and their agents, foreign organizations, foreign persons or international terrorists."

"In carrying out its signals intelligence mission, N.S.A. collects only what it is explicitly

authorized to collect,” she said. “Moreover, the agency’s activities are deployed only in response to requirements for information to protect the country and its interests.”

Hints of the surveillance appeared in a [set of rules](#), leaked by Mr. Snowden, for how the N.S.A. may carry out the 2008 FISA law. One paragraph mentions that the agency “seeks to acquire communications about the target that are not to or from the target.” The pages were [posted online by the newspaper The Guardian on June 20](#), but the telltale paragraph, the only rule marked “Top Secret” amid 18 pages of restrictions, went largely overlooked amid other disclosures.

To conduct the surveillance, the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border. The senior intelligence official, who, like other former and current government officials, spoke on condition of anonymity because of the sensitivity of the topic, said the N.S.A. makes a “clone of selected communication links” to gather the communications, but declined to specify details, like the volume of the data that passes through them.

Computer scientists said that it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data; fiber-optic networks work by breaking messages into tiny packets that flow at the speed of light over different pathways to their shared destination, so they would need to be captured and reassembled.

The official said that a computer searches the data for the identifying keywords or other “selectors” and stores those that match so that human analysts could later examine them. The remaining communications, the official said, are deleted; the entire process takes “a small number of seconds,” and the system has no ability to perform “retrospective searching.”

The official said the keyword and other terms were “very precise” to minimize the number of innocent American communications that were flagged by the program. At the same time, the official acknowledged that there had been times when changes by telecommunications providers or in the technology had led to inadvertent overcollection. The N.S.A. monitors for these problems, fixes them and reports such incidents to its overseers in the government, the official said.

The disclosure sheds additional light on statements intelligence officials have made

recently, reassuring the public that they do not “target” Americans for surveillance without warrants.

At a House Intelligence Committee oversight hearing in June, for example, a lawmaker pressed the deputy director of the N.S.A., John Inglis, to say whether the agency listened to the phone calls or read the e-mails and text messages of American citizens. Mr. Inglis replied, “We do not target the content of U.S. person communications without a specific warrant anywhere on the earth.”

Timothy Edgar, a former intelligence official in the Bush and Obama administrations, said that the rule concerning collection “about” a person targeted for surveillance rather than directed at that person had provoked significant internal discussion.

“There is an ambiguity in the law about what it means to ‘target’ someone,” Mr. Edgar, now a visiting professor at Brown, said. “You can never intentionally target someone inside the United States. Those are the words we were looking at. We were most concerned about making sure the procedures only target communications that have one party outside the United States.”

The rule they ended up writing, which was secretly approved by the Foreign Intelligence Surveillance Court, says that the N.S.A. must ensure that one of the participants in any conversation that is acquired when it is searching for conversations about a targeted foreigner must be outside the United States, so that the surveillance is technically directed at the foreign end.

Americans’ communications singled out for further analysis are handled in accordance with “minimization” rules to protect privacy approved by the surveillance court. If private information is not relevant to understanding foreign intelligence, it is deleted; if it is relevant, the agency can retain it and disseminate it to other agencies, the rules show.

While the paragraph hinting at the surveillance has attracted little attention, the American Civil Liberties Union did take note of the “about the target” language in a [June 21 post](#) analyzing the larger set of rules, arguing that the language could be interpreted as allowing “bulk” collection of international communications, including of those of Americans.

Jameel Jaffer, a senior lawyer at the A.C.L.U., said Wednesday that such “dragnet surveillance will be poisonous to the freedoms of inquiry and association” because people who know that their communications will be searched will change their behavior.

“They’ll hesitate before visiting controversial Web sites, discussing controversial topics or investigating politically sensitive questions,” Mr. Jaffer said. “Individually, these hesitations might appear to be inconsequential, but the accumulation of them over time will change citizens’ relationship to one another and to the government.”

The senior intelligence official argued, however, that it would be inaccurate to portray the N.S.A. as engaging in “bulk collection” of the contents of communications. “ ‘Bulk collection’ is when we collect and retain for some period of time that lets us do retrospective analysis,” the official said. “In this case, we do not do that, so we do not consider this ‘bulk collection.’ ”

Stewart Baker, a former general counsel for the N.S.A., said that such surveillance could be valuable in identifying previously unknown terrorists or spies inside the United States who unwittingly reveal themselves to the agency by discussing a foreign-intelligence “indicator.” He cited a situation in which officials learn that Al Qaeda was planning to use a particular phone number on the day of an attack.

“If someone is sending that number out, chances are they are on the inside of the plot, and I want to find the people who are on the inside of the plot,” he said.

The senior intelligence official said that the “about the target” surveillance had been valuable, but said it was difficult to point to any particular terrorist plot that would have been carried out if the surveillance had not taken place. He said it was one tool among many used to assemble a “mosaic” of information in such investigations. The surveillance was used for other types of foreign-intelligence collection, not just terrorism investigations, the official said.

There has been no public disclosure of any ruling by the Foreign Intelligence Surveillance Court explaining its legal analysis of the 2008 FISA law and the Fourth Amendment as allowing “about the target” searches of Americans’ cross-border communications. But in 2009, the Justice Department’s Office of Legal Counsel signed off on a similar process for searching federal employees’ communications without a warrant to make sure none contain malicious computer code.

That opinion, by Steven G. Bradbury, who led the office in the Bush administration, may echo the still-secret legal analysis. He wrote that because that system, called **EINSTEIN 2.0**, scanned communications traffic “only for particular malicious computer code” and there was no authorization to acquire the content for unrelated purposes, it “imposes, at worst, a

minimal burden upon legitimate privacy rights.”

Exhibit 5

Exhibit 5

TOP SECRET//COMINT//NOFORN//20320108

EXHIBIT A

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING
NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED
OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE
INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE
SURVEILLANCE ACT OF 1978, AS AMENDED

2009 JUL 29 PM 3:14
CLERK OF COURT

(S) These procedures address: (I) the manner in which the National Security Agency/Central Security Service (NSA) will determine that a person targeted under section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), is a non-United States person reasonably believed to be located outside the United States ("foreignness determination"); (II) the post-targeting analysis done by NSA to ensure that the targeting of such person does not intentionally target a person known at the time of acquisition to be located in the United States and does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States; (III) the documentation of NSA's foreignness determination; (IV) compliance and oversight; and (V) departures from these procedures.

I. (U) DETERMINATION OF WHETHER THE ACQUISITION TARGETS NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES

(S) NSA determines whether a person is a non-United States person reasonably believed to be outside the United States in light of the totality of the circumstances based on the information available with respect to that person, including information concerning the communications facility or facilities used by that person.

(S) NSA analysts examine the following three categories of information, as appropriate under the circumstances, to make the above determination: (1) they examine the lead information they have received regarding the potential target or the facility that has generated interest in conducting surveillance to determine what that lead information discloses about the person's location; (2) they conduct research in NSA databases, available reports and collateral information (i.e., information to which NSA has access but did not originate, such as reports from other agencies and publicly available information) to determine whether NSA knows the location of the person, or knows information that would provide evidence concerning that location; and (3) they conduct technical analyses of the facility or facilities to determine or verify information about the person's location. NSA may use information from any one or a combination of these categories of information in evaluating the totality of the circumstances to determine that the potential target is located outside the United States.

(TS//SI) In addition, in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

overseas, or it will target Internet links that terminate in a foreign country. In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.

(S) Lead Information

(S) When NSA proposes to direct surveillance at a target, it does so because NSA has already learned something about the target or the facility or facilities the target uses to communicate. Accordingly, NSA will examine the lead information to determine what it reveals about the physical location of the target, including the location of the facility or facilities being used by the potential target.

(S) The following are examples of the types of lead information that NSA may examine:

- a) Has the target stated that he is located outside the United States? For example, has NSA or another intelligence agency collected a statement or statements made by the target indicating that he is located outside the United States?
- b) Has a human intelligence source or other source of lead information indicated that the target is located outside the United States?
- c) Does the lead information provided by an intelligence or law enforcement agency of the United States government or an intelligence or law enforcement service of a foreign government indicate that the target is located outside the United States?
- d) Was the lead information about the target found on a hard drive or other medium that was seized in a foreign country?
- e) With whom has the target had direct contact, and what do we know about the location of such persons? For example, if lead information indicates the target is in direct contact with several members of a foreign-based terrorist organization or foreign-based political organization who themselves are located overseas, that may suggest, depending on the totality of the circumstances, that the target is also located overseas.

(S) Information NSA Has About the Target's Location and/or Facility or Facilities Used by the Target

(S) NSA may also review information in its databases, including repositories of information collected by NSA and by other intelligence agencies, as well as publicly available information, to determine if the person's location, or information providing evidence about the person's location, is already known. The NSA databases that would be used for this purpose contain information culled from signals intelligence, human intelligence, law enforcement information, and other sources. For example, NSA databases may include a report produced by the Central Intelligence Agency (CIA) with the fact that a known terrorist is using a telephone with a particular number, or detailed information on worldwide telephony numbering plans for wire and wireless telephone systems.

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

(S) NSA Technical Analysis of the Facility

(S) NSA may also apply technical analysis concerning the facility from which it intends to acquire foreign intelligence information to assist it in making determinations concerning the location of the person at whom NSA intends to direct surveillance. For example, NSA may examine the following types of information:

(S) For telephone numbers:

- a) Identify the country code of the telephone number, and determine what it indicates about the person's location.
- b) Review commercially available and NSA telephone numbering databases for indications of the type of telephone being used (e.g. landline, wireless mobile, satellite, etc.), information that may provide an understanding of the location of the target.

(S) For electronic communications accounts/addresses/identifiers:

Review NSA content repositories and Internet communications data repositories (which contain, among other things, Internet communications metadata) for previous Internet activity. This information may contain network layer (e.g., Internet Protocol addresses) or machine identifier (e.g., Media Access Control addresses) information, which NSA compares to information contained in NSA's communication network databases and commercially available Internet Protocol address registration information in order to determine the location of the target.

(S) Assessment of the Non-United States Person Status of the Target

(S) In many cases, the information that NSA examines in order to determine whether a target is reasonably believed to be located outside the United States may also bear upon the non-United States person status of that target. For example, lead information provided by an intelligence or law enforcement service of a foreign government may indicate not only that the target is located in a foreign country, but that the target is a citizen of that or another foreign country. Similarly, information contained in NSA databases, including repositories of information collected by NSA and by other intelligence agencies, may indicate that the target is a non-United States person.

(S) Furthermore, in order to prevent the inadvertent targeting of a United States person, NSA maintains records of telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are being used by United States persons. Prior to targeting, a particular telephone number or electronic communications account/address/identifier will be compared against those records in order to ascertain whether NSA has reason to believe that telephone number or electronic communications account/address/identifier is being used by a United States person.

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

(S) In the absence of specific information regarding whether a target is a United States person, a person reasonably believed to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person can be positively identified as a United States person, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

(S) Assessment of the Foreign Intelligence Purpose of the Targeting

(S) In assessing whether the target possesses and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory, NSA considers, among other things, the following factors:

a. With respect to telephone communications:

- Information indicates that the telephone number has been used to communicate directly with another telephone number reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
- Information indicates that a user of the telephone number has communicated directly with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Information indicates that the telephone number is listed in the telephone directory of a telephone used by an individual associated with a foreign power or foreign territory;
- Information indicates that the telephone number has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Publicly available sources of information (e.g., telephone listings) match the telephone number to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Information contained in various NSA-maintained knowledge databases containing foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register and trap or trace device, or other information, reveals that the telephone number has been previously used by an individual associated with a foreign power or foreign territory;¹ or

¹ (TS//SI//NF) The NSA knowledge databases that would be used to satisfy this factor contain fused intelligence information concerning international terrorism culled from signals intelligence, human intelligence, law enforcement information, and other sources. The information compiled in these databases is information that assists the signals intelligence system in effecting collection on intelligence targets. For example, a report produced by the CIA may include the fact that a known terrorist is using a telephone with a particular number. NSA would include that information in its knowledge databases.

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

- Information made available to NSA analysts as a result of processing telephony metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the telephone number is used by an individual associated with a foreign power or foreign territory.
- b. With respect to Internet communications:
- Information indicates that the electronic communications account/address/identifier has been used to communicate directly with an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
 - Information indicates that a user of the electronic communications account/address/identifier has communicated directly with an individual reasonably believed to be associated with a foreign power or foreign territory;
 - Information indicates that the electronic communications account/address/identifier is included in the "buddy list" or address book of an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
 - Information indicates that the electronic communications account/address/identifier has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
 - Public Internet postings match the electronic communications account/address/identifier to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
 - Information contained in various NSA-maintained knowledge databases of foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, the use of a pen register or trap and trace device, or other information, reveals that electronic communications account/address/identifier has been previously used by an individual associated with a foreign power or foreign territory;
 - Information made available to NSA analysts as a result of processing metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the electronic communications account/address/identifier is used by an individual associated with a foreign power or foreign territory; or
 - Information indicates that Internet Protocol ranges and/or specific electronic identifiers or signatures (e.g., specific types of cryptology or steganography) are used almost exclusively by individuals associated with a foreign power or foreign territory,

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

or are extensively used by individuals associated with a foreign power or foreign territory.

II. (S) POST-TARGETING ANALYSIS BY NSA

(S//SI) After a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis. Such analysis is designed to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States, and will enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States. Such analysis may include:

For telephone numbers:

- Routinely comparing telephone numbers tasked pursuant to these procedures against information that has been incidentally collected from the Global System for Mobiles (GSM) Home Location Registers (HLR). These registers receive updates whenever a GSM phone moves into a new service area. Analysis of this HLR information provides a primary indicator of a foreign user of a mobile telephone entering the United States.
- NSA analysts may analyze content for indications that a foreign target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

For electronic communications accounts/addresses/identifiers:

- Routinely checking all electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against available databases that contain Internet communications data (including metadata) to determine if an electronic communications account/address/identifier was accessed from overseas. Such databases contain communications contact information and summaries of communications activity from NSA signals intelligence collection. The foreign access determination is made based on comparing the Internet Protocol address associated with the account activity to other information NSA possesses about geographical area(s) serviced by particular Internet Protocol addresses. If the IP address associated with the target activity is identified as a U.S.-based network gateway (e.g., a Hotmail server) or a private Internet Protocol address, then NSA analysts will be required to perform additional research to determine if the access was in a foreign country using additional criteria such as machine identifier or case notation (NSA circuit identifier) of a communications link known to be foreign. Such databases normally maintain information about such activity for a 12-month period. This data will be used in an attempt to rule out false positives from U.S.-based network gateways. If the account access is determined to be from a U.S.-based machine, further analytic checks will be performed using content collection to determine if the target has moved into the United States.

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

- Routinely comparing electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against a list of electronic communications accounts/addresses/identifiers already identified by NSA as being accessed from inside the United States. This will help ensure that no target has been recognized to be located in the United States.
- NSA analysts may analyze content for indications that a target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

(S) If NSA determines that a target has entered the United States, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay. In cases where NSA cannot resolve an apparent conflict between information indicating that the target has entered the United States and information indicating that the target remains located outside the United States, NSA will presume that the target has entered the United States and will terminate the acquisition from that target. If at a later time NSA determines that the target is in fact located outside the United States, NSA may re-initiate the acquisition in accordance with these procedures.

(S) If NSA determines that a target who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay.

III. (U) DOCUMENTATION

(S) Analysts who request tasking will document in the tasking database a citation or citations to the information that led them to reasonably believe that a targeted person is located outside the United States. Before tasking is approved, the database entry for that tasking will be reviewed in order to verify that the database entry contains the necessary citations.

(S) A citation is a reference that identifies the source of the information, such as a report number or communications intercept identifier, which NSA will maintain. The citation will enable those responsible for conducting oversight to locate and review the information that led NSA analysts to conclude that a target is reasonably believed to be located outside the United States.

(S) Analysts also will identify the foreign power or foreign territory about which they expect to obtain foreign intelligence information pursuant to the proposed targeting.

IV. (U) OVERSIGHT AND COMPLIANCE

(S) NSA's Signals Intelligence Directorate (SID) Oversight and Compliance, with NSA's Office of General Counsel (OGC), will develop and deliver training regarding the applicable procedures to ensure intelligence personnel responsible for approving the targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information understand their responsibilities and the procedures that apply to this acquisition. SID Oversight and Compliance has established processes for ensuring that raw traffic is labeled and stored only in authorized repositories, and is accessible only to those who have had the proper training. SID

TOP SECRET//COMINT//NOFORN//20320108

TOP SECRET//COMINT//NOFORN//20320108

Oversight and Compliance will conduct ongoing oversight activities and will make any necessary reports, including those relating to incidents of noncompliance, to the NSA Inspector General and OGC, in accordance with its NSA charter. SID Oversight and Compliance will also ensure that necessary corrective actions are taken to address any identified deficiencies. To that end, SID Oversight and Compliance will conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures, and conduct periodic spot checks of queries in data repositories.

(S) The Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) will conduct oversight of NSA's exercise of the authority under section 702 of the Act, which will include periodic reviews by DOJ and ODNI personnel to evaluate the implementation of the procedures. Such reviews will occur at least once every sixty days.

(S) NSA will report to DOJ, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer any incidents of noncompliance with these procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the intentional targeting of a United States person, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States. NSA will provide such reports within five business days of learning of the incident. Any information acquired by intentionally targeting a United States person or a person not reasonably believed to be outside the United States at the time of such targeting will be purged from NSA databases.

(S) NSA will report to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer, any incidents of noncompliance (including overcollection) by any electronic communication service provider to whom the Attorney General and Director of National Intelligence issued a directive under section 702. Such report will be made within five business days after determining that the electronic communication service provider has not complied or does not intend to comply with a directive.

(S) In the event that NSA concludes that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will take the following steps:

- 1) Terminate the acquisition without delay and determine whether to seek a Court order under another section of the Act. If NSA inadvertently acquires a communication sent to or from the target while the target is or was located inside the United States, including any communication where the sender and all intended recipients are reasonably believed to be located inside the United States at the time of acquisition, such communication will be treated in accordance with the applicable minimization procedures.

TOP SECRET//COMINT//NOFORN//20320108

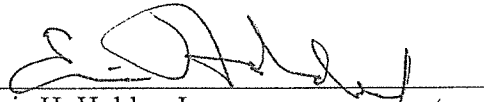
TOP SECRET//COMINT//NOFORN//20320108

- 2) Report the incident to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer within five business days.

V. (U) DEPARTURE FROM PROCEDURES

(S) If, in order to protect against an immediate threat to the national security, NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the Attorney General and Director of National Intelligence, NSA may take such action and will report that activity promptly to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer. Under such circumstances, the Government will continue to adhere to all of the statutory limitations set forth in subsection 702(b) of the Act.

7-28-09
Date


Eric H. Holder, Jr.
Attorney General of the United States

TOP SECRET//COMINT//NOFORN//20320108

Exhibit 6

Exhibit 6

DIRECTOR OF NATIONAL INTELLIGENCE

WASHINGTON, DC 20511

June 8, 2013

**Facts on the Collection of Intelligence Pursuant to Section 702
of the Foreign Intelligence Surveillance Act**

- PRISM is not an undisclosed collection or data mining program. It is an internal government computer system used to facilitate the government's statutorily authorized collection of foreign intelligence information from electronic communication service providers under court supervision, as authorized by Section 702 of the Foreign Intelligence Surveillance Act (FISA) (50 U.S.C. § 1881a). This authority was created by the Congress and has been widely known and publicly discussed since its inception in 2008.
- Under Section 702 of FISA, the United States Government does not unilaterally obtain information from the servers of U.S. electronic communication service providers. All such information is obtained with FISA Court approval and with the knowledge of the provider based upon a written directive from the Attorney General and the Director of National Intelligence. In short, Section 702 facilitates the targeted acquisition of foreign intelligence information concerning foreign targets located outside the United States under court oversight. Service providers supply information to the Government when they are lawfully required to do so.
- The Government cannot target anyone under the court-approved procedures for Section 702 collection unless there is an appropriate, and documented, foreign intelligence purpose for the acquisition (such as for the prevention of terrorism, hostile cyber activities, or nuclear proliferation) and the foreign target is reasonably believed to be outside the United States. We cannot target even foreign persons overseas without a valid foreign intelligence purpose.
- In addition, Section 702 cannot be used to intentionally target any U.S. citizen, or any other U.S. person, or to intentionally target any person known to be in the United States. Likewise, Section 702 cannot be used to target a person outside the United States if the purpose is to acquire information from a person inside the United States.
- Finally, the notion that Section 702 activities are not subject to internal and external oversight is similarly incorrect. Collection of intelligence information under Section 702 is subject to an extensive oversight regime, incorporating reviews by the Executive, Legislative and Judicial branches.

- *The Courts.* All FISA collection, including collection under Section 702, is overseen and monitored by the FISA Court, a specially established Federal court comprised of 11 Federal judges appointed by the Chief Justice of the United States.
 - The FISC must approve targeting and minimization procedures under Section 702 prior to the acquisition of any surveillance information.
 - Targeting procedures are designed to ensure that an acquisition targets non-U.S. persons reasonably believed to be outside the United States for specific purposes, and also that it does not intentionally acquire a communication when all the parties are known to be inside the US.
 - Minimization procedures govern how the Intelligence Community (IC) treats the information concerning any U.S. persons whose communications might be incidentally intercepted and regulate the handling of any nonpublic information concerning U.S. persons that is acquired, including whether information concerning a U.S. person can be disseminated. Significantly, the dissemination of information about U.S. persons is expressly prohibited unless it is necessary to understand foreign intelligence or assess its importance, is evidence of a crime, or indicates a threat of death or serious bodily harm.
- *The Congress.* After extensive public debate, the Congress reauthorized Section 702 in December 2012.
 - The law specifically requires a variety of reports about Section 702 to the Congress.
 - The DNI and AG provide exhaustive semiannual reports assessing compliance with the targeting and minimization procedures.
 - These reports, along with FISA Court opinions, and a semi-annual report by the Attorney General are provided to Congress. In short, the information provided to Congress by the Executive Branch with respect to these activities provides an unprecedented degree of accountability and transparency.
 - In addition, the Congressional Intelligence and Judiciary Committees are regularly briefed on the operation of Section 702.
- *The Executive.* The Executive Branch, including through its independent Inspectors General, carries out extensive oversight of the use of Section 702 authorities, which includes regular on-site reviews of how Section 702 authorities are being implemented. These regular reviews are documented in reports produced to Congress. Targeting decisions are reviewed by ODNI and DOJ.
 - Communications collected under Section 702 have provided the Intelligence Community insight into terrorist networks and plans. For example, the Intelligence

Community acquired information on a terrorist organization's strategic planning efforts.

- Communications collected under Section 702 have yielded intelligence regarding proliferation networks and have directly and significantly contributed to successful operations to impede the proliferation of weapons of mass destruction and related technologies.
- Communications collected under Section 702 have provided significant and unique intelligence regarding potential cyber threats to the United States including specific potential computer network attacks. This insight has led to successful efforts to mitigate these threats.

Exhibit 7

Exhibit 7

LIBERTY AND SECURITY IN A CHANGING WORLD

12 December 2013

**Report and Recommendations of
The President's Review Group on Intelligence
and Communications Technologies**

This page has been intentionally left blank.

Transmittal Letter

Dear Mr. President:

We are honored to present you with the Final Report of the Review Group on Intelligence and Communications Technologies. Consistent with your memorandum of August 27, 2013, our recommendations are designed to protect our national security and advance our foreign policy while also respecting our longstanding commitment to privacy and civil liberties, recognizing our need to maintain the public trust (including the trust of our friends and allies abroad), and reducing the risk of unauthorized disclosures.

We have emphasized the need to develop principles designed to create strong foundations for the future. Although we have explored past and current practices, and while that exploration has informed our recommendations, this Report should not be taken as a general review of, or as an attempt to provide a detailed assessment of, those practices. Nor have we generally engaged budgetary questions (although some of our recommendations would have budgetary implications).

We recognize that our forty-six recommendations, developed over a relatively short period of time, will require careful assessment by a wide range of relevant officials, with close reference to the likely consequences. Our goal has been to establish broad understandings and principles that

can provide helpful orientation during the coming months, years, and decades.

We are hopeful that this Final Report might prove helpful to you, to Congress, to the American people, and to leaders and citizens of diverse nations during continuing explorations of these important questions.

Richard A. Clarke

Michael J. Morell

Geoffrey R. Stone

Cass R. Sunstein

Peter Swire

Acknowledgements

The Review Group would like to thank the many people who supported our efforts in preparing this Report. A number of people were formally assigned to assist the Group, and all performed with professionalism, hard work, and good cheer. These included Brett Freedman, Kenneth Gould, and other personnel from throughout the government. We thank as well the many other people both inside and outside of the government who have contributed their time and energy to assisting in our work.

This page has been intentionally left blank.

Table of Contents

Preface

Executive Summary

Recommendations

Chapter I: Principles

Chapter II: Lessons of History

- A. The Continuing Challenge
- B. The Legal Framework as of September 11, 2001
- C. September 11 and its Aftermath
- D. The Intelligence Community

Chapter III: Reforming Foreign Intelligence Surveillance Directed at United States Persons

- A. Introduction
- B. Section 215: Background
- C. Section 215 and “Ordinary” Business Records

- D. National Security Letters
- E. Section 215 and the Bulk Collection of Telephony Meta-data
 - 1. The Program
 - 2. The Mass Collection of Personal Information
 - 3. Is Meta-data Different?
- F. Secrecy and Transparency

Chapter IV: Reforming Foreign Intelligence Surveillance Directed at Non-United States Persons

- A. Introduction
- B. Foreign Intelligence Surveillance and Section 702
- C. Privacy Protections for United States Persons Whose Communications are Intercepted Under Section 702
- D. Privacy Protections for Non-United States Persons

Chapter V: Determining What Intelligence Should Be Collected and How

- A. Priorities and Appropriateness
- B. Monitoring Sensitive Collection
- C. Leadership Intentions

D. Cooperation with Our Allies

Chapter VI: Organizational Reform in Light of Changing Communications Technology

A. Introduction

B. The National Security Agency

1. “Dual-Use” Technologies: The Convergence of Civilian Communications and Intelligence Collection
2. Specific Organizational Reforms

C. Reforming Organizations Dedicated to the Protection of Privacy and Civil Liberties

D. Reforming the FISA Court

Chapter VII: Global Communications Technology: Promoting Prosperity, Security, and Openness in a Networked World

A. Introduction

B. Background: Trade, Internet Freedom, and Other Goals

1. International Trade and Economic Growth
2. Internet Freedom

judicial approval would not be required under standard and well-established principles.

E. Section 215 and the Bulk Collection of Telephony Meta-data

1. The Program

One reading of section 215 is that the phrase “reasonable grounds to believe that the tangible things sought are *relevant* to an authorized investigation” means that the order must specify with reasonable particularity the records or other things that must be turned over to the government. For example, the order might specify that a credit card company must turn over the credit records of a particular individual who is reasonably suspected of planning or participating in terrorist activities, or that a telephone company must turn over to the government the call records of any person who called an individual suspected of carrying out a terrorist act within a reasonable period of time preceding the terrorist act. This interpretation of “relevant” would be consistent with the traditional understanding of “relevance” in the subpoena context.

In May 2006, however, the FISC adopted a much broader understanding of the word “relevant.”⁸⁴ It was that decision that led to the collection of bulk telephony meta-data under section 215. In that decision, and in thirty-five decisions since, fifteen different FISC judges have issued orders under section 215 directing specified United States telecommunications providers to turn over to the FBI and NSA, “on an

⁸⁴ See *In re Application of the Federal Bureau of Investigation for an Order Requiring the Prod. Of Tangible Things from [Telecommunications Providers] Relating to [Redacted version]*, Order No. BR-05 (FISC May 24, 2006).

ongoing daily basis,” for a period of approximately 90 days, “all call detail records or ‘telephony meta-data’ created by [the provider] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.”⁸⁵

The “telephony meta-data” that must be produced includes “comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile Station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.”⁸⁶ The orders expressly provide that the meta-data to be produced “does not include the substantive content of any communication . . . or the name, address, or financial information of a subscriber or customer,” nor does it include “cell site location information.”⁸⁷ The orders also contain a nondisclosure provision directing that, with certain exceptions, “no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order.”⁸⁸

The FISC authorized the collection of bulk telephony meta-data under section 215 in reliance “on the assertion of the [NSA] that having access to all the call records ‘is vital to NSA’s counterterrorism intelligence’ because ‘the only effective means by which NSA analysts are able

⁸⁵ *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR 13-109 (FISC Oct. 11, 2013) (hereinafter FISC order 10/11/2013).

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

continuously to keep track of” the activities, operatives, and plans of specific foreign terrorist organizations who “disguise and obscure their communications and identities” is “to obtain and maintain an archive of meta-data that will permit these tactics to be uncovered.”⁸⁹ The government has explained the rationale of the program as follows:

One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in this effort. It is imperative that we have the capability to rapidly identify any terrorist threat inside the United States. . . .

. . . By analyzing telephony meta-data based on telephone numbers or other identifiers associated with terrorist activity, trained expert analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the United States. . . . In this respect, the program helps to close critical intelligence gaps that were highlighted by the September 11, 2001 attacks.⁹⁰

⁸⁹ *In Re Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR-08-13 (FISC Dec. 12, 2008), quoting Application Exhibit A, Declaration of [Redacted version] (Dec. 11, 2008).

⁹⁰ Administration White Paper, *Bulk Collection of Telephony Meta-data Under Section 215 of the USA PATRIOT Act*, at 3-4 (August 9, 2013).

What this means, in effect, is that specified service providers must turn over to the government on an ongoing basis call records for every telephone call made in, to, or from the United States through their respective systems. NSA retains the bulk telephony meta-data for a period of five years. The meta-data are then purged automatically from NSA's systems on a rolling basis. As it currently exists, the section 215 program acquires a very large amount of telephony meta-data each day, but what it collects represents only a small percentage of the total telephony meta-data held by service providers. Importantly, in 2011 NSA abandoned a similar meta-data program for Internet communications.⁹¹

According to the terms of the FISC orders, the following restrictions govern the use of this telephony meta-data:

1. "NSA shall store and process the . . . meta-data in repositories with secure networks under NSA's control. The . . . meta-data shall carry unique markings such that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training," and

⁹¹ For several years, NSA used a similar meta-data program for Internet communications under the authority of FISA's pen register and trap-and-trace provisions rather than under the authority of section 215. NSA suspended this e-mail meta-data program in 2009 because of compliance issues (it came to light that NSA had inadvertently been collecting certain types of information that were not consistent with the FISC's authorization orders). After re-starting it in 2010, NSA Director General Keith Alexander decided to let the program expire at the end of 2011 because, for operational and technical reasons, the program was insufficiently productive to justify the cost. The possibility of revising and reinstating such a program was left open, however. This program posed problems similar to those posed by the section 215 program, and any effort to re-initiate such a program should be governed by the same recommendations we make with respect to the section 215 program.

- “NSA shall restrict access to the . . . meta-data to authorized personnel who have received” such training.
2. “The government is . . . prohibited from accessing” the meta-data “for any purpose” other than to obtain “foreign intelligence information.”⁹²
 3. “NSA shall access the . . . meta-data for purposes of obtaining foreign intelligence only through queries of the . . . meta-data to obtain contact chaining information . . . using selection terms approved as ‘seeds’ pursuant to the RAS approval process.” What this means is that NSA can access the meta-data only when “there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried,” that is, the specific phone number, “is associated with” a specific foreign terrorist organization. The government submits and the FISC approves a list of specific foreign terrorist organizations to which all queries must relate.
 4. The finding that there is a reasonable, articulable suspicion that any particular identifier is associated with a foreign terrorist organization can be made initially by only one of 22 specially trained persons at NSA (20 line personnel and two supervisors). All RAS determinations must be made

⁹² Appropriately trained and authorized technical personnel may also access the meta-data “to perform those processes needed to make it usable for intelligence analysis,” and for related technical purposes, according to the FISC orders.

independently by at least two of these personnel and then approved by one of the two supervisors before any query may be made.

5. Before any selection term may be queried, NSA's Office of General Counsel (OGC) "must first determine" whether it is "reasonably believed to be used by a United States person."⁹³ If so, then the selection term may not be queried if the OGC finds that the United States person was found to be "associated with" a specific foreign terrorist organization "solely on the basis of activities that are protected by the First Amendment to the Constitution."
6. "NSA shall ensure, through adequate and appropriate technical and management controls, that queries of the . . . meta-data for intelligence analysis purposes will be initiated using only selection terms that have been RAS-approved. Whenever the . . . meta-data is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis tools, an auditable record of the activity shall be generated."
7. The determination that a particular selection term may be queried remains in effect for 180 days if the selection term is reasonably believed to be used by a United States person, and otherwise for one year.

⁹³ 50 U.S.C. 1801(i). A "United States person" is either a citizen of the United States or a non-citizen who is a legal permanent resident of the United States.

8. Before any of the results from queries may be shared outside NSA (typically with the FBI), NSA must comply with minimization and dissemination requirements, and before NSA may share any results from queries that reveal information about a United States person, a high-level official must additionally determine that the information “is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.”
9. The FISA court does not review or approve individual queries either in advance or after the fact. It does set the criteria for queries, however, and it receives reports every 30 days from NSA on the number of identifiers used to query the meta-data and on the results of those queries. The Department of Justice and the Senate and House Intelligence Committees also receive regular briefings on the program.
10. Both NSA and the National Security Division of the Department of Justice (NSD/DOJ) conduct regular and rigorous oversight of this program. For example:
 - NSA’s OGC and Office of the Director of Compliance (ODOC) “shall ensure that personnel with access to the . . . meta-data receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and

retention of the . . . meta-data and the results of queries of the . . . meta-data.”⁹⁴

- NSD/DOJ receives “all formal briefing and/or training materials.” NSA’s ODOC “shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information.”⁹⁵
- NSA’s OGC “shall consult with NSD/DOJ “on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority,” and at least once every ninety days NSA’s OGC, ODOC and NSD/DOJ “shall meet for the purpose of assessing compliance” with the FISC’s orders. The results of that meeting “shall be reduced to writing and submitted” to the FISC “as part of any application to renew or reinstate the authority.”⁹⁶
- At least once every 90 days “NSD/DOJ shall meet with NSA’s Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA’s compliance” with the FISC’s orders, and at least once every 90 days NSA’s OGC and NSD/DOJ “shall review a

⁹⁴ *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR 13-158 (FISC, Dec. 2011).

⁹⁵ *Id.*, at 14.

⁹⁶ *Id.*, at 14-15.

sample of the justifications for RAS approvals for selection terms used to query the . . . meta-data.”⁹⁷

- Approximately every 30 days, NSA must file with the FISC “a report that includes a discussion of NSA’s application of the RAS standard,” “a statement of the number of instances . . . in which NSA has shared, in any form, results from queries of the . . . meta-data that contain United States person information, in any form, with anyone outside NSA,” and an attestation for each instance in which United States information has been shared that “the information was related to counterterrorism information and necessary to understand counterterrorism or to assess its importance.”⁹⁸

How does the section 215 bulk telephony meta-data program work in practice? In 2012, NSA queried 288 unique identifiers, each of which was certified by NSA analysts to meet the RAS standard. When an identifier, or “seed” phone number, is queried, NSA receives a list of every telephone number that either called or was called by the seed phone number in the past five years. This is known as the “first hop.” For example, if the seed phone number was in contact with 100 different phone numbers in the past five years, NSA would have a list of those phone numbers. Given that NSA

⁹⁷ *Id.*, at 15.

⁹⁸ *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR 13-109 (FISC Oct. 11, 2013) (hereinafter FISC order 10/11/2013).

has reasonable articulable suspicion to believe that the seed phone number is associated with a foreign terrorist organization, it then seeks to determine whether there is any reason to believe that any of the 100 numbers are *also* associated with a foreign terrorist organization. If so, the query has uncovered possible connections to a potential terrorist network that merits further investigation. Conversely, if none of the 100 numbers in the above hypothetical is believed to be associated with possible terrorist activity, there is less reason to be concerned that the potential terrorist is in contact with co-conspirators in the United States.

In most cases, NSA makes a second “hop.” That is, it queries the database to obtain a list of every phone number that called or was called by the 100 numbers it obtained in the first hop. To continue with the hypothetical: If we assume that the average telephone number called or was called by 100 phone numbers over the course of the five-year period, the query will produce a list of 10,000 phone numbers (100 x 100) that are two “hops” away from the person reasonably believed to be associated with a foreign terrorist organization. If one of those 10,000 phone numbers is thought to be associated with a terrorist organization, that is potentially useful information not only with respect to the individuals related to the first and third hops, but also with respect to individuals related to the second hop (the middleman). In a very few instances, NSA makes a third “hop,” which would expand the list of numbers to approximately one million (100 x 100 x 100).

In 2012, NSA's 288 queries resulted in a total of twelve "tips" to the FBI that called for further investigation. If the FBI investigates a telephone number or other identifier tipped to it through the section 215 program, it must rely on other information to identify the individual subscribers of any of the numbers retrieved. If, through further investigation, the FBI is able to develop probable cause to believe that an identifier in the United States is conspiring with a person engaged in terrorist activity, it can then seek an order from the FISC authorizing it to intercept the *contents* of future communications to and from that telephone number.

NSA believes that on at least a few occasions, information derived from the section 215 bulk telephony meta-data program has contributed to its efforts to prevent possible terrorist attacks, either in the United States or somewhere else in the world. More often, negative results from section 215 queries have helped to alleviate concern that particular terrorist suspects are in contact with co-conspirators in the United States. Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders. Moreover, there is reason for caution about the view that the program is efficacious in alleviating concern about possible terrorist connections, given the fact that the meta-data captured by the program covers only a portion of the records of only a few telephone service providers.

* * * * *

Exhibit 8

Exhibit 8

Would NSA surveillance have stopped 9/11 plot?

By Peter Bergen , CNN National Security Analyst
updated 7:28 PM EST, Mon December 30, 2013

CNN.com

Would NSA surveillance have stopped 9/11 plot?

Editor's note: Peter Bergen is CNN's national security analyst, a director at the [New America Foundation](#) and the author of ["Manhunt: The Ten-Year Search for bin Laden -- From 9/11 to Abbottabad"](#) which this article draws upon.

(CNN) -- The Obama administration has framed its defense of the controversial bulk collection of all American phone records as necessary to prevent a future 9/11.

During a House Intelligence Committee hearing on June 18, NSA director [Gen. Keith Alexander said](#), "Let me start by saying that I would much rather be here today debating this point than trying to explain how we failed to prevent another 9/11."

This closely mirrors talking points by the National Security Agency about how to defend the program.

In the [talking points](#), NSA officials are encouraged to use "sound bites that resonate," specifically, "I much prefer to be here today explain these programs, than explaining another 9/11 event that we were not able to prevent."

On Friday in New York, Judge William H. Pauley III [ruled that NSA's bulk collection of American telephone records is lawful](#). He cited Alexander's testimony and quoted him saying, "We couldn't connect the dots because we didn't have the dots."

But is it really the case that the U.S. intelligence community didn't have the dots in the lead up to 9/11? Hardly.

In fact, the intelligence community provided repeated strategic warning in the summer of 9/11 that al Qaeda was planning a large-scale attacks on American interests.

Here is a representative sampling of the [CIA threat reporting](#) that was distributed to Bush administration officials during the spring and summer of 2001:

- CIA, "Bin Ladin Planning Multiple Operations," April 20
- CIA, "Bin Ladin Attacks May Be Imminent," June 23
- CIA, "Planning for Bin Ladin Attacks Continues, Despite Delays," July 2
- CIA, "Threat of Impending al Qaeda Attack to Continue Indefinitely," August 3

The failure to respond adequately to these warnings was a *policy*



Federal judges at odds over NSA data collection



Rep. King: Snowden is a disgrace



Gellman: Snowden's mission accomplished



A surprise ruling for NSA

failure by the Bush administration, not an intelligence failure by the U.S. intelligence community.

A case of missed opportunities

The CIA itself also had its own spectacular failure in the run up to 9/11, which wasn't a failure to collect intelligence, but a

failure of information sharing. The CIA had quite a bit of information about two of the hijackers and their presence in the United States before 9/11, which the agency didn't share with other government agencies until it was too late to do anything about it.

The government missed multiple opportunities to catch al Qaeda hijacker Khalid al-Mihdhar when he was living in San Diego for a year and a half in the run up to 9/11, not because it lacked access to all Americans phone records but because it didn't share the information it already possessed about the soon-to-be hijacker within other branches of the government.

The missed opportunities in the al-Mihdhar case are well-documented. The CIA failed to "watch-list" al-Mihdhar and another suspected al Qaeda terrorist, Nawaf al-Hazmi, whom the agency had been tracking since they attended an al Qaeda summit in Malaysia on January 5, 2000.

The failure to put Mihdhar and Hamzi on a watch list meant that immigration and law enforcement authorities were not alerted to their presence when they entered the United States under their real names. Ten days after the meeting in Malaysia, on January 15, 2000, al-Hazmi and al-Mihdhar flew into Los Angeles.

The CIA also did not alert the FBI about the identities of the suspected terrorists so that the bureau could look for them once they were inside the United States.

An investigation by the CIA inspector general -- published in unclassified form in 2007 -- found that this was not the oversight of a couple of agency employees but rather that a large number of CIA officers and analysts had dropped the ball. Some 50 to 60 agency employees read cables about the two al Qaeda suspects without taking any action.

Some of those officers knew that one of the al Qaeda suspects had a visa for the United States, and by March 2001, some knew that the other suspect had flown to Los Angeles.

The soon-to-be hijackers would not have been difficult to find in California if their names had been known to law enforcement. Under their real names, they rented an apartment, got driver's licenses, opened bank accounts, purchased a car and took flight lessons. Al-Mihdhar even listed his name in the local phone directory.

It was only on August 24, 2001, as a result of questions raised by a CIA officer on assignment at the FBI, that the two al Qaeda suspects were watch-listed and their names communicated to the bureau. Even then, [the FBI sent out only a "routine" notice](#) requesting an investigation of al-Mihdhar. Nothing substantive came of this request.

A month later, al-Hamzi and al-Mihdhar were two of the hijackers on American Airlines Flight 77 that plunged into the Pentagon, killing 189 people.

[The CIA inspector general's report concluded](#) that "informing the FBI and good operational follow-through by CIA and FBI might have resulted in surveillance of both al-Mihdhar and al-Hazmi. Surveillance, in turn, would have had the potential to yield information on flight training, financing, and links to others who were complicit in the 9/11 attacks."

It's about the sharing

These multiple missed opportunities challenge the administration's claims that the NSA's bulk phone data surveillance program could have prevented the 9/11 attacks. The key problem was one of information sharing, not the lack of information.

Obama administration officials who defend the NSA bulk collection of phone records program cite the failure to detect al-Mihdhar's presence in San Diego before 9/11 as a reason to justify the program.

Then-FBI Director [Robert Mueller argued](#) before the House Judiciary Committee on June 13 that bulk collection of telephone records might have prevented 9/11.

"Before 9/11, there was an individual by the name of Khalid al-Mihdhar, who came to be one of the principal hijackers. He was being tracked by the intelligence agencies in the Far East. They lost track of him. At the same time, the intelligence agencies had identified an al Qaeda safe house in Yemen.

"They understood that that al Qaeda safe house had a telephone number, but they could not know who was calling into that particular safe house. We came to find out afterwards that the person who had called into that safe house was al-Mihdhar, who was in the United States in San Diego. If we had had this program in place at the time, we would have been able to identify that particular telephone number in San Diego."

As documented above, however, the government missed multiple opportunities to catch al-Mihdhar, and the failure was one of information sharing inside the U.S. intelligence community. Since we can't run history backward, all we can say with certainty is that it is an indisputable fact that the proper sharing of intelligence by the CIA with other agencies about al-Mihdhar may well have derailed the 9/11 plot. And it is merely an untestable hypothesis that if the NSA bulk phone collection program had been in place at the time that it might have helped to find the soon-to-be-hijackers in San Diego.

Indeed, the overall problem for U.S. counterterrorism officials is not that they don't gather enough

information from the bulk surveillance of American phone data but that they don't sufficiently understand or widely share the information they already possess that is derived from conventional law enforcement and intelligence techniques.

An unfortunate pattern of cases

What was true of the two 9/11 hijackers living in San Diego was also the unfortunate pattern we have seen in several other significant terrorism cases:

-- Chicago resident David Coleman Headley was central to the planning of the 2008 terrorist attacks in Mumbai that killed 166 people. Yet, following the 9/11 attacks, U.S. authorities received plausible tips regarding Headley's associations with militant groups at least five times from his family members, friends and acquaintances. [These multiple tips were never followed up](#) in an effective fashion.

-- Maj. Nidal Hasan, a military psychiatrist, killed 13 people at Fort Hood, Texas, in 2009. Yet intelligence agencies had intercepted multiple e-mails between Hasan and Anwar al-Awlaki, a U.S.-born cleric living in Yemen who was notorious for his ties to militants. The e-mails included a discussion of the permissibility in Islam of killing U.S. soldiers. Counterterrorism investigators [didn't follow up](#) on these e-mails, believing they were somehow consistent with Hasan's job as a military psychiatrist.

-- Carlos Bledsoe, a convert to Islam, fatally shot a soldier at a Little Rock, Arkansas, military recruiting office in 2009. Shortly before the attack, Bledsoe had traveled to Yemen. As a result, Bledsoe was under investigation by the FBI yet he was [still able to buy](#) the weapons he needed for his deadly attack when he was back in the United States.

-- Nigerian Umar Farouk AbdulMutallab attempted to blow up Northwest Flight 253 over Detroit on Christmas Day 2009 with an "underwear bomb." Luckily, the bomb failed to explode. Yet, a few weeks before the botched attack, AbdulMutallab's father contacted the U.S. Embassy in Nigeria with concerns that his son had become radicalized and might be planning something. [This information](#) wasn't further investigated.

AbdulMutallab had been recruited by al Qaeda's branch in Yemen for the mission.

The [White House's review](#) of the underwear bomb plot concluded that there was sufficient information known to the U.S. government to determine that AbdulMutallab was likely working for al Qaeda in Yemen and that the group was looking to expand its attacks beyond Yemen. Yet AbdulMutallab was allowed to board a plane bound for the United States without any question.

All of these serious terrorism cases argue not for the gathering of ever vaster troves of information but simply for a better understanding of the information the government has already collected and that are derived from conventional law enforcement and intelligence methods.

Follow us on Twitter

Join us on

Exhibit 9

Exhibit 9

Surveillance

Judge on NSA Case Cites 9/11 Report, But It Doesn't Actually Support His Ruling

by Justin Elliott
ProPublica, Dec. 28, 2013, 11:35 a.m.

Update Dec. 28, 2013: In a new decision in support of the NSA's phone metadata surveillance program, U.S. district court Judge William Pauley cites [1] an intelligence failure involving the agency in the lead-up to the 9/11 attacks. But the judge's cited source, the 9/11 Commission Report, doesn't actually include the account he gives in the ruling. What's more, experts say the NSA could have avoided the pre-9/11 failure even without the metadata surveillance program.

We previously explored the key incident in question, involving calls made by hijacker Khalid al-Mihdhar from California to Yemen, in a story we did over the summer, which you can read below.

In his decision, Pauley writes: "The NSA intercepted those calls using overseas signals intelligence capabilities that could not capture al-Mihdhar's telephone number identifier. Without that identifier, NSA analysts concluded mistakenly that al-Mihdhar was overseas and not in the United States."

As his source, the judge writes in a footnote, "See generally, The 9/11 Commission Report." In fact, the 9/11 Commission report does not detail the NSA's intercepts of calls between al-Mihdhar and Yemen. As the executive director of the commission told us over the summer, "We could not, because the information was so highly classified publicly detail the nature of or limits on NSA monitoring of telephone or email communications."

To this day, some details related to the incident and the NSA's eavesdropping have never been aired publicly. And some experts told us that even before 9/11 -- and before the creation of the metadata surveillance program -- the NSA did have the ability to track the origins of the phone calls, but simply failed to do so.

* * *

This story was originally published on June 20, 2013 and updated [2] on June 21, 2013.

In defending the NSA's sweeping collection of Americans' phone call records, Obama administration officials have repeatedly [3] pointed out [4] how it could have helped thwart the 9/11 attacks: If only the surveillance program been in place before Sept. 11, 2001, U.S. authorities would have been able to identify one of the future hijackers who was living in San Diego.

Last weekend, former Vice President Dick Cheney invoked [5] the same argument.

It is impossible to know for certain whether screening phone records would have stopped the attacks -- the program didn't exist at the time. It's also not clear whether the program would have given the NSA abilities it didn't already possess with respect to the case. Details of the current program and as well as NSA's role in intelligence gathering around the 9/11 plots remain secret.

But one thing we do know: Those making the argument have ignored a key aspect of historical record.

U.S. intelligence agencies knew the identity of the hijacker in question, Saudi national Khalid al Mihdhar, long before 9/11 and had the ability find him, but they failed to do so.

"There were plenty of opportunities without having to rely on this metadata system for the FBI and intelligence agencies to have located Mihdhar," says former Senator Bob Graham, the Florida Democrat who extensively investigated [6] 9/11 as chairman of the Senate's intelligence committee.

These missed opportunities are described in detail in the joint congressional report [6] produced by Graham and his colleagues as well as in the 9/11 Commission report [7].

Mihdhar is at the center of the well-known story of the failure of information sharing between the CIA and FBI and other agencies.

Indeed, the Obama administration's invocation of the Mihdhar case echoes a nearly identical argument made by [8] the Bush administration eight years ago when it defended the NSA's warrantless wiretapping program.



Hijacker Khalid al Mihdhar, wearing the yellow shirt, foreground, passes through the security checkpoint at Dulles International Airport on Sept. 11, 2001, just hours before American Airlines Flight 77 crashed into the Pentagon. (AP Photo/APTN)

Mihdhar and the other hijacker with whom he lived in California, Nawaf al Hazmi, were “experienced mujahideen [9]” who had traveled to fight in Bosnia in the mid-1990s and spent time in Afghanistan.

Mihdhar was on the intelligence community’s radar at least as early as 1999. That’s when the NSA had picked up communications from a “terrorist facility” in the Mideast suggesting that members of an “operational cadre” were planning to travel to Kuala Lumpur in January 2000, according to the commission report [10]. The NSA picked up the first names of the members, including a “Khalid.” The CIA identified him as Khalid al Mihdhar.

The U.S. got photos of those attending the January 2000 meeting in Malaysia, including of Mihdhar, and the CIA also learned that his passport had a visa for travel to the U.S. But that fact was not shared with FBI headquarters until much later, in August 2001, which proved too late.

“Critical parts of the information concerning al-Mihdhar and al-Hazmi lay dormant

within the Intelligence Community for as long as eighteen months,” the congressional 9/11 report concludes [11], “at the very time when plans for the September 11 attacks were proceeding.

The CIA missed repeated opportunities to act based on information in its possession that these two Bin Ladin associated terrorists were traveling to the United States, and to add their names to watchlists.”

Using their true names, Mihdhar and Hazmi for a time beginning in May 2000 even lived [12] with [13] an active FBI informant in San Diego.

The U.S. lost track of Mihdhar’s trail in Asia in early 2000, but there were more chances.

“On four occasions in 2001, the CIA, the FBI, or both had apparent opportunities to refocus on the significance of Hazmi and Mihdhar and reinvigorate the search for them,” the 9/11 Commission report says [14]. The report concludes that if more resources had been applied and a different approach taken, Mihdhar could have been found and stopped.

So, apart from all the missed opportunities, would a theoretical metadata program capturing phone records of all Americans made a difference before 9/11?

Key details about Mihdhar’s activities and the NSA before 9/11 remain classified so it’s difficult answer conclusively.

Let’s turn to the comments [15] of FBI Director Robert Mueller before the House Judiciary Committee last week.

Mueller noted that intelligence agencies lost track of Mihdhar following the January 2000 Kuala Lumpur meeting but at the same time had identified an “Al Qaida safe house in Yemen.”

He continued: “They understood that that Al Qaida safe house had a telephone number but they could not know who was calling into that particular safe house. We came to find out afterwards that the person who had called into that safe house was al Mihdhar, who was in the United States in San Diego. If we had had this [metadata] program in place at the time we would have been able to identify that particular telephone number in San Diego.”

In turn, the number would have led to Mihdhar and potentially disrupted the plot, Mueller argued.

(Media accounts [16] indicate that the “safe house” was actually the home of Mihdhar’s father-in-law, himself a longtime al Qaida figure, and that the NSA had been intercepting calls to the home for several years.)

The congressional 9/11 report sheds some further light [17] on this episode, though in highly redacted form.

The NSA had in early 2000 analyzed communications between a person named “Khaled” and “a suspected terrorist facility in the Middle East,” according to this account. But, crucially, the intelligence community “did not determine the location from which they had been made.”

In other words, the report suggests, the NSA actually picked up the content of the communications between Mihdhar and the “Yemen safe house” but was not able to figure out who was calling or even the phone number he was calling from.

“[Y]ou should not assume that the NSA was then able to determine, from the contents of communications, the originating phone number or IP address of an incoming communication to that place in Yemen,” said Philip Zelickow, who was executive director of the 9/11 Commission, in an email to ProPublica. “It would depend on the technical details of how the signals were being monitored.”

It wasn’t until after 9/11 that the FBI figured out that “Khaled” was hijacker Khalid al-Mihdhar, calling from San Diego.

The 9/11 Commission report itself does not appear to describe the communication between Mihdhar and Yemen.

When the Commission report was released in 2004, according to Zelikow, "we could not, because the information was so highly classified publicly detail the nature of or limits on NSA monitoring of telephone or email communications." Information on the topic remains classified, he added.

Zelikow called Mueller's recent assertion about the metadata program "accurate and fair."

"It is definitely possible that, with the kind of databases that Mueller is discussing, used properly, the US government would have been alerted during 2000 to the presence in the U.S. -- and possibly the location -- of these individuals -- and possibly others he did not mention who arrived later," Zelikow said.

Theories about the metadata program aside, it's not clear why the NSA couldn't or didn't track the originating number of calls to Yemen it was already listening to.

Intelligence historian Matthew Aid, who wrote the 2009 NSA history *Secret Sentry* [18], says that the agency would have had both the technical ability and legal authority to determine the San Diego number that Mihdhar was calling from.

"Back in 2001 NSA was routinely tracking the identity of both sides of a telephone call," he told ProPublica.

The NSA did not respond to a request for comment. The FBI stood by Mueller's argument but declined to further explain how the metadata program would have come into play before 9/11.

There's another wrinkle in the Mihdhar case: In the years after 9/11, media [19] reports [20] also suggested that there were multiple calls that went in the other direction: from the house in Yemen to Mihdhar in San Diego. But the NSA apparently also failed to track where those calls were going.

In 2005, the Los Angeles Times quoted [19] unnamed officials saying the NSA had well-established legal authority before 9/11 to track calls made from the Yemen number to the U.S. In that more targeted scenario, a metadata program vacuuming the phone records of all Americans would appear to be unnecessary.

That story followed President Bush's defense of the NSA warrantless wiretapping program, which had just been revealed [21] by the New York Times.

"We didn't know they were here, until it was too late," Bush said in a December 2005 live radio address [8] from the White House.

It's not clear how the wiretapping program would have come into play in the Mihdhar case. The program at issue in 2005 involved getting the actual content of communications, which the NSA had already been doing in the Mihdhar case.

Update: Richard Clarke, who was the White House counterterrorism czar beginning in 1998 and through 9/11, told ProPublica that the NSA had both the ability and legal authority to trace calls from Mihdhar to Yemen in 2000.

"Justice could have asked the FISA Court for a warrant to all phone companies to show all calls from the U.S. which went to the Yemen number. As far as I know, they did not do so. They could have," Clarke wrote in an email. "My understanding is that they did not need the current All Calls Data Base FISA warrant to get the information they needed. Since they had one end of the calls (the Yemen number), all they had to do was ask for any call connecting to it."

Like this story? Sign up for our daily newsletter [22] to get more of our best work.

-
1. https://www.aclu.org/sites/default/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf
 2. #clarke-update
 3. http://www.nypost.com/p/news/international/dozens_of_attacks_thwarted_nXJ10NuPkMd1RrIT1U8J
 4. <http://www.guardian.co.uk/world/2013/jun/13/fbi-mueller-spy-tactics-9-11-boston>
 5. http://firstread.nbcnews.com/_news/2013/06/16/18987472-cheney-says-nsa-monitoring-could-have-prevented-911?lite
 6. <http://www.propublica.org/documents/item/716032-congressional-911-report-crpt-107hrpt792>
 7. <http://www.propublica.org/documents/item/712496-911report>
 8. <http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html>
 9. <http://www.propublica.org/documents/item/712496-911report#document/p172/a106116>
 10. <http://www.propublica.org/documents/item/712496-911report#document/p198>
 11. <http://www.propublica.org/documents/item/716032-congressional-911-report-crpt-107hrpt792#document/p44>
 12. <http://www.justice.gov/oig/special/0506/chapter5.htm>
 13. <http://www.propublica.org/documents/item/716032-congressional-911-report-crpt-107hrpt792#document/p49>
 14. <http://www.propublica.org/documents/item/712496-911report#document/p283/a106115>
 15. <http://www.nydailynews.com/opinion/-article-1.1373310>
 16. <http://www.amazon.com/The-Secret-Sentry-National-Security/dp/B003L1ZX4S>

17. <http://www.propublica.org/documents/item/716032-congressional-911-report-crpt-107hrpt792#document/p48>
18. <http://www.amazon.com/The-Secret-Sentry-ebook/dp/B002WOD8X8>
19. http://articles.baltimoresun.com/2005-12-21/news/0512210353_1_surveillance-al-qaida-domestic-spying
20. <http://www.nbcnews.com/id/5486840/#.UcHqfvF1FA>
21. <http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all>
22. http://www.propublica.org/forms/newsletter_daily_email?utm_campaign=subscribe&utm_source=propublica&utm_medium=article&utm_term=footer

© Copyright 2013 Pro Publica Inc.

Steal Our Stories

Unless otherwise noted, you can republish our stories for free if you [follow these rules](#).



Exhibit 10

Exhibit 10



No NSA Poster Child: The Real Story of 9/11 Hijacker Khalid al-Mihdhar

By Michael German

October 16, 2013

Since whistleblower Edward Snowden exposed the incredible scope of the government's domestic spying programs, two different narratives are moving forward in Congress.

One, expressed most recently by Sen. Dianne Feinstein, D-Calif., in the *Wall Street Journal*, argues that the government's collection of all Americans' calling data "is necessary and must be preserved if we are to prevent terrorist attacks."

The other, offered by Sen. Ron Wyden, D-Ore., Rep. James Sensenbrenner, R-Ohio, and others is that the Justice Department, National Security Agency and FBI have repeatedly misled members of Congress and the public about the nature of their spying programs, as well as their effectiveness, and they need to be reined in to protect Americans' rights.

Unfortunately for Feinstein, a simple review of the facts she marshals to support her position reveals a total reliance on dubious intelligence community statements that have already been widely debunked. The actual facts make clear that the NSA doesn't need an enormous database of everyone's phone records to track a discrete number of terrorists -- the NSA just needs to use the traditional tools it has to investigate its targets.

Feinstein's first claim, based on recent testimony from FBI Director Robert Mueller and the NSA's director, Gen. Keith Alexander, is that the domestic telephone data collection program would have enabled the intelligence community to prevent the 9/11 attacks by revealing that al-Qaeda operative and future 9/11 hijacker Khalid al Mihdhar was inside the United States. On June 12, 2013, Alexander told the Senate Appropriations Committee:

"We all had this concern coming out of 9/11: How are we going to protect the nation? Because we did get intercepts on Mihdhar, but we didn't know where he was. We didn't have the data collected to know that he was a bad person. And because he was in the United States, the way we treat it is he's a U.S. person. So we had no information on that."

Mueller made a similar statement the following day in testimony to the House Judiciary Committee:

"[Khalid al-Mihdhar] was being tracked by the intelligence agencies in the Far East. They lost track of him. At the same time, the intelligence agencies had identified an al Qaeda safe house in Yemen. They understood that the al-Qaeda safe house had a telephone, but they could not know who was calling into that particular safe

house. We came to find out afterwards that the person who had called into that safe house was al-Mihdhar, who was in the United States in San Diego. If we had this program in place at the time, we would have been able to identify that particular telephone number in San Diego.”

The Justice Department previously made this claim in classified talking points provided to the Senate and House Intelligence Committees in 2009, and again in 2011, as Congress was locked in a debate over reauthorizing the Patriot Act.

There are a few problems with using Mihdhar as the poster child for new domestic spying programs, however. The intelligence agencies, which normally benefit from being able to keep secret any facts that might undermine their arguments, seem to have forgotten that the 9/11 Commission, the Justice Department Inspector General and the intelligence committees in Congress published in detail what the government knew about Mihdhar before the attacks. It turns out that the NSA was intercepting calls to the al Qaeda safe house in Yemen as early as 1999, and both the FBI and CIA knew Mihdhar was an al Qaeda operative long before the 9/11 attacks.

The safe house was discovered during the FBI’s investigation into the 1998 bombings of two U.S. embassies in East Africa, and had been monitored by the NSA and CIA ever since. The inspector general’s report couldn’t be clearer that the intercepts were being broadly shared:

“The NSA’s reporting about these communications was sent, among other places, to FBI Headquarters, the FBI’s Washington and New York Field Offices, and the CIA’s CTC. At the FBI, this information appeared in the daily threat update to the Director on January 4, 2000.”

Intercepted communications from this location allowed the CIA to follow Mihdhar to an al Qaeda meeting in Kuala Lumpur in January 2000. Though they lost him in Thailand, as Mueller suggested, the CIA knew he had a visa to enter the United States and that his travel companion and fellow hijacker, Nawaf al Hazmi, had a plane ticket to fly to Los Angeles.

The CIA, however, failed to place Mihdhar on a watch list or “notify the FBI when it learned Mihdhar possessed a valid U.S. visa,” according to the 9/11 Commission report. The inspector general’s report revealed that five FBI officials assigned to the CIA Counterterrorism Center viewed CIA cables indicating Mihdhar had a U.S. visa. A week after the Kuala Lumpur meeting, Mihdhar and Hazmi flew into Los Angeles International Airport and entered the United States without a problem. After their entrance, the NSA would intercept at least six calls from the al Qaida safe house in Yemen to the United States, according to the Los Angeles Times.

By all accounts FBI officials knew Mihdhar had a visa to enter the United States by July 2001, and knew he was in the United States by August 22, 2001. As the Joint Intelligence Committee investigation found:

“A review was launched at CIA of all cables regarding the Malaysia meeting. The task fell largely to an FBI analyst assigned to CTC. On August 21, 2001, the analyst put together two key pieces of information: the intelligence the CIA received in January 2000 that al-Mihdhar had a multiple entry visa to the United States, and the information it received in March 2000 that al Hazmi had traveled to the United States. Working with an INS representative assigned to CTC, the analyst learned that al-Mihdhar had entered the United States on January 15, 2000, had departed on June 10, and had re-entered the United States on July 4, 2001.”

Yet neither the FBI nor NSA apparently attempted to trace the calls coming into the al Qaeda safe house until after 9/11, when telephone toll records obtained by the FBI confirmed Mihdhar made the calls.

In other words, the problem was not that the government lacked the right tools to do its job (it had ample authority to trace Mihdhar's calls). The problem was that the government apparently failed to use them.

It's pretty cynical for the intelligence community to use its repeated failures to properly assess information it collected prior to 9/11 as justification for wholesale spying on Americans. But Feinstein's continuing reliance on the Mihdhar canard is even more inexplicable given that ProPublica published [an article thoroughly rebutting these claims](#) shortly after Alexander's and Mueller's June 2013 testimony. It's troubling when the Senate Intelligence Committee Chairwoman ignores more accurate information from public sources in deference to U.S. intelligence agencies, which have not only misled members of Congress but the Foreign Intelligence Surveillance Court, as well.

But Feinstein doesn't only peddle falsehoods from the past. She then points to the NSA's claim that dozens of terrorist events were disrupted through these domestic spying programs, though this too was publicly debunked. During a Senate Judiciary Committee hearing on Oct. 2, 2013, Sen. Patrick Leahy, D-Vt., questioned Alexander directly on the NSA's claims that these programs prevented 54 terrorist plots. Leahy called them "plainly wrong" and pointed out that the listed incidents "weren't all plots and they weren't all thwarted." Only 13 had any nexus to the U.S. and only one case relied on the bulk call records' program in a significant way. And even that case didn't involve any plot on the US -- it involved a material support prosecution relating to someone who allegedly sent \$8500 to al Shabaab in Somalia.

Alexander sheepishly agreed with Sen. Leahy's analysis, leading the senator to tell the NSA director that the government's use of inaccurate statistics undermined its credibility with Congress and the American people. Feinstein was on hand when Alexander admitted to Leahy that these statistics were misleading.

These repeated efforts to mislead Congress and the American people only make the case more strongly that the government's surveillance authorities need to be sharply curbed with strong legislation that ends the bulk collection programs, protects Americans' private communications and adds more transparency and public accountability to these activities. Americans have the right to truthful information about their government's intelligence activities, and the current oversight system, which depends on whistleblowers willing to risk jail, certainly isn't working.

Michael German is a senior policy counsel at the ACLU's Washington Legislative Office and a former FBI agent.

By Michael German // Michael German is a senior policy counsel at the ACLU's Washington Legislative Office and a former FBI agent.
October 16, 2013

<http://www.defenseone.com/ideas/2013/10/no-nsa-poster-child-real-story-911-hijacker-khalid-al-mihdhar/72047/>