

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

AMERICAN CIVIL LIBERTIES UNION;
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION; NEW YORK CIVIL
LIBERTIES UNION; and NEW YORK
CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs,

v.

JAMES R. CLAPPER, in his official capacity
as Director of National Intelligence; KEITH
B. ALEXANDER, in his official capacity as
Director of the National Security Agency and
Chief of the Central Security Service;
CHARLES T. HAGEL, in his official
capacity as Secretary of Defense; ERIC H.
HOLDER, in his official capacity as Attorney
General of the United States; and ROBERT S.
MUELLER III, in his official capacity as
Director of the Federal Bureau of
Investigation,

Defendants.

13 Civ. 3994 (WHP)

ECF Case

Notice of Motion

PLEASE TAKE NOTICE that upon the accompanying memorandum of law in support of defendants' motion to dismiss the complaint, dated August 26, 2013, and the exhibits thereto, defendants James R. Clapper, in his official capacity as Director of National Intelligence; Keith B. Alexander, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; Charles T. Hagel, in his official capacity as Secretary of Defense; Eric H. Holder, in his official capacity as Attorney General of the United States; and Robert S. Mueller, in his official capacity as Director of the Federal Bureau of Investigation, will move this Court, before the Honorable William J. Pauley, at the United States Courthouse, 500 Pearl Street,

New York, New York, for an Order dismissing the complaint pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure.

PLEASE TAKE FURTHER NOTICE that pursuant to the Court's Corrected Scheduling Order dated August 8, 2013, opposition papers, if any, are to be served on or before September 26, 2013.

Dated: New York, New York
August 26, 2013

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director

ANTHONY J. COPPOLINO
Deputy Director

By: /s/ James Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel

BRYAN DEARINGER
Trial Attorney

Civil Division,
Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Avenue, N.W.
Washington, DC 20001
Tel.: (202) 514-3358

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for Defendants

By: /s/ David S. Jones
DAVID S. JONES
TARA M. La MORTE
JOHN D. CLOPPER
CHRISTOPHER HARWOOD
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel. (212) 637-
2739/2746/2716/2728
Fax (212) 637-2730
david.jones6@usdoj.gov
tara.lamorte2@usdoj.gov
john.clopper@usdoj.gov
christopher.harwood@usdoj.gov

Multiple Documents

Part	Description
1	52 pages
2	Exhibit 1
3	Exhibit 2
4	Exhibit 3
5	Exhibit 4
6	Exhibit 5
7	Exhibit 6
8	Exhibit 7
9	Exhibit 8
10	Exhibit 9
11	Exhibit 10
12	Exhibit 11
13	Exhibit 12
14	Exhibit 13

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

AMERICAN CIVIL LIBERTIES UNION; AMERICAN
CIVIL LIBERTIES UNION FOUNDATION; NEW YORK
CIVIL LIBERTIES UNION; and NEW YORK CIVIL
LIBERTIES UNION FOUNDATION,

Plaintiffs,

v.

JAMES R. CLAPPER, in his official capacity as Director
of National Intelligence; KEITH B. ALEXANDER, in his
official capacity as Director of the National Security
Agency and Chief of the Central Security Service;
CHARLES T. HAGEL, in his official capacity as Secretary
of Defense; ERIC H. HOLDER, in his official capacity as
Attorney General of the United States; and ROBERT S.
MUELLER III, in his official capacity as Director of the
Federal Bureau of Investigation,

Defendants.

13 Civ. 3994 (WHP)
ECF Case

**DEFENDANTS' MEMORANDUM OF LAW
IN SUPPORT OF MOTION TO DISMISS THE COMPLAINT**

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director

ANTHONY J. COPPOLINO
Deputy Director

JAMES J. GILLIGAN
Special Litigation Counsel

MARCIA BERMAN
Senior Trial Counsel

BRYAN DEARINGER
Trial Attorney
U.S. Department of Justice
Washington, D.C.

PREET BHARARA
United States Attorney for
the Southern District of New York

DAVID S. JONES
TARA M. La MORTE
JOHN D. CLOPPER
CHRISTOPHER HARWOOD
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
Tel. No. (212) 637-2739 (Jones)
Fax No. (212) 637-2730
david.jones6@usdoj.gov
tara.lamorte2@usdoj.gov
john.clopper@usdoj.gov
christopher.harwood@usdoj.gov

TABLE OF CONTENTS

	Page
PRELIMINARY STATEMENT.....	1
STATEMENT OF FACTS.....	2
A. Statutory Background.....	2
B. The Collection of Telephony Metadata Records Authorized by the FISC.....	4
C. Plaintiffs’ Allegations.....	7
ARGUMENT.....	9
POINT I: THE COMPLAINT SHOULD BE DISMISSED BECAUSE PLAINTIFFS HAVE NOT ESTABLISHED THEIR STANDING	9
A. The Requirements of Article III Standing	9
B. Plaintiffs Allege Injuries That Are Speculative and Conjectural, Not Certainly Impending.....	11
POINT II: CONGRESS IMPLIEDLY PRECLUDED JUDICIAL REVIEW OF PLAINTIFFS’ STATUTORY CLAIM	14
POINT III: THE GOVERNMENT’S BULK COLLECTION OF TELEPHONY METADATA IS AUTHORIZED UNDER SECTION 215.....	19
A. The Telephony Metadata Collected Under the FISC’s Orders Are “Relevant” to Authorized National Security Investigations	20
1. Congress Intended Section 215 To Incorporate a Broad Concept of Relevance, Drawn from the Legal Meaning Applied in Grand Jury, Civil, and Administrative Proceedings, That Also Takes Into Account the Special Characteristics of the Terrorism Investigations to Which It Applies.....	21
2. Congress Has Legislatively Ratified the Construction of Section 215 as Allowing for the Bulk Collection of Telephony Metadata Records.....	26

3. Telephony Metadata Are “Relevant” Within the
Meaning of Section 215 Because Bulk Collection of
the Data Enhances the Government’s Ability To Detect
Terrorist Operatives and Prevent Terrorist Attacks..... 28

B. Nothing in the Text of Section 215 Prohibits the Collection
of Records “as They Are Generated” 29

POINT IV: THE GOVERNMENT’S COLLECTION OF TELEPHONY
METADATA DOES NOT VIOLATE PLAINTIFFS’ FOURTH
AMENDMENT RIGHTS 31

A. Plaintiffs Have No Fourth Amendment Privacy Interest in Telephony
Metadata..... 31

B. The Government’s Acquisition of Metadata Is Reasonable..... 35

POINT V: PLAINTIFFS HAVE NOT PLAUSIBLY ALLEGED THAT THE
GOVERNMENT’S COLLECTION OF TELEPHONY METADATA
VIOLATES THE FIRST AMENDMENT 37

A. Plaintiffs’ Failure To Allege An Actionable Fourth Amendment Claim
Is Also Fatal To Their First Amendment Claim 37

B. Plaintiffs Make No Allegations That the Government’s Collection of
Telephony Metadata Is Intended to Curtail Protected Expressive or
Associational Activity..... 39

CONCLUSION..... 40

TABLE OF AUTHORITIES

<i>Cases</i>	<i>Page(s)</i>
<i>ACLU Found. of S. California v. Barr</i> , 952 F.2d 457 (D.C. Cir. 1991)	38
<i>Am. Civil Liberties Union v. Nat'l Sec. Agency</i> , 493 F.3d 644 (6th Cir. 2007)	38
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	<i>passim</i>
<i>Atkins v. Parker</i> , 472 U.S. 115 (1985)	28
<i>Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls</i> , 536 U.S. 822 (2002)	36
<i>Block v. Cmty. Nutrition Inst.</i> , 467 U.S. 340 (1984)	16, 19
<i>Block v. N. Dakota ex rel. Bd. of Univ. & Sch. Lands</i> , 461 U.S. 273 (1983)	16
<i>C.I.A. v. Sims</i> , 471 U.S. 159 (1985)	25
<i>Carrillo Huettel, LLP v. U.S. S.E.C.</i> , 2011 WL 601369 (S.D. Cal. Feb. 11, 2011)	22
<i>Chambers v. Time Warner, Inc.</i> , 282 F.3d 147 (2d Cir. 2002)	5, 6
<i>Clapper v. Amnesty Int'l USA</i> , 133 S. Ct. 1138 (2013)	<i>passim</i>
<i>Conopco, Inc. v. Roll Int'l</i> , 231 F.3d 82 (2d Cir. 2000)	5
<i>DaimlerChrysler Corp. v. Cuno</i> , 547 U.S. 332 (2006)	9, 10
<i>Dew v. United States</i> , 192 F.3d 366 (2d Cir. 1999)	19
<i>E.E.O.C. v. Shell Oil Co.</i> , 466 U.S. 54 (1984)	21, 28

<i>F.A.A. v. Cooper</i> , 132 S. Ct. 1441 (2012)	15
<i>F.T.C. v. Invention Submission Corp.</i> , 965 F.2d 1086 (D.C. Cir. 1992)	22
<i>FDIC v. Meyer</i> , 510 U.S. 471 (1994)	15
<i>Forest Grove Sch. Dist. v. T.A.</i> , 557 U.S. 230 (2009)	28
<i>Gordon v. Warren Consol. Bd. of Educ.</i> , 706 F.2d 778 (6th Cir. 1983)	38
<i>Goshawk Dedicated Ltd. v. Am. Viatical Servs., LLC</i> , 2007 WL 3492762 (N.D. Ga. Nov. 5, 2007)	22
<i>Guest v. Leis</i> , 255 F.3d 325 (6th Cir. 2001)	33
<i>Haig v. Agee</i> , 453 U.S. 280 (1981)	28, 36
<i>In re Adelphia Commc'ns Corp.</i> , 338 B.R. 546 (Bankr. S.D.N.Y. 2005)	22
<i>In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)</i> 830 F. Supp. 2d 114 (E.D. Va. 2011)	19, 33
<i>In re Application of the United States</i> , 632 F. Supp. 2d 202 (E.D.N.Y. 2008)	30
<i>In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.</i> , 460 F. Supp. 2d 448 (S.D.N.Y. 2006)	30
<i>In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act</i> , 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008)	36
<i>In re Grand Jury Proceedings</i> , 616 F.3d 1186 (10th Cir. 2010)	21
<i>In re Grand Jury Proceedings: Subpoenas Duces Tecum</i> , 827 F.2d 301 (8th Cir. 1987)	22, 35
<i>In re Motion for Release of Court Records</i> , 526 F. Supp. 2d 484 (Foreign Intel. Surv. Ct. 2007)	3

<i>In re Subpoena Duces Tecum</i> , 228 F.3d 341 (4th Cir. 2000)	22
<i>Jabara v. Kelley</i> , 476 F. Supp. 561 (E.D. Mich. 1979).....	38
<i>Jewel v. Nat'l Sec. Agency</i> , 2013 WL 3829405 (N.D. Cal. July 23, 2013).....	17
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	32
<i>Kiobel v. Royal Dutch Petroleum Co.</i> , 621 F.3d 111(2d Cir. 2010).....	7
<i>Laird v. Tatum</i> , 408 U.S. 1 (1972).....	14, 39
<i>Langford v. Chrysler Motors Corp.</i> , 513 F.2d 1121 (2d Cir. 1975).....	19
<i>Lorillard v. Pons</i> , 434 U.S. 575 (U.S. 1978).....	28
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992).....	10, 14
<i>Maryland v. King</i> , 133 S. Ct. 1958 (2013).....	35, 36
<i>Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak</i> , 132 S. Ct. 2199 (2012).....	15-16
<i>McLean v. United States</i> , 566 F.3d 391 (4th Cir. 2009)	23
<i>Medtronic Sofamor Danek, Inc. v. Michelson</i> , 229 F.R.D. 550 (W.D. Tenn. 2003)	22
<i>Members of City Council of City of Los Angeles v. Taxpayers for Vincent</i> , 466 U.S. 789 (1984).....	39
<i>Michigan Dep't of State Police v. Sitz</i> , 496 U.S. 444 (1990).....	36, 37
<i>Minnesota v. Carter</i> , 525 U.S. 83 (1998)	35

<i>N.L.R.B. v. Am. Med. Response, Inc.</i> , 438 F.3d 188 (2d Cir. 2006).....	21, 23
<i>N.L.R.B. v. Amax Coal Co.</i> , 453 U.S. 322 (1981).....	22
<i>Oklahoma Press Pub. Co. v. Walling</i> , 327 U.S. 186 (1946).....	25, 29
<i>Oneida Indian Nation of New York v. State of N.Y.</i> , 691 F.2d 1070 (2d Cir. 1982).....	27
<i>Oppenheimer Fund, Inc. v. Sanders</i> , 437 U.S. 340 (1978).....	21
<i>PBGC. ex rel. St. Vincent Catholic Med. Centers Ret. Plan v. Morgan Stanley Inv. Mgmt. Inc.</i> , 712 F.3d 705 (2d Cir. 2013)	9
<i>Port Washington Teachers' Ass'n v. Bd. of Educ. of Port Washington Union free Sch. Dist.</i> , 478 F.3d 494 (2d Cir. 2007).....	14
<i>Quon v. Arch Wireless Operating Co., Inc.</i> , 529 F.3d 892 (9th Cir. 2008)	33
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978).....	35
<i>Redd v. City of Enter.</i> , 140 F.3d 1378 (11th Cir. 1998)	38
<i>Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co.</i> , 593 F.2d 1030 (D.C. Cir. 1978).....	38, 39, 40
<i>S.E.C. v. Jerry T. O'Brien, Inc.</i> , 467 U.S. 735 (1984).....	34
<i>Smith v. Bowersox</i> , 159 F.3d 345 (8th Cir. 1998)	23
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	<i>passim</i>
<i>Socialist Workers Party v. Attorney Gen. of U.S.</i> , 510 F.2d 253 (2d Cir. 1974).....	39
<i>Steagald v. United States</i> , 451 U.S. 204 (1981).....	35

<i>Steel Co. v. Citizens for a Better Env't</i> , 523 U.S. 83 (1998).....	10
<i>United States v. Aguilar</i> , 883 F.2d 662 (9th Cir. 1989)	39
<i>United States v. Anderson-Bagshaw</i> , 2012 WL 774964 (N.D. Ohio Mar. 8, 2012)	34
<i>United States v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008)	33
<i>United States v. Gering</i> , 716 F.2d 615 (9th Cir. 1983)	38
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006)	22
<i>United States v. Jones</i> , 132 S. Ct. 945 (2012).....	32, 34
<i>United States v. Kennedy</i> , 81 F. Supp. 2d 1103 (D. Kan. 2000).....	33
<i>United States v. Martinez-Fuerte</i> , 428 U.S. 543 (1976).....	36, 37
<i>United States v. Mayer</i> , 503 F.3d 740 (9th Cir. 2007)	38
<i>United States v. Maynard</i> , 615 F.3d 544 (D.C. Cir. 2010).....	34
<i>United States v. Merrick Sponsor Corp.</i> , 421 F.2d 1076 (2d Cir. 1970).....	5
<i>United States v. Miller</i> , 425 U.S. 435 (1976)	18-19, 33, 34
<i>United States v. Mitchell</i> , 445 U.S. 535 (1980)	15
<i>United States v. R. Enterprises, Inc.</i> , 498 U.S. 292 (1991).....	21, 23
<i>United States v. Ramsey</i> , 431 U.S. 606 (1977).....	38

<i>United States v. Rigmaiden</i> , 2013 WL 1932800 (D. Ariz. May 8, 2013)	35
<i>United States v. Shabani</i> , 513 U.S. 10 (1994).....	23
<i>United States v. Smith</i> , 426 F.3d 567 (2d Cir. 2005).....	36
<i>United States v. Upham</i> , 168 F.3d 532 (1st Cir. 1999).....	22
<i>Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.</i> , 454 U.S. 464 (1982).....	9
<i>Vernonia Sch. Dist. 47J v. Acton</i> , 515 U.S. 646 (1995).....	35, 36
<i>Whitmore v. Arkansas</i> , 495 U.S. 149 (1990).....	10
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978).....	38, 39

STATUTES

5 U.S.C. § 701.....	15, 18
5 U.S.C. § 702.....	8, 15
18 U.S.C. § 2703.....	30
18 U.S.C. § 2712.....	16,17
50 U.S.C. § 1801.....	18
50 U.S.C. § 1803.....	3, 4
50 U.S.C. § 1806.....	17, 18
50 U.S.C. § 1821	18
50 U.S.C. § 1825	17, 18
50 U.S.C. § 1841	18
50 U.S.C. § 1845	17, 18

50 U.S.C. § 1861.....	<i>passim</i>
50 U.S.C. § 1862.....	7, 26
50 U.S.C. § 1871.....	7, 27
50 U.S.C. § 1881a.....	12

RULES AND REGULATIONS

47 C.F.R. § 42.6.....	30
-----------------------	----

FEDERAL RULES OF CIVIL PROCEDURE

Fed. R. Civ. P. 12(b)(6).....	7
Fed. R. Civ. P. 26(b)(1).....	24

FEDERAL RULES OF CRIMINAL PROCEDURE

Fed. R. Crim. P. 41(e)(2)(B).....	22
-----------------------------------	----

LEGISLATIVE MATERIAL

S. 2369, 109th Cong., 2d Sess. (2006)	24
S. Rep. No. 109-85 (2005)	26
S. Rep. No. 111-92 (2009)	28
S. Rep. No. 112-13 (2011)	28
H.R. Rep. No. 94-1656 (1976)	16
H.R. Rep. 109-174 (2005).....	18, 23, 25, 26
151 Cong. Rec. S13636 (Dec. 15, 2005)	23
151 Cong. Rec. S14275-01 (2005)	24
152 Cong. Rec. H581-02 (2006)	24
152 Cong. Rec. S1325 (Feb. 15, 2006)	25
152 Cong. Rec. S1379 (Feb. 16, 2006).....	23

152 Cong. Rec. S1598-03 (2006)	23, 24
156 Cong. Rec. H838 (Feb. 25, 2010)	27
156 Cong. Rec. S2109 (Mar. 25, 2010)	27

OTHER AUTHORITIES

D. Kris & J. Wilson, <i>National Security Investigations & Prosecutions</i> (2d ed. 2012)	4, 17
---	-------

PRELIMINARY STATEMENT

Plaintiffs seek to invalidate an important element of the Government's efforts to protect the Nation from the very real and unrelenting threat of terrorist attack. Specifically, Plaintiffs challenge the Government's bulk collection of "telephony metadata," business records created by (and belonging to) telecommunications service providers that include such information as the time and duration of calls made, and the numbers dialed, but not the content of anyone's calls, or their names and addresses. Collection of these records, which has been repeatedly authorized by the Foreign Intelligence Surveillance Court (FISC) as consistent with governing law, permits National Security Agency (NSA) analysts, acting under strict controls imposed by FISC orders, to detect communications between foreign terrorists and any of their contacts located in the United States. Plaintiffs maintain that this activity is unauthorized by the Foreign Intelligence Surveillance Act (FISA), and violates the First and Fourth Amendments. For the reasons discussed herein, the Court lacks jurisdiction to entertain these claims, and Plaintiffs fail in any event to state claims on which relief can be granted. Thus, the Complaint should be dismissed.

First, Plaintiffs' Complaint fails to establish their standing to sue, as their alleged injuries are entirely speculative. The FISC's orders limit review of the metadata for intelligence purposes to those records responsive to queries conducted using identifiers (*e.g.*, telephone numbers) chosen based on reasonable, articulable suspicion that they are associated with foreign terrorist organizations approved for targeting by the FISC. There is no non-speculative basis to expect that queries of the metadata under this standard will return information about calls either made by Plaintiffs, or made to them by others. Thus, Plaintiffs' allegations that records of their calls could be used to glean sensitive information about their work and clients, and that persons with whom they collaborate could be "chilled" by that prospect from contacting them, are wholly conjectural. Second, Congress impliedly precluded review of Plaintiffs' statutory claim, that the

bulk collection of telephony metadata exceeds the Government's authority under FISA. FISA's detailed statutory scheme for judicial review of specified intelligence activities conducted under its purview reflects a Congressional purpose to preclude third parties such as Plaintiffs from mounting FISA-based challenges to FISC business records orders in federal district court.

Apart from these jurisdictional deficiencies, the Government's collection of telephony metadata is lawful under FISA and the Constitution, and the Complaint states no plausible claim to the contrary. As the FISC repeatedly has found (as recently as last month), telephony metadata are relevant to authorized counter-terrorism investigations, and their collection by the Government is authorized by FISA. Plaintiffs also fail to state a Fourth Amendment claim. There has been no search or seizure of their property or effects, and, as the Supreme Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), telephone subscribers have no protected privacy interest in the type of information at issue here. In addition, even if the Government's conduct implicated a protected Fourth Amendment interest, the bulk collection of telephony metadata would be "reasonable" and permissible in light of the strong national interest in preventing terrorist attacks, and the minimal intrusion on individual privacy. Finally, Plaintiffs fail to state a First Amendment claim, because intelligence-gathering conducted in a manner consistent with the Fourth Amendment, for purposes unrelated to the suppression of protected speech or association, does not violate the First Amendment. For these reasons, elaborated below, the Court should reject Plaintiffs' effort to preclude the use of this important intelligence tool.

STATEMENT OF FACTS

A. Statutory Background

Congress enacted FISA to authorize and regulate certain governmental surveillance of communications and other activities conducted for purposes of gathering foreign intelligence. In enacting FISA, Congress also created the FISC, an Article III court of 11 appointed U.S. district

judges with authority to consider applications for and grant orders authorizing electronic surveillance and other forms of intelligence-gathering by the Government. 50 U.S.C. § 1803(a); *see In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 486 (F.I.S.C. 2007).

At issue here is the “business records” provision of FISA, 50 U.S.C. § 1861, enacted by section 215 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (“Section 215”). Section 215 authorizes the FISC to issue an order for the “production of any tangible things (including books, records, papers, documents, and other items) for an investigation [1] to obtain foreign intelligence information not concerning a United States person or [2] to protect against international terrorism” (provided, in the case of a counter-terrorism investigation of a “United States person,” that “such investigation ... is not conducted solely upon the basis of activities protected by the first amendment to the Constitution”). 50 U.S.C. § 1861(a)(1). The records must be of a type obtainable by either a grand jury subpoena, or an order issued by a U.S. court directing the production of records or tangible things. *Id.* § 1861(c)(2)(D).

The Government’s application for an order under Section 215 must include, among other things, a statement of facts showing that there are “reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation ... to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism.” *Id.* § 1861(b)(2)(A). The investigation must be authorized and conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor thereto). *Id.* § 1861(a)(2)(A), (b)(2)(A). Information acquired from the records or other tangible items received in response to a Section 215 order “concerning any United States person may be used and disclosed by [the Government] without the consent of [that] person only in accordance with ... minimization procedures,” adopted by the Attorney General and enumerated in the Government’s application, that “minimize the retention, and prohibit the dissemination, of

nonpublicly available information concerning unconsenting United States persons consistent with the [Government's] need ... to obtain, produce, and disseminate foreign intelligence information.” *Id.* § 1861(b)(2)(B), (g)(2), (h). The FISC must find that these requirements have been met before it issues the requested order, which in turn must direct that the minimization procedures described in the application be followed. *Id.* § 1861(c)(1).

Section 215 includes a scheme providing for judicial review of a business records order, but only in limited circumstances. Specifically, it allows “[a] person receiving a production order [to] challenge the legality of that order” by filing a petition with the “review pool” of FISC judges designated under 50 U.S.C. § 1803(e)(1) to review production orders under Section 215. *Id.* § 1861(f)(1), (2)(A)(i). A “pool” judge considering a petition to modify or set aside a production order may grant the petition if the judge finds that the order does not meet the requirements of Section 215 or “is otherwise unlawful.” *Id.* § 1861(f)(2)(B). Thus, a production order can be set aside if it exceeds the authority conferred by Section 215 or is unconstitutional. 1 D. Kris & J. Wilson, *National Security Investigations & Prosecutions* § 19:10 at 714 (2d ed. 2012) (“Kris & Wilson”). Either the Government or a recipient of a production order may appeal the decision of the pool judge to the FISC Court of Review, with review available thereafter on writ of certiorari in the Supreme Court. 50 U.S.C. § 1861(f)(3); *see id.* § 1803(b). Section 215’s carefully circumscribed provisions for judicial review were added when Congress reauthorized the USA PATRIOT Act in 2006, and these provisions authorized contested litigation before the FISC for the first time. 1 Kris & Wilson §5:5, 19:7 (2d ed. 2012). The FISA does not provide for review of Section 215 orders at the behest of third parties.

B. The Collection of Telephony Metadata Records Authorized by the FISC

Plaintiffs challenge the Government’s exercise of authority, as reflected in a secondary order of the FISC, to collect telephony metadata records in bulk. Compl. ¶ 30, citing *In re*

Application of the FBI for an Order Requiring the Production of Tangible Things [etc.], Dkt. No. BR 13-80, Secondary Order 1-2 (F.I.S.C. Apr. 25, 2013) (the “Secondary Order”) (Exhibit 1, hereto). The Secondary Order was issued in conjunction with, and on the same day as, a primary order in which the FISC granted the Government’s application for production of these records, finding “reasonable grounds to believe that the [records] sought are relevant to authorized investigations ... being conducted by the FBI ... to protect against terrorism.” *In re Application of the FBI for an Order Requiring the Production of Tangible Things [etc.]*, Dkt. No. BR 13-80, Primary Order 1-2 (F.I.S.C. Apr. 25, 2013) (the “Primary Order”) (Exhibit 2, hereto).¹

These Orders directed the daily production to NSA of electronic copies of “all call detail records, or ‘telephony metadata,’” created by a recipient telecommunications service provider for calls to, from, or wholly within the United States. Primary Order at 3-4; Secondary Order at 1-2. “Telephony metadata” is defined by the Orders as “comprehensive communications routing information” including but not limited to “originating and terminating telephone number[s], International Mobile Subscriber Identity (IMSI) number[s], International Mobile Station Equipment Identity (IMEI) number[s], trunk identifier[s], telephone calling card numbers, and time and duration of call.” Primary Order at 3 n.1. By the express terms of the Orders, “[t]elephony metadata does not include the name, address, or financial information of a subscriber or customer.” *Id.*; Secondary Order at 2. The Court’s Orders do not permit the Government to listen to or record the contents of any telephone conversations.

As required by FISA, the terms of the Primary Order direct the Government to comply with “minimization procedures” that strictly limit the extent to which information received under

¹ The Court may consider the Secondary Order on this motion, as it is specifically referenced in and integral to the Complaint. *See Chambers v. Time Warner, Inc.*, 282 F.3d 147, 152 (2d Cir. 2002). The Court may take judicial notice of the publicly available portions of the Primary Order as an official judicial act. *See Conopco, Inc. v. Roll Int’l*, 231 F.3d 82, 86 n.3 (2d Cir. 2000); *United States v. Merrick Sponsor Corp.*, 421 F.2d 1076, 1079 n.2 (2d Cir. 1970).

the FISC's Orders can be reviewed, used, or disseminated, and prevent Government personnel from indiscriminately sifting through the data. *See* 50 U.S.C § 1861(b)(2)(B), (g)-(h); Primary Order at 4-14. The metadata must be stored by NSA in secure networks with access restricted to authorized personnel who have received appropriate training. Primary Order at 4-5. NSA analysts may "query" (electronically search) the metadata "for purposes of obtaining foreign intelligence information" – that is, to identify terrorism-related communications – only when there is reasonable, articulable suspicion, based on specific facts, that the "identifier" (*e.g.*, a telephone number) used to query the database is associated with a specific foreign terrorist organization that was previously identified to and approved for targeting by the FISC. Primary Order at 6-8; DNI Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013) ("DNI Statement") (Exhibit 3, hereto) at 2.² Only a small number of NSA officials designated by the Primary Order are authorized to make findings of reasonable, articulable suspicion, and NSA's Office of General Counsel (OGC) must review such findings for numbers reasonably believed to be used by United States persons, to ensure the findings are not based on activities protected by the First Amendment. Primary Order at 7-9. Although the FISC has authorized the collection and maintenance of large amounts of metadata, only those records responsive to queries based on approved identifiers may be disseminated. *See id.* at 12-13. Therefore, "only a small fraction of the records are ever reviewed." DNI Statement at 2.

The results of these "contact-chaining queries," Primary Order at 6, following analysis by NSA, may be shared with the FBI and allow Government investigators to discover persons, including persons (and associates of persons) located in the United States, who have been in contact with known or suspected terrorist organizations and may themselves be engaged in

² The Court may consider this statement on the Government's motion to dismiss because it is a document "of which [P]laintiffs had possession and relied on in bringing suit." *Chambers*, 282 F.3d at 152 (internal quotation marks and citation omitted); *see* Compl. ¶ 31.

terrorist activity. DNI Statement at 1-2; *see* Primary Order at 4. However, before the NSA may disseminate information about a U.S. person outside the agency, a high-ranking NSA official “must determine that the information identifying the U.S. person is in fact related to counterterrorism information and is necessary to understand the counterterrorism information or assess its importance.” Primary Order at 13. The FBI, in turn, must handle the information it receives from NSA in accordance with the minimization procedures set forth in *The Attorney General’s Guidelines for Domestic Operations*. *Id.* at 4.

The NSA’s activities under the FISC’s Orders are subject, in addition, to an extensive regime of internal reporting, audits, and oversight; regular consultation with the NSA Office of the Inspector General, and the Department of Justice, to assess compliance with the FISC’s Orders; and monthly reports to the FISC including, *inter alia*, a discussion of NSA’s application of the “reasonable, articulable suspicion” standard and the number of times that query results containing U.S. person information have been shared with anyone outside NSA. *Id.* at 4-16. As acknowledged in the Complaint, ¶ 31, the FISC must renew Government’s authority to collect telephony metadata under its orders every 90 days. *See* Primary Order at 17 (setting expiration date of collection authority); Secondary Order at 4 (same).³

C. Plaintiffs’ Allegations⁴

Plaintiffs are non-profit organizations that engage in civil rights litigation, education, and lobbying. Compl. ¶¶ 6-9, 24. They allege that the Government has engaged in “dragnet

³ FISA also requires the Government to report to Congress regarding the use of its Section 215 authority, including copies of significant FISC orders and the Government’s supporting pleadings. 50 U.S.C. §§ 1862, 1871.

⁴ For purposes of a motion to dismiss under Fed. R. Civ. P. 12(b)(6), the well-pleaded factual allegations of a complaint must be accepted as true. *Kiobel v. Royal Dutch Petroleum Co.*, 621 F.3d 111, 124 (2d Cir. 2010). Defendants reserve the right, however, to contest Plaintiffs’ allegations, and/or their ability to prove their allegations without implicating protected state secrets, as may be necessary or appropriate in further proceedings.

acquisition” of telephony metadata concerning their communications, *id.* ¶¶ 1-2, 30, although they acknowledge that the collection of the metadata is court-authorized. *Id.* ¶¶ 2, 22, 23, 31.

Plaintiffs contend that the telephony metadata provide the government with “a comprehensive record” of “sensitive and often privileged” information about their communications with “journalists, current and potential clients, legislators and legislative staff, and members of the public,” concerning “Plaintiffs’ advocacy, representation of clients, and efforts to lobby Congress.” Compl. ¶¶ 3, 24-25, 35. These include communications with potential witnesses and informants, whistleblowers, and lobbyists who consider their associations with Plaintiffs confidential. *Id.* ¶¶ 26-27. Plaintiffs specifically allege that the telephony metadata maintained by the Government “could readily be used to identify those who contact Plaintiffs for legal assistance or to report human-rights or civil-liberties violations, as well as those whom Plaintiffs contact in connection with their work.” *Id.* ¶¶ 1, 35. Therefore, the Government’s maintenance of these records, according to Plaintiffs, “is likely to have a chilling effect on whistleblowers and others who would otherwise contact Plaintiffs.” *Id.* ¶¶ 3, 35. Plaintiffs make no allegations, however, that the Government has reviewed metadata of any of their communications, whether pursuant to queries based on reasonable, articulable suspicion that particular telephone numbers (or other identifiers) are associated with specific foreign terrorist organizations approved for targeting by the FISC, or otherwise.

Plaintiffs contend that this court-sanctioned collection of telephony metadata exceeds the authority conferred by Section 215, and violates the First and Fourth Amendments. *Id.* ¶¶ 36-38. They bring suit under the Declaratory Judgment Act, 28 U.S.C. §§ 2201-2202, predicated jurisdiction on, *inter alia*, the waiver of sovereign immunity codified in the Administrative Procedure Act, 5 U.S.C. § 702. *Id.* ¶ 4. Plaintiffs seek a declaration that the telephony metadata collection is unlawful; a permanent injunction against future collection of telephony metadata

concerning their communications, whether under the Secondary Order “or any successor thereto”; and an order directing the Government “to purge from [its] possession” all such metadata collected to date. *Id.* at 10 (Prayer for Relief ¶¶ 2-5).

ARGUMENT

Under the pleading standards set forth in *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009), to survive a motion to dismiss a complaint must contain “sufficient factual matter, accepted as true, to state a claim that is plausible on its face.” Mere “labels and conclusions,” and “naked assertion[s] devoid of further factual enhancement,” are not sufficient. Rather, considering only the well-pleaded, non-conclusory allegations of a complaint, and “assum[ing] their veracity,” the court must determine whether they “plausibly give rise to an entitlement to relief.” *Id.* at 678-79 (internal quotations omitted), *see id.* at 680-81; *PBGC ex rel. St. Vincent Catholic Med. Ctr. Ret. Plan v. Morgan Stanley Inv. Mgmt., Inc.*, 712 F.3d 705, 717 (2d Cir. 2013) (“*St. Vincent*”). To reach the level of plausibility, the well-pleaded facts “must demonstrate ‘more than a sheer possibility that a defendant has acted unlawfully.’” *St. Vincent*, 712 F.3d at 717 (quoting *Iqbal*, 556 U.S. at 678). Facts that “are merely consistent with” a defendant’s liability “stop[] short of the line between possibility and plausibility.” *Iqbal*, 556 U.S. at 678; *St. Vincent*, 712 F.3d at 717. The Complaint in this case falls well short of that line, and must be dismissed.

POINT I: THE COMPLAINT SHOULD BE DISMISSED BECAUSE PLAINTIFFS HAVE NOT ESTABLISHED THEIR STANDING

A. The Requirements of Article III Standing

“The judicial power of the United States” is limited by Article III of the Constitution “to the resolution of ‘cases’ and ‘controversies.’” *Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 471 (1982). “No principle is more fundamental to the judiciary’s proper role in our system of government.” *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 341 (2006) (internal quotation marks and citation omitted). A

demonstration by plaintiffs of their standing to sue “is an essential and unchanging part of the case-or-controversy requirement,” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992), “serv[ing] to prevent the judicial process from being used to usurp the powers of the political branches.” *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1146 (2013) (citations omitted). The “standing inquiry has been especially rigorous when reaching the merits of the dispute would force [a court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional.” *Id.* at 1147 (citations and quotations omitted). Similarly, as the Supreme Court recently observed in *Amnesty Int’l*, it has “often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs.” *Id.*

To establish Article III standing, Plaintiffs must seek relief from an injury that is “‘concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.’” *Id.* Although “imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes – that the injury is *certainly* impending.” *Id.* (citations and internal quotation marks omitted); *see also id.* (“‘threatened injury must be *certainly impending* to constitute injury in fact,’” and “[a]llegations of *possible* future injury’ are not sufficient” (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990), and citing multiple additional cases)); *see also DaimlerChrysler*, 547 U.S. at 345. If Plaintiffs cannot carry the threshold jurisdictional burden of adequately pleading their standing to sue, *see Defenders of Wildlife*, 504 U.S. at 561, then “the [C]ourt cannot proceed” and must dismiss the case. *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 94 (1998).

B. Plaintiffs Allege Injuries That Are Speculative and Conjectural, Not Certainly Impending

The Complaint should be dismissed because Plaintiffs have failed to plausibly allege an injury meeting Article III's standards. As discussed below, Plaintiffs' allegations of the consequences they will suffer as a result of the challenged intelligence-gathering activities depend on speculation that the Government has reviewed, or might in future review, call detail records of their communications, and that persons who would otherwise contact Plaintiffs by telephone may be "chilled" from doing so by that conjectural prospect. Such speculation is insufficient for purposes of Article III, and, as a result, Plaintiffs lack standing.

Plaintiffs' allegations of injury stem from their assertion that for purposes of civil rights litigation, education, and lobbying they engage in "sensitive" and "privileged" communications with clients, witnesses, whistleblowers, and other persons who consider their associations and "even the fact of their discussions" with Plaintiffs to be confidential. Compl. ¶¶ 3, 6-9, 24-27. They allege that metadata records of their calls "could readily be used to identify those who contact Plaintiffs for legal assistance or to report human-rights or civil-liberties violations, as well as those whom Plaintiffs contact in connection with their work." *Id.* ¶ 35. On the basis that records of their calls "could readily be used" for this purpose, Plaintiffs allege further that the Government's acquisition of such records "is likely to have a chilling effect on people who would otherwise contact Plaintiffs." *Id.* These allegations are too conjectural to demonstrate that "the threatened injur[ies] [are] certainly impending." *Amnesty Int'l*, 133 S. Ct. at 1147.

Plaintiffs' first alleged harm, the potential use of call detail records to identify persons with whom Plaintiffs speak, cannot support their standing. Government personnel could identify persons with whom Plaintiffs speak by phone, either individually or collectively, only by retrieving and reviewing the metadata records of calls to or from Plaintiffs (and then taking the next step of ascertaining the identities of the subscribers whose numbers are memorialized in the

records). But under the FISC's Orders, Government personnel may only review records responsive to queries initiated using identifiers that are believed, based on reasonable, articulable suspicion, to be associated with specific foreign terrorist organizations approved for targeting by the FISC. *See supra* at 6; Primary Order at 7. The Complaint contains no allegations, much less well-pleaded, non-conclusory allegations, that the Government has accessed or reviewed metadata records of Plaintiffs' calls as a result of queries made under the "reasonable, articulable suspicion" standard (or otherwise). Thus, it is sheer speculation to suggest that metadata records of calls to or from Plaintiffs either have been or ever will be retrieved or reviewed through queries of the database, much less mined by the Government "to learn sensitive and privilege information about [Plaintiffs'] work and clients." Compl. ¶ 3.⁵

The Supreme Court's decision in *Amnesty Int'l* addressed a similar standing question and establishes that Plaintiffs' reliance on speculation concerning the reach of Government intelligence-gathering activities is insufficient to demonstrate their standing. In *Amnesty Int'l*, various human rights, labor, and media organizations challenged the constitutionality of the FISA Amendments Act of 2008, which expanded the Government's authority to intercept the communications of non-U.S. persons located abroad. 133 S. Ct. at 1144. The organizations alleged that they interacted and engaged in sensitive communications with persons who were likely to be considered by the Government as potential terrorists, or persons of interest in

⁵ In a 2011 FISC opinion recently declassified and publicly released by the Government (concerning the adequacy of the Government's minimization procedures for Internet communications data collected under authority of section 702 of FISA, 50 U.S.C. § 1881a), the FISC alluded to a 2009 opinion in which it found that, due to "misperceptions by the FISC" and "inaccurate statements made in the government's submissions," the "NSA had been routinely running queries of [telephony] metadata [collected under Section 215] using query terms that did not meet the required standard." October 3, 2011, FISC Memorandum Opinion and Order (Bates, J.) at 16 n.14 (available at <http://icontherecord.tumblr.com/tagged/declassified>). Any allegation by Plaintiffs, however, that past incidents of non-compliance with the "reasonable, articulable suspicion" standard make it likely that records of their calls have been or will be reviewed, would be equally speculative, and insufficient under Article III.

terrorism investigations. *See id.* at 1145-46. They further alleged that they would suffer harms as a result of the Government surveillance program, including a compromised ability to “locate witnesses, cultivate sources, obtain information, and communicate confidential information,” and a need to undertake various costly measures to avoid possible surveillance. *Id.*

The Supreme Court, however, held that none of these alleged harms was sufficient to confer standing, because it was “speculative whether the Government will imminently target communications to which respondents are parties.” *Id.* at 1148. Rather, the Court held that the plaintiffs’ harm rested on a “speculative chain of possibilities,” including “that the Government [would] target the communications of non-U.S. persons with whom they communicate,” that the Government would succeed in intercepting those communications, and that the plaintiffs would be parties to the particular communications the Government intercepts. *Id.* at 1148-50. So, too, here. The idea that the course of unspecified Government counter-terrorism investigations would lead to particular telephone numbers; that these numbers would be reasonably suspected of association with unidentified foreign terrorist organizations; that these numbers would be used to formulate queries of the collected telephony metadata; and that these queries would retrieve metadata records of Plaintiffs’ calls that the Government would in turn review, is just as speculative as the allegations of harm that were rejected as insufficient in *Amnesty Int’l.*

Equally unavailing as a claim of injury is the asserted possibility that others might refrain from communicating with Plaintiffs because they fear disclosure of their associations with Plaintiffs. Plaintiffs allege that, because the metadata records of their calls “could readily be used to identify” those with whom Plaintiffs communicate, individuals who would otherwise contact Plaintiffs will “likely” be chilled from doing so. Compl. ¶ 35. Plaintiffs’ burden, however, is to allege facts plausibly suggesting that their injury is certainly impending. *Iqbal*, 556 U.S. at 678; *Amnesty Int’l.* 133 S. Ct. at 1147. The “naked assertion,” *Iqbal*, 556 U.S. at

678, that unnamed individuals who regard their communications with Plaintiffs as “confidential” may be so unnerved by the idea of the Government reviewing telephony metadata that they will refrain from calling Plaintiffs does not suffice. The Complaint is “devoid of further factual enhancement” that elevates this allegation from the field of mere possibility to the required crest of plausibility. *Id.* That is especially so because the occurrence of the alleged injury “depends on the unfettered choices made by independent actors not before the court[] ... whose exercise of broad and legitimate discretion the court[] cannot presume . . . to predict.” *Defenders of Wildlife*, 504 U.S. at 562. In this event, it becomes the Plaintiffs’ burden “to adduce facts showing that those choices have been or *will be* made in such manner” as to produce cognizable harm, *id.* (emphasis added), which the Complaint does not even endeavor to do. *See also Port Washington Teachers’ Ass’n v. Bd. of Educ.*, 478 F.3d 494, 499 (2d Cir. 2007) (teachers’ union lacked standing to challenge policy on reporting student pregnancies where they failed to show that “students will bring suit against [them] for [making] any such disclosure[s]”).

In addition, even if as yet unnamed third persons refrained from contacting Plaintiffs out of fear that their association with Plaintiffs could be revealed, that would not constitute an injury attributable to the Government’s actions. Rather, such a decision by third parties would instead be the product of subjective and speculative fears on the part of those individuals that the Government might retrieve and review metadata records of their calls with Plaintiffs. As such it would not be “fairly traceable” to the Government’s exercise of authority under Section 215. *Amnesty Int’l*, 133 S. Ct. at 1152 & n.7, citing *Laird v. Tatum*, 408 U.S. 1, 10-14 (1972).

For all of the above reasons, the Complaint should be dismissed for lack of standing.

POINT II: CONGRESS IMPLIEDLY PRECLUDED JUDICIAL REVIEW OF PLAINTIFFS’ STATUTORY CLAIM

Congress has impliedly precluded judicial review of the type of statutory claim Plaintiffs assert – that is, a claim by telephone subscribers that the provision of telephony metadata to the

Government, pursuant to a FISC order, violates Section 215. *See* Compl. ¶ 36. Thus, Plaintiffs cannot rely on the waiver of sovereign immunity codified in the Administrative Procedure Act (APA), 5 U.S.C. § 702; *see* Compl. ¶ 4, to supply the needed waiver for their statutory claim. The APA's waiver of sovereign immunity does not apply where, as here, Congress has granted consent to suit in specified circumstances or fora, or by specified parties, under another statute, and thus impliedly foreclosed the relief sought. 5 U.S.C. § 702. Nor does the APA authorize suit where "statutes preclude judicial review," as Section 215 clearly does. *Id.* § 701(a)(1). Plaintiffs' statutory claim must therefore be dismissed.

"It is elementary that the United States, as sovereign, is immune from suit save as it consents to be sued" *United States v. Mitchell*, 445 U.S. 535, 538 (1980) (internal quotations omitted); *see also FDIC v. Meyer*, 510 U.S. 471, 475 (1994) ("Absent a waiver, sovereign immunity shields the Federal Government and its agencies from suit."). "A waiver of sovereign immunity cannot be implied but must be unequivocally expressed." *Mitchell*, 445 U.S. at 538 (internal quotations omitted). Any ambiguity is construed in favor of immunity. *FAA v. Cooper*, 132 S. Ct. 1441, 1448 (2012). Ambiguity exists if there is a "plausible interpretation" of the statute that would *not* authorize the relief sought. *Id.*

As a general matter, section 702 of the APA grants the Government's consent to suit in actions "seeking relief other than money damages." It is subject to a number of significant exceptions, however, two of which apply here. First, section 702 itself provides that "[n]othing herein . . . confers authority to grant relief if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." 5 U.S.C. § 702. Second, mirroring the first exception, the APA provides that its chapter on judicial review, including section 702, does not apply "to the extent that . . . statutes preclude judicial review." 5 U.S.C. § 701(a)(1).

The first exception “prevents plaintiffs from exploiting the APA’s waiver to evade limitations on suit contained in other statutes.” *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, 132 S. Ct. 2199, 2204-05 (2012). As Congress explained when it enacted the APA’s waiver of immunity, this “important carve-out,” *id.* at 2204, makes clear that section 702 was “not intended to permit suit in circumstances where statutes forbid or limit the relief sought,” that is, where “Congress has consented to suit and the remedy provided is intended to be the exclusive remedy.” H.R. Rep. No. 94-1656, at 12-13 (1976), 1976 WL 14066, * 12-13. “For example, . . . a statute granting the United States’ consent to suit, i.e., the Tucker Act, ‘impliedly forbids’ relief other than the [damages] remedy provided by the Act.” *Id.* Thus, “[w]hen Congress has dealt in particularity with a claim and [has] intended a specified remedy’—including its exceptions—to be exclusive, that is the end of the matter; the APA does not undo the judgment.” *Pottawatomi Indians*, 132 S. Ct. at 2205 (quoting *Block v. North Dakota ex rel. Bd. of Univ. and Sch. Lands*, 461 U.S. 273, 286, n. 22 (1983)).

To much the same effect, section 701(a)(1) of the APA withdraws section 702’s waiver of immunity where “statutes preclude judicial review.” § 701(a)(1) (“This chapter applies, according to the provisions thereof, except to the extent that (1) statutes preclude judicial review”). “Whether and to what extent a particular statute precludes judicial review is determined not only from its express language, but also from the structure of the statutory scheme, its objectives, its legislative history, and the nature of the administrative action involved.” *Block v. Cmty. Nutrition Inst.*, 467 U.S. 340, 345 (1984). “[W]hen a statute provides a detailed mechanism for judicial consideration of particular issues at the behest of particular persons, judicial review of those issues at the behest of other persons may be found to be impliedly precluded.” *Id.*; see *Pottawatomi Indians*, 132 S. Ct. at 2213.

Here, a provision of the USA PATRIOT Act that permits specified suits against the United States impliedly forbids Plaintiffs' statutory claim for equitable relief. Pub. L. No. 107-56, § 223, 115 Stat. 294 (2001), codified at 18 U.S.C. § 2712. Section 2712, titled "Civil actions against the United States," authorizes suits against the United States to recover money damages for willful violations of the Wiretap Act, the Stored Communications Act (SCA), and three particular provisions of FISA. 18 U.S.C. § 2712(a). The three specified provisions of FISA are sections 106(a), 305(a), and 405(a), which respectively impose restrictions on the use and disclosure of information obtained from electronic surveillance, physical searches, and pen registers or trap and trace devices authorized under FISA. *See* 50 U.S.C. §§ 1806(a), 1825(a), 1845(a). Significantly, violations of the parallel "use" provision of Section 215, 50 U.S.C. § 1861(h), which restricts the Government's use and disclosure of tangible things received in response to a production order, are *not* made actionable under section 2712.⁶ Congress further stipulated that an action under § 2712 shall be the exclusive remedy against the United States for claims falling within its purview. *Id.* § 2712(d). Section 2712 thus deals with claims for misuses of information obtained under FISA in great detail, including the intended remedy, and Plaintiffs cannot rely on section 702 to bring a claim for violation of FISA's terms that Congress did not provide for under 18 U.S.C. § 2712. *Pottawatomi Indians*, 132 S. Ct. at 2205.

The same conclusion was reached by another district court in a suit challenging alleged NSA "dragnet" surveillance after the 9/11 attacks. *Jewel v. NSA*, 2013 WL 3829405 (N.D. Cal. July 23, 2013). The court in *Jewel* held that § 2712, "by allowing suits against the United States only for damages based on three provisions of [FISA], impliedly bans suits against the United

⁶ The enactment of section 223 of the USA PATRIOT Act in 2001 preceded enactment of 50 U.S.C. § 1861(h) in 2006. 1 Kris & Wilson § 19:11 at 718. Congress has not since amended § 2712 to include violations of § 1861(h) as a basis for suit. In fact, when Congress amended Section 215 to add subsection (h), it also added the review provision at subsection (f), but made review available only to persons to whom Section 215 orders are directed.

States that seek injunctive relief under any provision of FISA.” *Id.* at *12. Accordingly, the plaintiffs there could not rely on section 702 of the APA as a waiver of sovereign immunity for their FISA-based claim for injunctive relief. *Id.* The same result is required in this case.

Section 215 also reflects an intent by Congress to foreclose the statutory claim asserted here, by this type of plaintiff, in this forum, and thus qualifies as a “statute[] [that] preclude[s] judicial review.” 5 U.S.C. § 701(a)(1). Section 215 carefully delineates who may seek review of a production order and in what court, specifying that “[a] person receiving a production order” may challenge its legality “by filing a petition with [the FISC review] pool” to “modify or set [it] aside.” 50 U.S.C. § 1861(f)(2)(A)(i), (B). Making the preclusive intent of this provision even clearer, Congress punctuated it with the instruction that “[a]ny production ... order not explicitly modified or set aside consistent with [subsection 1861(f)],” that is, on pool review of a provider petition, “shall remain in effect.” *Id.* § 1861(f)(2)(D). Thus, Congress clearly limited the right to contest the legality of Section 215 production orders to recipients of such orders who file petitions for review with the FISC. Indeed, when Congress authorized providers to petition the FISC for review of Section 215 orders, it rejected an amendment that would have allowed such review in federal district court. *See* H. R. Rep. 109-174 at 128-29, 134, 137.⁷

Like the statutory scheme under § 2712, Section 215 indicates that Congress meant to exclude a suit such as the instant one, brought by parties that are not recipients of a production order, in federal district court, not the FISC, seeking equitable relief in a challenge to the

⁷ Further telling is Congress’s decision to not authorize motions to suppress information obtained from a Section 215 order. When the United States or a state intends to use evidence obtained or derived from electronic surveillance, physical searches, or use of pen register or trap-and-trace (PR/TT) devices authorized under FISA in judicial or administrative proceedings against a person, FISA permits that person to contest the legality of the evidence through a suppression motion. 50 U.S.C. §§ 1806(e), 1825(f), 1845(e). But tangible things acquired under Section 215 are not the products of electronic surveillance, physical searches, or use of PR/TT devices. *See* 50 U.S.C. § 1801(f) (defining electronic surveillance), § 1821(5) (physical search), § 1841(2) (PR/TT devices).

statutory validity of a Section 215 production order. This limitation on judicial review makes sense, given that the tangible things that are the subject of a Section 215 order belong to the recipients of the production order, not to third parties such as plaintiffs here. *See United States v. Miller*, 425 U.S. 435, 440-41 (1976).⁸ This “detailed mechanism for judicial consideration of particular issues” under Section 215 “at the behest of particular persons” means that “judicial review of those issues at the behest of other persons” is “impliedly precluded.” *Cnty Nutrition Inst.*, 467 U.S. at 349 (holding that statutory scheme allowing dairy handlers to seek review of milk marketing orders precluded actions by consumers); *see also Dew v. United States*, 192 F.3d 366, 371-74 (2d Cir. 1999) (statute prohibiting employment discrimination on the basis of military service, which authorized civil enforcement action against state and private employers, impliedly precluded suit for equitable relief under the APA by employees of federal intelligence community agencies); *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 128-29 (E.D. Va. 2011) (provision of SCA allowing Twitter subscribers to challenge orders requiring production to Government of “backup information” impliedly prohibited statutory challenge by subscribers to order requiring production of electronic records pertaining to them).

For these reasons, Plaintiffs’ first cause of action, alleging that the Government has acted in excess of its authority under Section 215, should be dismissed.

POINT III: THE GOVERNMENT’S BULK COLLECTION OF TELEPHONY METADATA IS AUTHORIZED UNDER SECTION 215

Even setting aside the jurisdictional deficiencies described above, the Complaint should still be dismissed for failure to state a claim, because it does not “plausibly suggest” that the

⁸ Nor does a party, in the absence of a claim of privilege, typically have standing to object to a subpoena directed to a non-party witness. *Langford v. Chrysler Motors Corp.*, 513 F.2d 1121, 1126 (2d Cir. 1975).

collection of metadata authorized by the FISC either exceeds the bounds of Section 215, or (as discussed in Points IV and V, *infra*) violates the Constitution. *Iqbal*, 556 U.S. at 681.

As their first cause of action Plaintiffs assert that bulk collection of telephony metadata as contemplated by the FISC's Orders exceeds the authority granted by Section 215. Compl. ¶ 36. The Complaint does not set forth the basis for this claim, but, in their July 2, 2013, pre-conference letter to the Court, Plaintiffs suggest that the production ordered by the FISC is unauthorized because (i) the records in question are not "relevant" to an authorized national security investigation, and (ii) Section 215 does not authorize collection of records "as they are generated." Both of these contentions lack merit and should be rejected.

A. The Telephony Metadata Collected Under the FISC's Orders Are "Relevant" to Authorized National Security Investigations

Section 215 authorizes the FISC to order "production of any tangible things" upon the Government's application showing "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation ... to protect against international terrorism." 50 U.S.C. § 1861(a)(1), (b)(2)(A). As recited in the Secondary Order, at 1, the FBI made such an application for an order directing the production of telephony metadata, and the FISC specifically found, in the Primary Order, at 2, "reasonable grounds to believe" that the telephony metadata sought by the Government "are relevant to authorized investigations ... being conducted by the FBI ... to protect against international terrorism." Plaintiffs now ask this Court to second-guess the FISC's conclusion and declare instead that the records the FISC ordered produced to the Government are not, in fact, relevant to authorized counter-terrorism investigations, on the apparent ground that the vast majority of those records do not themselves document calls made in connection with terrorist plots. *See* Compl. ¶¶ 2, 30-34. Plaintiffs' position is contrary to Congress's understanding of the term "relevant" under Section 215, the statute's intended purpose, and repeated decisions of the FISC, and should be rejected.

1. Congress Intended Section 215 To Incorporate a Broad Concept of Relevance, Drawn from the Legal Meaning Applied in Grand Jury, Civil, and Administrative Proceedings, That Also Takes Into Account the Special Characteristics of the Terrorism Investigations to Which It Applies

Even in common usage, “relevant” broadly connotes anything “[b]earing on or connected with,” or “pertinent to,” a specified matter or thing. Oxford English Dictionary (3d ed. 2009) (*available at* www.OED.com). Relevance, however, has developed an even broader legal meaning in the context of official investigations and civil proceedings, for which purposes documents are considered “relevant” not only where they directly bear on a matter, but also where they reasonably could lead to other information that may bear on the matter.

In civil discovery, for example, the phrase “relevant to the subject matter involved in the pending action” broadly encompasses “any matter that bears on, *or that reasonably could lead to other matters that could bear on*, any issue that is or may be in the case.” *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978) (emphasis added). An even broader relevance standard applies to grand jury subpoenas, which will be upheld, notwithstanding the incidental production of irrelevant documents, unless “there is no reasonable possibility that *the category of materials* the Government seeks will produce information relevant to the general subject of the grand jury’s investigation.” *United States v. R. Enters., Inc.*, 498 U.S. 292, 301 (1991) (emphasis added); *In re Grand Jury Proceedings*, 616 F.3d 1186, 1202, 1205 (10th Cir. 2010). Likewise, the statutory authority conferred on administrative agencies to subpoena evidence that is “relevant to [a] charge under investigation” affords them “access to virtually any material that might cast light on the allegations” at issue in an investigation, *EEOC v. Shell Oil Co.*, 466 U.S. 54, 68-69 (1984) (internal quotations omitted), and courts generally defer to an agency’s appraisal of what is relevant to the investigation at hand, *see NLRB v. Am. Med. Response, Inc.*, 438 F.3d 188, 193 (2d Cir. 2006).

In light of that basic understanding of relevance, courts in each of these contexts have categorically authorized the production of entire repositories of records, even when any particular record is unlikely to bear directly on the matter being investigated, where searching a large volume of information is the only feasible means of locating much smaller amounts of critical information within the data that directly bears on the matter under investigation.⁹ In the analogous field of search warrants for data stored on computers, courts also permit Government agents to copy entire computer hard drives and then later review the entire drive for the specific evidence described in the warrant. *See* Fed. R. Crim. P. 41(e)(2)(B).¹⁰ These practices, in a variety of settings, demonstrate the broad understanding of the concept of relevance developed in the context of investigatory information gathering.

Congress incorporated this accepted, broad, and context-dependent legal meaning of the term “relevant” into Section 215. Ordinarily, Congress is presumed to adopt the common understanding of the legal terms it employs. *See NLRB v. Amax Coal Co.*, 453 U.S. 322, 329 (1981) (“Where Congress uses terms that have accumulated settled meaning under either equity or the common law, a court must infer, unless the statute otherwise dictates, that Congress means

⁹ *See, e.g., In re Subpoena Duces Tecum*, 228 F.3d 341, 350-51 (4th Cir. 2000) (subpoena for 15,000 patient files); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987) (upholding grand jury subpoenas for records of wire money transfers “involving hundreds of innocent people”); *FTC v. Invention Submission Corp.*, 965 F.2d 1086 (D.C. Cir. 1992); *Carrillo Huettel, LLP v. SEC*, 2011 WL 601369, at *2 (S.D. Cal. Feb. 11, 2011) (trust account information for all of law firm’s clients held relevant to SEC investigation); *Goshawk Dedicated, Ltd. v. Am. Viatical Servs., LLC*, 2007 WL 3492762 at *1 (N.D. Ga. Nov. 5, 2007) (compelling production of business’s entire underwriting database); *In re Adelphia Commc’ns. Corp.*, 338 B.R. 546, 549 and 553 (Bankr. S.D.N.Y. 2005) (permitting inspection of “approximately 20,000 large bankers boxes of business records”); *Medtronic Sofamor Danek, Inc. v. Michelson*, 229 F.R.D. 550, 552 (W.D. Tenn. 2003) (compelling discovery of “approximately 996 network backup tapes ... plus an estimated 300 gigabytes of other electronic data).

¹⁰ *See, e.g., United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006) (recognizing that “blanket seizure” of the defendant’s entire computer system, followed by subsequent review, may be permissible); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999).

to incorporate the established meaning of these terms”).¹¹ In this case, however, both the text and legislative history confirm that Congress was acutely aware of the accepted legal meaning of relevance when it enacted Section 215’s relevance requirement.

When Congress codified the relevance requirement under Section 215, *see* USA PATRIOT Act Improvement Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192 (2006), it was understood that relevance was the equivalent of the “well established standard” applied to grand jury subpoenas, administrative subpoenas, and civil discovery requests. *See* 152 Cong. Rec. S1598, 1606 (Mar. 2, 2006) (statement of Sen. Kyl).¹² Indeed, Congress described the items subject to production under Section 215 as things obtainable by “a subpoena duces tecum issued by a court ... in aid of a grand jury investigation” or “any other order issued by a court ... directing the production of records or tangible things.” 50 U.S.C. § 1861(c)(2)(D). And in codifying the relevance standard applicable here, Congress provided that the Government need only show “reasonable grounds to believe” that the records sought are relevant to an authorized investigation, *id* § 1861(b)(2)(A), thus incorporating, too, the deferential standard of review applied to the Government’s relevance determinations when it issues investigatory subpoenas. *See R. Enters.*, *supra* at 21, 498 U.S. at 301; *Am. Med. Response*, 438 F.3d at 193.

¹¹ *See also United States v. Shabani*, 513 U.S. 10, 14 (1994); *McLean v. United States*, 566 F.3d 391, 396 (4th Cir. 2009) (“When Congress directly incorporates language with an established legal meaning into a statute, we may infer that Congress intended the language to take on its established meaning”); *Smith v. Bowersox*, 159 F.3d 345, 347 (8th Cir. 1998) (same).

¹² *See also* 152 Cong. Rec. S1379, 1395 (Feb. 16, 2006) (statement of Sen. Kyl) (“We all know the term ‘relevance.’ It is a term that every court uses ... The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation, and for each and every one of the 335 different administrative subpoenas currently authorized by the United States Code”); 151 Cong. Rec. S13636, 13642 (Dec. 15, 2005) (statement of Sen. Hatch) (the relevance standard incorporated into Section 215 “has been used for years in the issuance of grand jury subpoenas,” and is “strictly in the mainstream of American criminal law”); H.R. Rep. No. 109-174, pt. 1 at 131 (statement of Rep. Lungren) (“the standard proposed here is really the relevance standard under which Federal grand juries ... operate”).

Of course, the case law in the contexts of civil discovery, grand jury subpoenas, and administrative investigations does not involve data acquisition on the scale of the telephony metadata collection authorized by the FISC, because the information gathered in those contexts is sought in aid of focused judicial and administrative proceedings involving identifiable individuals and events. But there are a number of textual and contextual indications that Congress also intended Section 215 to embody a sufficiently flexible standard of relevance to take into account the uniquely important purposes and special characteristics of the national security investigations to which the statute applies.

First, unlike the rules that limit civil discovery to information that is relevant “to the subject matter involved” in a case, Fed. R. Civ. P. 26(b)(1), Section 215 permits the collection of information relevant “to an authorized investigation.” 50 U.S.C. § 1861(b)(2)(A). Business records can therefore be relevant to an investigation not merely if they relate to the subject matter of an inquiry, but also if there is reason to believe they are necessary to the application of investigative techniques that will advance its purposes. The bulk collection of telephony metadata is necessary to enable discovery of otherwise hidden connections between individuals suspected of engaging in terrorist activity and unknown co-conspirators with whom they maintain contact in the United States. The metadata records are therefore relevant to FBI investigations whose object is to thwart the plots in which these individuals are engaged before they come to bitter fruition.¹³

¹³ Notably, when Congress codified the relevance standard in Section 215 it *specifically rejected* proposals to limit its scope so that it would encompass only records pertaining to individuals suspected of terrorist activity. See S. 2369, 109th Cong., 2d Sess., § 3 (Mar. 6, 2006); 151 Cong. Rec. S14275-01 (Dec. 21, 2005) (statement of Sen. Dodd) (“Unfortunately, the conference report ... maintains the minimal standard of relevance without a requirement of fact connecting the records sought, or the individual, suspected of terrorist activity”). See also 152 Cong. Rec. S1598-03 (2006) (statement of Sen. Levin); 152 Cong. Rec. H581-02 (Mar. 7, 2006) (statement of Rep. Nadler).

Second, relevance in the context of national security investigations cannot be evaluated in a vacuum but must be considered in light of their special nature, purpose, and scope. *See Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946). Counter-terrorism investigations serve important purposes beyond the ambit of routine criminal inquiries, which ordinarily focus retrospectively on specific crimes that have already occurred and the persons known or suspected to have committed them. The key purpose of terrorism investigations, in contrast, is to prevent terrorist attacks before they occur. Hence, national security investigations often have remarkable breadth, spanning long periods of time and multiple geographic regions to identify terrorist groups, their members, intended targets, and means of attack, many of which are often unknown to the intelligence community at the outset. *See CIA v. Sims*, 471 U.S. 159, 171 (1985) (“foreign intelligence [gathering] consists of securing all possible data pertaining to ... the national defense and security of the United States”). National security investigations thus require more far-reaching means of information-gathering to shed light on suspected terrorist organizations, their size and composition, recruitment, geographic reach, relation to foreign powers, financial resources, past acts, goals, and capacity for carrying out their plans.

When Congress codified the relevance standard under Section 215, the critical differences between the breadth and attributes of counter-terrorism investigations and routine criminal investigations were well understood. *See* H.R. Rep. No. 109-174(1) at 129 (statement of Rep. Lungren) (“[t]his is in the nature of trying to stop terrorists before they act, not in the nature of a regular criminal investigation ... and it strikes ... precisely at when a 215 order is most useful”); *see also* 152 Cong. Rec. S1325, 1330 (Feb. 15, 2006) (statement of Sen. Feingold). The purpose underlying the USA PATRIOT Act, and Section 215 in particular, was to provide the intelligence community the enhanced investigatory tools needed to bring terrorist activities to light before they culminate in a loss of life and property. *See* H.R. Rep. No. 109-

174, pt. 2 at 4 (“many of the core enhanced authorities of the [Patriot Act] are fundamentally intelligence authorities intended to gather information to counter threats to national security from terrorists”); S. Rep. No. 109-85 at 40 (noting “critical” nature and “broad reach” of authority conferred by Section 215). To achieve this core objective, the Government must have authority to collect records that can produce information revealing previously unknown operatives and activities, and thus detect and prevent terrorist attacks before they are launched. Limiting the reach of Section 215 to specific records bearing directly on known terrorist threats and operatives would inhibit the use of this authority for its intended purposes – detecting unknown terrorist threats – and frustrate the will of Congress.¹⁴

2. Congress Has Legislatively Ratified the Construction of Section 215 as Allowing for the Bulk Collection of Telephony Metadata Records

Congress’s adoption of this expansive understanding of relevance under Section 215 is further confirmed by the fact that Congress had already been notified of the Government’s bulk

¹⁴ When it codified Section 215’s relevance requirement, Congress simultaneously built protections into the statutory scheme not found in the other legal contexts. Section 215’s requirement for prior judicial authorization – not required for grand jury subpoenas, administrative subpoenas, or civil discovery – serves as a check on the broad investigatory powers granted to the Government in counter-terrorism investigations. For example, the Government’s authority to collect telephony metadata must be renewed by the FISC every 90 days, and, pursuant to statutory minimization requirements, the FISC’s orders require reasonable, articulable suspicion that identifiers (*e.g.*, telephone numbers) used to query the data are associated with specific foreign terrorist organizations that have previously been identified to and approved for targeting by the Court. *See* Primary Order at 7. Moreover, once information is produced under a Section 215 order, the Government can retain and disseminate it only in accordance with minimization procedures reported to and approved by the Court. *See* 50 U.S.C. § 1861(c)(1), (g). The entire process is subject to active congressional oversight. *See, e.g., id.* § 1862. These multiple and interlocking layers of oversight and regulation further reflect a recognition on Congress’s part of the broad authority conferred by Section 215 to gather information “relevant” to a counter-terrorism investigation, and the need for correspondingly robust safeguards to promote responsible use of that authority.

As recent disclosures by the Government demonstrate, *see* n. 5, *supra*, this system of interactive administrative, judicial, and legislative safeguards has succeeded in identifying and correcting issues of unauthorized access to telephony metadata when they have arisen.

collection of telephony metadata when it twice re-authorized Section 215, without change, in 2010 and 2011. Pursuant to – indeed, well beyond – FISA’s Congressional notification requirements, *see* 50 U.S.C. 1871(a), the Executive Branch worked to ensure that *all* Members of Congress had access to information about this program and the legal authority for it. In December 2009, a classified briefing paper, explaining that the Government and the FISC had interpreted Section 215 to authorize the bulk collection of telephony metadata, was provided to the House and Senate Intelligence Committees and made available for review, as well, by all Members of Congress, “to inform the legislative debate about reauthorization of Section 215.”¹⁵ Additionally, the classified use of this authority has been briefed numerous times over the years to the Senate and House Intelligence and Judiciary Committees, including in connection with reauthorization efforts, as several Members of Congress have acknowledged.¹⁶

¹⁵ *See* Letter from Ronald Weich to the Hon. Silvestre Reyes (Dec. 14, 2009) (Exh. 4, hereto); Report on the [NSA’s] Bulk collection Programs for USA PATRIOT Act Reauthorization (Exh. 5, hereto). Both Intelligence Committees made this document available to all Members of Congress prior to the February 2010 reauthorization of Section 215. *See* Letter from Sens. Feinstein and Bond to Colleagues (Feb. 23, 2010) (Exh. 6, hereto); Letter from Rep. Reyes to Colleagues (Feb. 24, 2010) (Exh. 7, hereto); *see also* 156 Cong. Rec. H838 (daily ed. Feb. 25, 2010) (statement of Rep. Hastings); 156 Cong. Rec. S2109 (daily ed. Mar. 25, 2010) (statement of Sen. Wyden).

An updated version of the briefing paper, *see* Exhibit 8, hereto, was provided to the Senate and House Intelligence Committees again in February 2011 in connection with the reauthorization that occurred later that year. *See* Letter from Ronald Weich to Hon. Diane Feinstein and the Hon. Saxby Chambliss (Feb. 2, 2011) (Exh. 9, hereto); Letter from Ronald Weich to the Hon. Mike Rogers and the Hon. C.A. Dutch Ruppersberger (Feb. 2, 2011) (Exh. 10, hereto). The Senate Intelligence Committee made this updated paper available to all Senators later that month. *See* Letter from Sens. Feinstein and Chambliss to Colleagues (Feb. 8, 2011).

The Court may judicially notice these records and correspondence concerning the legislative history of Section 215’s reenactment. *Oneida Indian Nation of N.Y. v. State of New York*, 691 F.2d 1070, 1086 (2d Cir. 1982).

¹⁶ *See* Press Release of Sen. Select Comm. on Intelligence (June 6, 2013) (Exh. 11, hereto) (“The ... use of this authority has been briefed extensively to the Senate and House Intelligence and Judiciary Committees, and detailed information has been made available to all members of Congress prior to each reauthorization of this law.”); *How Disclosed NSA Programs*

After receiving these classified briefings, Congress twice reauthorized Section 215, in 2010 and again in 2011.¹⁷ “‘Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change.’” *Forest Grove Sch. Dist. v. T.A.*, 557 U.S. 230, 239-40 (2009) (quoting *Lorillard v. Pons*, 434 U.S. 575, 580 (1978)). That presumption is ironclad in this instance, where Congress had actual and repeated notice of the Executive Branch’s administrative construction of Section 215 over a period of years.¹⁸ Imposing a limiting construction now on Section 215’s relevance standard that would prohibit bulk collection of telephony metadata would be contrary to the express understanding of the statute that Congress ratified on two separate occasions.

3. Telephony Metadata Are “Relevant” Within the Meaning of Section 215 Because Bulk Collection of the Data Enhances the Government’s Ability To Detect Terrorist Operatives and Prevent Terrorist Attacks

Acknowledging the intended scope of Section 215 is not to say that the authority it confers is boundless. The Government’s ability to analyze telephony metadata to discover connections between individuals fundamentally distinguishes such data from other information,

Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the House Perm. Select Comm. on Intelligence 2, 35, 58, 113th Cong., 1st Sess. (2013) (statements of Reps. Rogers, Langevin, and Pompeo) (Exh. 12, hereto).

¹⁷ USA PATRIOT Act – Extension of Sunsets, Pub. L. No. 111-141, § 1(a), 124 Stat. 37; PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, § 2(a), 125 Stat. 216.

¹⁸ *See Atkins v. Parker*, 472 U.S. 115, 140 (1985) (“Congress was thus well aware of, and legislated on the basis of, the contemporaneous administrative practice . . . and must be presumed to have intended to maintain that practice absent some clear indication to the contrary”); *Shell Oil*, 466 U.S. at 69; *Haig v. Agee*, 453 U.S. 280, 297-98 (1981).

Moreover, in both 2009 and 2011, when the Senate Judiciary Committee was considering possible amendments to Section 215, it made clear that it had no intention of affecting the telephony metadata collection program. The Committee reports accompanying the USA PATRIOT Act Sunset Extension Acts of 2009 and 2011 explained that proposed changes to Section 215 were “not intended to affect or restrict any activities approved by the FISA court under existing statutory authorities.” S. Rep. No. 111-92, at 7 (2009); S. Rep. No. 112-13, at 10 (2011). Ultimately, Section 215 was extended to June 1, 2015 without change. *See Patriot Sunsets Extension Act of 2011*, Pub. L. No. 112-14, 125 Stat. 216 (2011).

such as library or medical records. For example, while an identified suspect's medical history might be relevant to an investigation of that individual, searching an aggregate database of medical records—which do not interconnect with one another—would not typically enable the Government to identify otherwise unknown relationships among individuals and organizations and thereby ascertain information about terrorist networks. Ordinarily, therefore, bulk collection of such records would not meet the “relevance” standard. *See Okla. Press*, 327 U.S. at 209 (explaining that “relevancy and adequacy or excess in the breadth of [a] subpoena are matters variable in relation to the nature, purposes and scope of the inquiry”).

But in light of Congress's broad understanding of “relevance” under Section 215 as it necessarily applies to national security investigations, and Congress's repeated, informed decisions to reauthorize the statute without change, the telephony metadata collection clearly meets the Section 215 “relevance” standard, as the judges of the FISC have repeatedly found. Collecting these data is necessary to the effective use of NSA analytical tools, which, when applied to the data, produce information that can help identify clandestine terrorist operatives or networks within the United States. That process is not feasible without bulk collection of the data, because NSA analysts cannot know in advance which of the many phone numbers obtained might have connections to known or suspected terrorists. And unless the telephony metadata are aggregated and retained for appropriate periods, it may not be feasible to identify chains of communications that cross different time periods and telecommunications networks. Thus, the telephony metadata records are “relevant” to authorized investigations of international terrorism.

B. Nothing in the Text of Section 215 Prohibits the Collection of Records “as They Are Generated”

Plaintiffs' next contention, that Section 215 authorizes only the collection of business records “already in existence,” and not the production of records “as they are generated,” July 3, 2013, Letter at 3, is erroneous as a matter of law.

Section 215 authorizes the FISC to direct the production of “*any* tangible things,” “documents,” or “records.” 50 U.S.C. § 1861(a)(1)(emphasis added). Nothing in the text of the statute suggests that FISC orders may apply only to records previously created. That requested information is not created until after a FISC order has been rendered, and is produced on an ongoing basis, does not affect its basic character as “documents,” “records,” or other “tangible things” subject to production under the statute. Nor do the FISC’s orders require the creation or preservation of documents that would otherwise not exist, or compel telecommunications service providers to retain information they would otherwise discard. For example, telephony metadata such as the information at issue here is routinely maintained by providers for at least 18 months pursuant to Federal Communications Commission regulations. *See* 47 C.F.R. § 42.6.

Prospective production of business records has been deemed appropriate in analogous contexts. For example, under the SCA the Government may obtain a court order requiring a provider of cell-phone service to produce non-content “record[s] or other information pertaining to a subscriber ... or customer” on a specific showing of “reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(c)(1), (d). Courts including this one have held that the Government may seek prospective disclosure of records under the SCA because “the prospective ... information sought by the Government ... becomes a ‘historical record’ as soon as it is recorded by the provider,” and the statute “in no way limits the ongoing disclosure of records to the Government as soon as they are created.” *In re Application of the United States*, 632 F. Supp. 2d 202, 207 n.8 (E.D.N.Y. 2008); *In re Application of the United States*, 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006) (the SCA “contains no explicit limitation on the disclosure of prospective data”). Like the SCA, there is nothing in the text or legislative history of FISA indicating that Congress meant to prohibit the contemporaneous production to the Government

of business records that are generated on a daily basis.¹⁹ Any contention otherwise fails as a matter of law.

POINT IV: THE GOVERNMENT’S COLLECTION OF TELEPHONY METADATA DOES NOT VIOLATE PLAINTIFFS’ FOURTH AMENDMENT RIGHTS

Plaintiffs also fail to state a claim that the collection of telephony metadata pursuant to the FISC’s Orders violates their Fourth Amendment rights. *See* Compl. ¶ 37. The Supreme Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), that there is no reasonable expectation of privacy in this exact kind of information – dialed telephone numbers – and therefore the Fourth Amendment is not implicated here. Moreover, even if the Fourth Amendment were applicable, the production of metadata ordered by the FISC would satisfy the reasonableness standard applicable to suspicionless searches that serve special government needs, in which the intrusion on privacy interests is balanced against the Government’s interest in the search. Here, the collection of metadata is minimally intrusive despite its breadth, as the data include no content, and the FISC’s Orders impose restrictions on both access to the data and their dissemination. On the other hand, the metadata collection promotes a governmental interest of the utmost importance – thwarting terrorist attacks.

A. Plaintiffs Have No Fourth Amendment Privacy Interest in Telephony Metadata

The Fourth Amendment provides in relevant part that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” As the Supreme Court remarked just last year, “for most of our history the

¹⁹ This type of prospective order also provides efficient administration for all parties involved—the Court, the Government, and the provider. There is little doubt that the Government could seek a new order on a daily basis for the records created within the last 24 hours, but doing so would unnecessarily burden the Court, the Government, and providers alike. Prospective orders merely ensure that the records can be sought in a reasonable manner for a reasonable period of time while avoiding unreasonable and burdensome paperwork.

Fourth Amendment was understood to embody a particular concern for government trespass upon the areas (‘persons, houses, papers, and effects’) it enumerates.” *United States v. Jones*, 132 S. Ct. 945, 949-50 (2012). In addition to the core concern over searches and seizures within these enumerated areas, it is now understood that a Fourth Amendment “search” takes place when the government’s investigative activities “violate a person’s ‘reasonable expectation of privacy.’” *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967)).

The Government’s collection of telephony metadata under the FISC’s Orders does not involve a “search” of individual telephone subscribers or their property. The Orders are directed to telecommunications service providers, not to subscribers, and direct the production of what are indisputably the providers’ own business records. Nor do telephone subscribers have a reasonable expectation of privacy in telephony metadata. In *Smith v. Maryland*, the Supreme Court held that the government’s recordation of numbers dialed from an individual’s home telephone, through a pen register installed at the telephone company’s central offices, did not constitute a search of that individual under the Fourth Amendment, because persons making telephone calls, even from their own homes, lack a reasonable expectation of privacy in the numbers they call. 442 U.S. at 741-46. In contrast to the contents of telephone calls, the Court held that there is no reasonable expectation of privacy in the telephone numbers dialed, because telephone users “typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes,” such as billing and fraud detection. *Id.* at 743.

Furthermore, the Court reasoned, even if a subscriber harbored a subjective expectation that the phone numbers he dialed would remain private, such an expectation of privacy would not be reasonable, because “a person has no legitimate expectation of privacy in information he

voluntarily turns over to third parties.” *Id.* at 743-44. The Court explained that someone who uses a phone has “voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business,” and therefore has “assumed the risk that the company would reveal to police the numbers he dialed.” *Id.* at 744. Courts have followed *Smith* to find no reasonable expectation of privacy in email “to/from” and Internet protocol (“IP”) addressing information, *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008); *In re Application of the United States*, 830 F. Supp. 2d at 131-38, in text message addressing information, *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 905 (9th Cir. 2008), *rev’d on other grounds*, 130 S. Ct. 2619 (2010), and in subscriber information, such as subscribers’ names, addresses, birthdates, and passwords, communicated to system operations and Internet service providers, *Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

Smith is fatal to Plaintiffs’ claim that the collection of metadata records of their communications violates the Fourth Amendment. So far as metadata include such information as the times and duration of their calls and the numbers of the parties with whom they spoke, that is information that telephone subscribers voluntarily turned over to their providers. The remaining data, such as trunk identifiers, is information generated by the phone companies themselves. *See* Primary Order at 3 n.1. Call-detail records memorializing this information belong to the phone companies, as the parties providing the equipment and services required to make those calls possible. *See United States v. Miller*, 425 U.S. at 440-41 (rejecting a bank depositor’s Fourth Amendment challenge to a subpoena of bank records because, inasmuch as the bank was a party to the transactions, the records belonged to the bank). Thus, under *Smith*, there can be no reasonable expectation of privacy in this information, even if – as has not been alleged here – there were an understanding that the third party (*i.e.*, the telephone company) would treat the

information as confidential. *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984); *Miller*, 425 U.S. at 443 (“the Fourth Amendment does not prohibit the obtaining of information revealed to a third party ... even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”).

Plaintiffs’ July 2, 2013, pre-conference letter cites *Jones* for the proposition that metadata collection “over long periods” constitutes a Fourth Amendment search, but *Jones* is inapplicable here. *Jones* held that “the Government’s installation of a GPS [tracking] device on a [targeted individual’s] vehicle, and its use of that device to monitor the vehicle’s movements, constitutes a ‘search.’” 132 S. Ct. at 949. The Court reached that conclusion on the basis of considerations that are entirely absent here – namely, attachment of a tracking device to an individual’s vehicle to collect track his whereabouts, thus effecting a physical intrusion on that person’s “effects,” one of the spheres that the Fourth Amendment explicitly enumerates as protected. *Id.* (“It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information”). The collection of telephony metadata, unlike affixing a GPS device to a vehicle, does not involve any trespass or other intrusion on Plaintiffs’ property, or tracking of locations from which telephone calls are made.

Moreover, contrary to Plaintiffs’ contentions, the majority in *Jones* expressly disclaimed reliance on the duration of the monitoring (a factor on which the court below had relied, *see United States v. Maynard*, 615 F.3d 544, 558 (D.C. Cir. 2010), *aff’d on other grounds sub nom. United States v. Jones*, 132 S. Ct. 945 (2012)), as a basis for concluding that a search had occurred. 132 S. Ct. at 954; *see also United States v. Anderson-Bagshaw*, 2012 WL 774964, at *2 (N.D. Ohio. Mar. 8, 2012) (“The [*Jones*] majority limited its analysis to the trespassory nature of the GPS installation, refusing to establish some point at which uninterrupted surveillance might become constitutionally problematic.”).

Nor does the scope of the metadata collection under the FISC's Orders alter the Fourth Amendment analysis. Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched." *Steagald v. United States*, 451 U.S. 204, 219 (1981); accord, e.g., *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (a person "claim[ing] the protection of the Fourth Amendment ... must demonstrate that he personally has an expectation of privacy in the place searched"); *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (Fourth Amendment rights are personal rights which may not be vicariously asserted). No Fourth Amendment-protected interest of Plaintiffs is implicated, therefore, by virtue of the fact that the metadata records of many other individuals' calls are collected as well as their own. See *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987) (rejecting argument that a subpoena was unreasonable under the Fourth Amendment because it "may make available to the grand jury [money transfer] records involving hundreds of innocent people"); *United States v. Rigmaiden*, 2013 WL 1932800, at * 13 (D. Ariz. May 8, 2013) (Government did not violate defendant's Fourth Amendment rights by acquiring a high volume (1.8 million) of IP addresses).

B. The Government's Acquisition of Metadata Is Reasonable

Even if collecting telephony metadata involved a Fourth Amendment "search" (it does not), the Fourth Amendment bars only "unreasonable" searches and seizures, whereas the collection of metadata at issue here is reasonable under the standard the Supreme Court applies to assess suspicionless searches that serve special government needs. That standard requires a court to balance "the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy." *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013) (internal citation and quotation marks omitted); see also *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652-53 (1995). That balance overwhelmingly favors the Government here.

First, if, contrary to *Smith*, Plaintiffs could be said to have any Fourth Amendment privacy interest that is implicated by collection of non-content telephony metadata, that interest would be minimal. Moreover, the intrusion on that interest would be mitigated still further by the statutorily mandated restrictions on access to and dissemination of the metadata that are written into the FISC’s Primary Order, at 4-14. *See King*, 133 S. Ct. at 1979 (safeguards limiting DNA analysis to identification information alone reduced any intrusion into privacy); *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 833 (2002) (restrictions on access to drug testing results lessened intrusion on privacy); *Vernonia Sch. Dist.*, 515 U.S. at 658 (intrusion of urine-testing on student athletes’ privacy was significantly reduced by the fact that they were tested only for illegal drugs and not for any medical condition).

On the other side of the balance, the collection and analysis of telephony metadata promotes overriding public interests. The Government’s interest in identifying and tracking terrorist operatives for the purpose of preventing terrorist attacks is a national security concern of overwhelming importance. *See Haig*, 453 U.S. at 307 (“no governmental interest is more compelling than the security of the Nation.”) (internal quotation marks omitted); *In re Directives*, 551 F.3d 1004, 1012 (FISC-R 2008) (“the relevant governmental interest – the interest in national security – is of the highest order of magnitude.”); *United States v. Smith*, 426 F.3d 567, 573 (2d Cir. 2005). Bulk collection of telephony metadata is a “reasonably effective means” of promoting the Government’s national security objectives, *Earls*, 536 U.S. at 837, inasmuch as accumulating metadata enhances the Government’s ability to uncover and monitor unknown terrorist operatives who could otherwise elude detection.²⁰ Given that the Government’s

²⁰ The Government need not show that it is using the least intrusive means available to accomplish its goal, *id.*; *United States v. Martinez-Fuerte*, 428 U.S. 543, 556 n. 12 (1976), and a low percentage of positive outcomes among the total number of searches or seizures does not render a program ineffective. *See Mich. Dep’t of State Police v. Sitz*, 496 U.S. 444, 454 (1990)

collection of metadata serves exceedingly important public interests, with minimal, if any, intrusion on the privacy of telephone subscribers, it would be constitutional even if the Fourth Amendment's reasonableness standard applied.

For these reasons, the Plaintiffs' Fourth Amendment claim should be dismissed.

POINT V: PLAINTIFFS HAVE NOT PLAUSIBLY ALLEGED THAT THE GOVERNMENT'S COLLECTION OF TELEPHONY METADATA VIOLATES THE FIRST AMENDMENT

Plaintiffs' final claim, that FISC-authorized collection of telephony metadata violates the First Amendment, Compl. ¶ 38, perishes in the wake of their failed Fourth Amendment claim. The law is clear that governmental investigations conducted in observance of Fourth Amendment requirements, without purpose to deter or penalize protected expression or association, do not violate the First Amendment. Plaintiffs do not allege that the Government's collection of telephony metadata is intended for any purpose other than to identify terrorist operatives, and prevent terrorist attacks. Accordingly, their First Amendment claim should be dismissed.

A. Plaintiffs' Failure to Allege an Actionable Fourth Amendment Claim Is Also Fatal to Their First Amendment Claim

Plaintiffs allege the same injury in support of their First Amendment claim as their Fourth Amendment claim: that telephony metadata collected under the FISC's Orders gives the Government the wherewithal to piece together "a comprehensive record" of "sensitive" information about Plaintiffs and their associations that is "likely to have a chilling effect on people who would otherwise contact Plaintiffs" for purposes related to Plaintiffs' organizational mission. Compl. ¶¶ 1, 3, 35. Thus, Plaintiffs' putative First Amendment claim is at best

(detention of 126 vehicles entering a highway sobriety checkpoint resulted in arrest of two drunken drivers); *Martinez-Fuerte*, 428 U.S. at 554 (out of 146,000 vehicles passing through border checkpoint, 171 were found to contain deportable aliens). Government officials are given a degree of latitude and deference in choosing among reasonable alternatives in structuring a program involving suspicionless search or seizure. *Sitz*, 496 U.S. at 453-54.

derivative of their Fourth Amendment claim. *See, e.g., ACLU v. NSA*, 493 F.3d 644, 657 (6th Cir. 2007) (opinion of Batchelder, J.) (observing that plaintiffs who challenged alleged warrantless wiretapping by NSA on various constitutional grounds “have only one claim, namely, breach of privacy, based on a purported violation of the Fourth Amendment or FISA ... On a straightforward reading, this claim does not implicate the First Amendment.”).

The Supreme Court and every court of appeals to consider the issue have concluded that when governmental investigative activities have an impact on the exercise of First Amendment freedoms, those interests are safeguarded by adherence to Fourth Amendment standards. *See, e.g., Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *United States v. Mayer*, 503 F.3d 740, 747-48 (9th Cir. 2007).²¹ Accordingly, “surveillance consistent with Fourth Amendment protections . . . does not violate First Amendment rights, even though it may be directed at communicative or associative activities.” *Gordon v. Warren Consol. Bd. of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983) (collecting cases).²² Inasmuch as Plaintiffs have failed to state a claim under the Fourth Amendment, this precedent alone requires dismissal of Plaintiffs’ First Amendment claim, too. *Reporters Comm.*, 593 F.2d at 1059; *see also Mayer*, 503 F.3d 750 (similar); *United States v. Gering*, 716 F.2d 615, 620 (9th Cir. 1983) (rejecting surveilled party’s argument that First Amendment afforded him an expectation of privacy where the Fourth Amendment would not); *ACLU v. NSA*, 493 F.3d at 657 (similar).

²¹ *See also Redd v. City of Enter.*, 140 F.3d 1378, 1383 (11th Cir. 1998); *Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1055-59 (D.C. Cir. 1978); *Jabara v. Kelley*, 476 F. Supp. 561, 572 (E.D. Mich. 1979) (the First and Fourth Amendments “provide coextensive zones of privacy in the context of a good faith criminal investigation,” including warrantless electronic surveillance), *vacated on other grounds*, 691 F.2d 272 (6th Cir. 1982).

²² *See Mayer*, 503 F.3d at 750 (same); *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 471 (D.C. Cir. 1991) (same in context of FISA surveillance). *See also United States v. Ramsey*, 431 U.S. 606, 623-24 (1977) (where mail is subject to inspection by customs officers only when they have “reasonable cause to suspect” it contains something other than correspondence, and the correspondence may not be read absent a warrant, the First Amendment is not violated).

B. Plaintiffs Make No Allegations That the Government’s Collection of Telephony Metadata Is Intended to Curtail Protected Expressive or Associational Activity

Plaintiffs’ First Amendment claim is also subject to dismissal because it is based solely on the alleged incidental effects of good-faith investigatory conduct. “Not every Government action that affects, has an impact on, or indeed inhibits First Amendment activity constitutes the kind of ‘abridgement’ condemned by the First Amendment.” *Reporters Comm.*, 593 F.2d at 1052; *see also City Council of Los Angeles v. Taxpayers for Vincent*, 466 U.S. 789, 803-04 (1984). Courts have long recognized the need, even when summoned to action in the name of constitutionally protected rights, to accommodate the Government’s competing interests where prevention of crime, or, even more imperatively, potential threats to national security are concerned. *See, e.g., Socialist Workers Party v. Attorney General*, 510 F.2d 253, 256 (2d Cir. 1974) (“The FBI has a right, indeed a duty, to keep itself informed with respect to the possible commission of crimes; it is not obliged to wear blinders until it may be too late for prevention.”).

Accordingly, courts distinguish for purposes of First Amendment analysis between government investigations that may have the incidental effect of deterring First Amendment activity, and concrete government action of a regulatory, proscriptive, compulsory, or intrusive nature that is specifically directed against individuals or organizations based on their expressive or associational activities. *See, e.g., Zurcher*, 436 U.S. at 564; *Laird*, 408 U.S. at 11; *Reporters Comm.*, 593 F.2d at 1051-55. Otherwise lawful investigative activities conducted in good faith—that is, “not for the purpose of abridging first amendment freedoms,” *United States v. Aguilar*, 883 F.2d 662, 705 (9th Cir. 1989)—do not violate the First Amendment. *See Reporters Comm.*, 593 F.2d at 1051 (concluding that First Amendment protects activities “*subject to* the general and incidental burdens that arise from good faith enforcement of otherwise valid criminal and civil laws that are not themselves solely directed” at First Amendment conduct).

Here, Plaintiffs advance no claim that the Government's collection and analysis of telephony metadata has any objective other than furthering the compelling national interest in identifying and tracking terrorist operatives and ultimately thwarting terrorist attacks. The Complaint certainly contains no allegations, well-pled or otherwise, from which it could plausibly be concluded that the Government's collection of non-content telephony metadata is aimed at curtailing any First Amendment expressive or associational activities. To the contrary, the Complaint's allegations regarding the authorized breadth of the collection, Compl. ¶¶ 30-34, highlight the fact that it is undertaken without targeting Plaintiffs or any other persons, and without reference to anyone's conduct protected by the First Amendment. Plaintiffs have thus failed to state a First Amendment claim that plausibly gives rise to an entitlement to relief. *Iqbal*, 556 U.S. at 678-79; see *Reporters Comm.*, 593 F.2d at 1052 (“[T]he Government's good faith inspection of [telephone] toll call records does not infringe on plaintiffs' First Amendment rights, because that Amendment guarantees no freedom from such investigation.”).

CONCLUSION

For the reasons stated above, the Court should dismiss the complaint.

Dated: New York, New York
August 26, 2013

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director

ANTHONY J. COPPOLINO
Deputy Director

By: /s/ James Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel

MARCIA BERMAN
Senior Trial Counsel

BRYAN DEARINGER
Trial Attorney

Civil Division,
Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Avenue, N.W.
Washington, DC 20001
Tel.: (202) 514-3358

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for Defendants

By: /s/ David S. Jones
DAVID S. JONES
TARA M. La MORTE
JOHN D. CLOPPER
CHRISTOPHER HARWOOD
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel. (212) 637-
2739/2746/2716/2728
Fax (212) 637-2730
david.jones6@usdoj.gov
tara.lamorte2@usdoj.gov
john.clopper@usdoj.gov
christopher.harwood@usdoj.gov

Exhibit 1

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

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

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR

13 - 8 0

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon") satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

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

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

Declassified and Approved for Release by DNI
on 07-11-2013 pursuant to E.O. 13526

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

on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries.

Telephony metadata 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. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c)

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

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

shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

IT IS FURTHER ORDERED that service of this Order shall be by a method agreed upon by the Custodian of Records of Verizon and the FBI, and if no agreement is reached, service shall be personal.

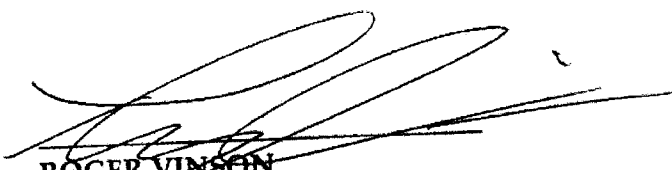
-- Remainder of page intentionally left blank. --

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

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

This authorization requiring the production of certain call detail records or "telephony metadata" created by Verizon expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time


ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

I, Beverly C. Queen, Chief Deputy
Clerk, FISC, certify that this document
is a true and correct copy of the
original. *BQ*

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

Exhibit 2

13-80

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

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

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

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

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number [REDACTED] and its predecessors. [50 U.S.C. § 1861(c)(1)]

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

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

Accordingly, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"¹ created by [REDACTED]

B. The Custodian of Records of [REDACTED]

[REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

¹ For purposes of this Order "telephony metadata" 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. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

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

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

thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by [REDACTED] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [REDACTED]

[REDACTED]

[REDACTED]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.² The BR metadata shall carry unique markings such

² The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

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

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

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.³

Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms⁴ that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

³ The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.

[REDACTED]

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

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

but the results of any such queries will not be used for intelligence analysis purposes.

An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through contact chaining queries of the BR metadata as described in paragraph 17 of the Declaration of [REDACTED], attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.⁵ NSA shall ensure, through adequate and

⁵ For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.

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

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

appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.⁶

(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [REDACTED]

[REDACTED]

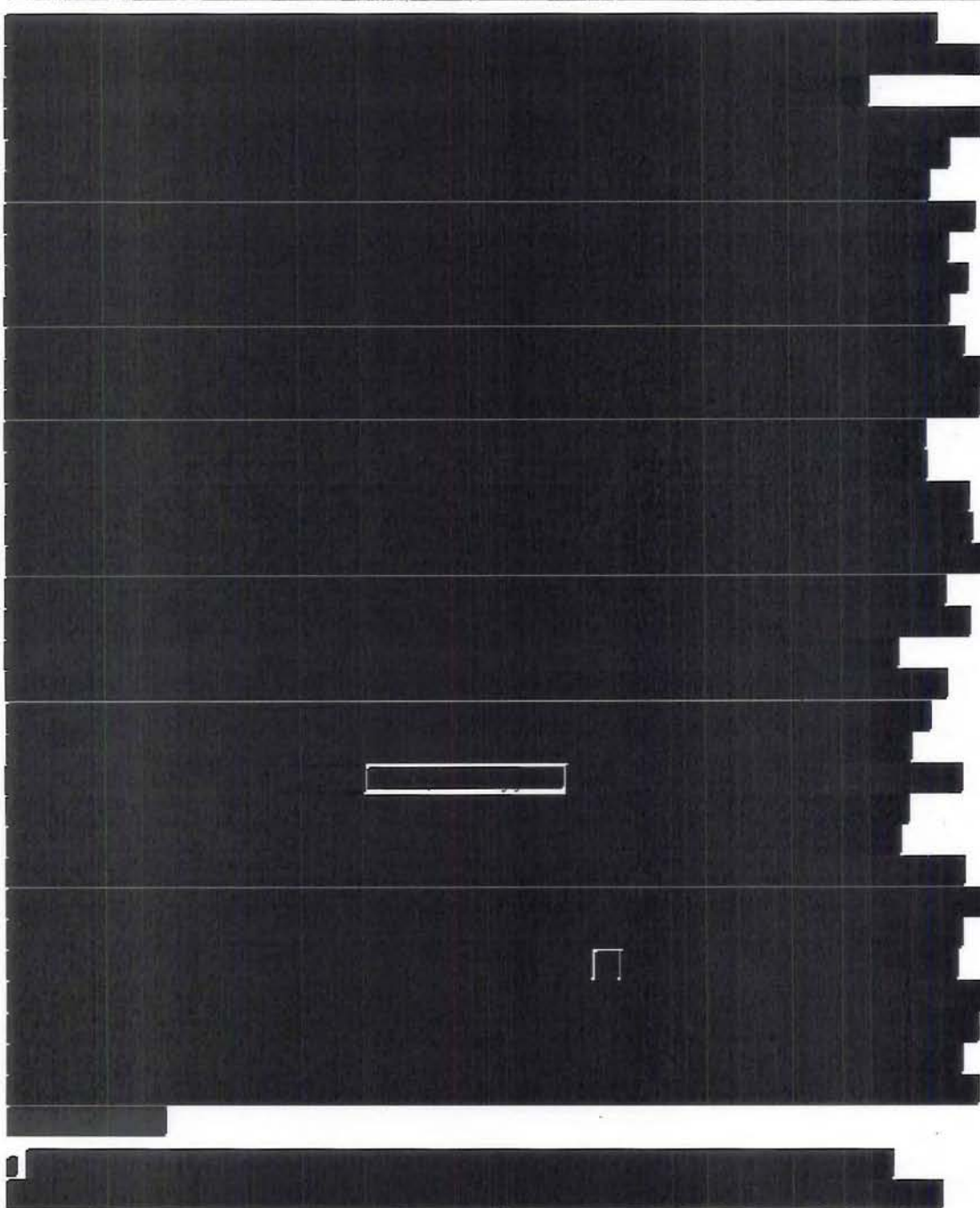
⁶ This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[REDACTED]

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

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

 provided, however, that NSA's Office of General Counsel (OGC)



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

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

shall first determine that any selection term reasonably believed to be used by a

United States (U.S.) person is not regarded as associated with [REDACTED]

[REDACTED]
[REDACTED] on the basis of activities that are protected by the
First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [REDACTED]

[REDACTED]
[REDACTED] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. The preceding sentence shall not apply to selection terms under surveillance

[REDACTED]

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

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

pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated with [REDACTED] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.^{9,10}

⁹ The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the selection term is or was associated with a Foreign Power shall be specified. The automated query process described in the [REDACTED] Declaration limits the first hop query results to the specified time frame. Analysts conducting manual queries using that selection term shall continue to properly minimize information that may be returned within query results that fall outside of that timeframe.

[REDACTED]

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

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

(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.¹¹ This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns the hop-limited results from those queries to a "corporate store." The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms. The specifics of the automated query process, as described in the [REDACTED] Declaration, are as follows:

[REDACTED]

¹¹ This automated query process was initially approved by this Court in its [REDACTED] 2012 Order amending docket number [REDACTED]

¹² As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms have not expired. This step does not use expired RAS-approved selection terms to create the list of "authorized query terms" (described below) regardless of whether the list of RAS-approved selection terms is up-to-date.

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

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

[REDACTED]

[REDACTED]

D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first

[REDACTED]

[REDACTED]

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

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

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.¹⁵ NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (*i.e.*, the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.¹⁶ Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch

¹⁵ In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

¹⁶ In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

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

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

personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.¹⁷ OGC shall provide NSD/DoJ with copies

¹⁷ The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

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

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

of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) 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 referenced above.

(iii) 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. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, 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 Court's orders.

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

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

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.

(vii) Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of NSA's application of the RAS standard, as well as NSA's implementation of the automated query process. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand

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

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

counterterrorism information or to assess its importance.

This authorization regarding [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] expires on the 19th day

of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time



ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

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

Exhibit 3



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

DNI Statement on Recent Unauthorized Disclosures of Classified Information

June 6, 2013

DNI Statement on Recent Unauthorized Disclosures of Classified Information

The highest priority of the Intelligence Community is to work within the constraints of law to collect, analyze and understand information related to potential threats to our national security.

The unauthorized disclosure of a top secret U.S. court document threatens potentially long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our nation.

The article omits key information regarding how a classified intelligence collection program is used to prevent terrorist attacks and the numerous safeguards that protect privacy and civil liberties.

I believe it is important for the American people to understand the limits of this targeted counterterrorism program and the principles that govern its use. In order to provide a more thorough understanding of the program, I have directed that certain information related to the "business records" provision of the Foreign Intelligence Surveillance Act be declassified and immediately released to the public.

The following important facts explain the purpose and limitations of the program:

- The judicial order that was disclosed in the press is used to support a sensitive intelligence collection operation, on which members of Congress have been fully and repeatedly briefed. The classified program has been authorized by all three branches of the Government.
- Although this program has been properly classified, the leak of one order, without any context, has created a misleading impression of how it operates. Accordingly, we have determined to declassify certain limited information about this program.
- The program does not allow the Government to listen in on anyone's phone calls. The information acquired does not include the content of any communications or the identity of any subscriber. The only type of information acquired under the Court's order is telephony metadata, such as telephone numbers dialed and length of calls.
- The collection is broad in scope because more narrow collection would limit our ability to



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

DNI Statement on Recent Unauthorized Disclosures of Classified Information

screen for and identify terrorism-related communications. Acquiring this information allows us to make connections related to terrorist activities over time. The FISA Court specifically approved this method of collection as lawful, subject to stringent restrictions.

- The information acquired has been part of an overall strategy to protect the nation from terrorist threats to the United States, as it may assist counterterrorism personnel to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities.
- There is a robust legal regime in place governing all activities conducted pursuant to the Foreign Intelligence Surveillance Act, which ensures that those activities comply with the Constitution and laws and appropriately protect privacy and civil liberties. The program at issue here is conducted under authority granted by Congress and is authorized by the Foreign Intelligence Surveillance Court (FISC). By statute, the Court is empowered to determine the legality of the program.
- By order of the FISC, the Government is prohibited from indiscriminately sifting through the telephony metadata acquired under the program. All information that is acquired under this program is subject to strict, court-imposed restrictions on review and handling. The court only allows the data to be queried when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization. Only specially cleared counterterrorism personnel specifically trained in the Court-approved procedures may even access the records.
- All information that is acquired under this order is subject to strict restrictions on handling and is overseen by the Department of Justice and the FISA Court. Only a very small fraction of the records are ever reviewed because the vast majority of the data is not responsive to any terrorism-related query.
- The Court reviews the program approximately every 90 days. DOJ conducts rigorous oversight of the handling of the data received to ensure the applicable restrictions are followed. In addition, DOJ and ODNI regularly review the program implementation to ensure it continues to comply with the law.
- The Patriot Act was signed into law in October 2001 and included authority to compel production of business records and other tangible things relevant to an authorized national security investigation with the approval of the FISC. This provision has subsequently been reauthorized over the course of two Administrations – in 2006 and in 2011. It has been an important investigative tool that has been used over the course of two Administrations, with



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

DNI Statement on Recent Unauthorized Disclosures of Classified Information

the authorization and oversight of the FISC and the Congress.

Discussing programs like this publicly will have an impact on the behavior of our adversaries and make it more difficult for us to understand their intentions. Surveillance programs like this one are consistently subject to safeguards that are designed to strike the appropriate balance between national security interests and civil liberties and privacy concerns. I believe it is important to address the misleading impression left by the article and to reassure the American people that the Intelligence Community is committed to respecting the civil liberties and privacy of all American citizens.

James R. Clapper, Director of National Intelligence

###

Exhibit 4

~~TOP SECRET//COMINT//NOFORN~~



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

December 14, 2009

The Honorable Silvestre Reyes
Chairman
Permanent Select Committee on Intelligence
United States House of Representatives
HVC-304, The Capitol
Washington, DC 20515

Dear Chairman Reyes:

~~(TS)~~ Thank you for your letter of September 30, 2009, requesting that the Department of Justice provide a document to the House Permanent Select Committee on Intelligence (HPSCI) that describes the bulk collection program conducted under Section 215 -- the "business records" provision of the Foreign Intelligence Surveillance Act (FISA). We agree that it is important that all Members of Congress have access to information about this program, as well as a similar bulk collection program conducted under the pen register/trap and trace authority of FISA, when considering reauthorization of the expiring USA PATRIOT Act provisions.

~~(TS)~~ The Department has therefore worked with the Intelligence Community to prepare the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States. We believe that making this document available to all Members of Congress is an effective way to inform the legislative debate about reauthorization of Section 215 and any changes to the FISA pen register/trap and trace authority. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the HPSCI's plan to make the document available to other Members is subject to strict rules.

~~Classified by: Assistant Attorney General, NSD
Reason: 1.4(c)
Declassify on: 11 December 2034~~

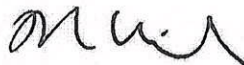
~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

~~(TS)~~ Therefore, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared HPSCI, Judiciary Committee, and leadership staff), in a secure location in the HPSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the HPSCI regarding review of classified information and non-disclosure agreements. No photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that HPSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the Senate Select Committee on Intelligence (SSCI) under similar conditions, so that it may be made available to the Members of the Senate, as well as cleared leadership, SSCI and Senate Judiciary Committee staff.

(U) Thank you again for your letter, and we look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,



Ronald Weich
Assistant Attorney General

~~TOP SECRET//COMINT//NOFORN~~

Exhibit 5

~~TOP SECRET//COMINT//NOFORN~~~~(TS//SI//NF)~~ Report on the National Security Agency's Bulk Collection Programs
Affected by USA PATRIOT Act Reauthorization

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED AND ONLY A LIMITED NUMBER OF EXECUTIVE BRANCH OFFICIALS HAVE ACCESS TO IT. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT ALL WHO HAVE ACCESS TO THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

Key Points

- ~~(TS//SI//NF)~~ Provisions of the USA PATRIOT Act affected by reauthorization legislation support two sensitive intelligence collection programs;
- ~~(TS//SI//NF)~~ These programs are authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls and electronic communications, such as the telephone numbers or e-mail addresses that were communicating and the times and dates but not the content of the calls or e-mail messages themselves;
- ~~(TS//SI//NF)~~ Although the programs collect a large amount of information, the vast majority of that information is never reviewed by anyone in the government, because the information is not responsive to the limited queries that are authorized for intelligence purposes;
- ~~(TS//SI//NF)~~ The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the Foreign Intelligence Surveillance Court ("FISA Court") and Congress;
- ~~(TS//SI//NF)~~ The Executive Branch, including DOJ, ODNI, and NSA, takes any compliance problems in the programs very seriously, and substantial progress has been made in addressing those problems. [REDACTED]
- ~~(TS//SI//NF)~~ NSA's bulk collection programs provide important tools in the fight against terrorism, especially in identifying terrorist plots against the homeland. These tools are also unique in that they can produce intelligence not otherwise available to NSA.

~~Classified by: Assistant Attorney General NSD~~~~Reason: 1.4(c)~~~~Declassify on: 11 December 2034~~~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~Background

~~(TS//SI//NF)~~ Since the tragedy of 9/11, the Intelligence Community has developed an array of capabilities to detect, identify and disrupt terrorist plots against the United States and its interests. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in that effort. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States.

~~(TS//SI//NF)~~ Prior to the attacks of 9/11, the National Security Agency (NSA) intercepted and transcribed seven calls from hijacker Khalid al-Mihdhar to a facility associated with an al-Qa'ida safehouse in Yemen. However, NSA's access point overseas did not provide the technical data indicating the location from where al-Mihdhar was calling. Lacking the originating phone number, NSA analysts concluded that al-Mihdhar was overseas. In fact, al-Mihdhar was calling from San Diego, California. According to the 9/11 Commission Report (pages 269-272):

"Investigations or interrogation of them [Khalid al-Mihdhar, etc], and investigation of their travel and financial activities could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity did not arise."

~~(TS//SI//NF)~~ Today, under Foreign Intelligence Surveillance Court authorization pursuant to the "business records" authority of the Foreign Intelligence Surveillance Act (FISA) (commonly referred to as "Section 215"), the government has developed a program to close the gap that allowed al-Mihdhar to plot undetected within the United States while communicating with a known terrorism target overseas. This and similar programs operated pursuant to FISA provide valuable intelligence information.

(U) USA PATRIOT Act reauthorization legislation currently pending in both the House and the Senate would alter, among other things, language in two parts of FISA: Section 215 and the FISA "pen register/trap and trace" (or "pen-trap") authority. Absent legislation, Section 215 will expire on December 31, 2009, along with the so-called "lone wolf" provision and roving wiretaps (which this document does not address). The FISA pen-trap authority does not expire, but the pending legislation in the Senate and House includes amendments of this provision.

~~(TS//SI//NF)~~ The Section 215 and pen-trap authorities are used by the U.S. Government in selected cases to acquire significant foreign intelligence information that cannot otherwise be acquired either at all or on a timely basis. Any U.S. person information that is acquired is subject to strict, court-imposed restrictions on the retention, use, and dissemination of such information and is also subject to strict and frequent audit and reporting requirements.

~~(TS//SI//NF)~~ The largest and most significant uses of these authorities are to support two critical and highly sensitive intelligence collection programs under which NSA collects and analyzes large amounts of transactional data obtained from telecommunications providers [REDACTED]

[REDACTED] Although these programs have been briefed to

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about these two programs when considering reauthorization of the expiring PATRIOT Act provisions. The Executive Branch views it as essential that an appropriate statutory basis remains in place for NSA to conduct these two programs.

Section 215 and Pen-Trap Collection

~~(TS//SI//NF)~~ Under the program based on Section 215, NSA is authorized to collect from telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call. There is no collection of the content of any telephone call under this program, and under longstanding Supreme Court precedent the information collected is not protected by the Fourth Amendment. In this program, court orders (generally lasting 90 days) are served on [REDACTED] telecommunications companies [REDACTED]

[REDACTED] The orders generally require production of the business records (as described above) relating to substantially all of the telephone calls handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.

~~(TS//SI//NF)~~ Under the program based on the pen-trap provisions in FISA, the government is authorized to collect similar kinds of information about electronic communications – such as “to” and “from” lines in e-mail and the time an e-mail is sent – excluding the content of the e-mail and the “subject” line. Again, this information is collected pursuant to court orders (generally lasting 90 days) and, under relevant court decisions, is not protected by the Fourth Amendment. [REDACTED]

~~(TS//SI//NF)~~ Both of these programs operate on a very large scale. [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~Checks and BalancesFISA Court Oversight

~~(TS//SI//NF)~~ To conduct these bulk collection programs, the government has obtained orders from several different FISA Court judges based on legal standards set forth in Section 215 and the FISA pen-trap provision. Before obtaining any information from a telecommunication service provider, the government must establish, and the FISA Court must conclude, that the information is relevant to an authorized investigation. In addition, the government must comply with detailed "minimization procedures" required by the FISA Court that govern the retention and dissemination of the information obtained. Before an NSA analyst may query bulk records, they must have reasonable articulable suspicion – referred to as "RAS" – that the number or e-mail address they submit is associated with [REDACTED]

The RAS requirement is designed to protect against the indiscriminate querying of the collected data so that only information pertaining to one of the foreign powers listed in the relevant Court order [REDACTED] is provided to NSA personnel for further intelligence analysis. There are also limits on how long the collected data can be retained (5 years in the Section 215 program, and 4½ years in the pen-trap program).

Congressional Oversight

(U) These programs have been briefed to the Intelligence and Judiciary Committees, to include hearings, briefings, and, with respect to the Intelligence Committees, visits to NSA. In addition, the Intelligence Committees have been fully briefed on the compliance issues discussed below.

Compliance Issues

~~(TS//SI//NF)~~ There have been a number of technical compliance problems and human implementation errors in these two bulk collection programs, discovered as a result of Department of Justice reviews and internal NSA oversight. However, neither the Department, NSA nor the FISA Court has found any intentional or bad-faith violations. The problems generally involved the implementation of highly sophisticated technology in a complex and ever-changing communications environment which, in some instances, resulted in the automated tools operating in a manner that was not completely consistent with the specific terms of the Court's orders. In accordance with the Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The incidents, and the Court's responses, were also reported to the Intelligence Committees in great detail. The Committees, the Court and the Executive Branch have responded actively to the incidents. The Court has imposed additional safeguards. In response to compliance problems, the Director of NSA also ordered "end-to-end" reviews of the Section 215 and pen-trap collection programs, and created a new position, the Director of Compliance, to help ensure the integrity of future collection. In early September of 2009, the Director of NSA made a presentation to the FISA Court about the steps taken to address the compliance issues. All

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

parties will continue to report to the FISA Court and to Congress on compliance issues as they arise, and to address them effectively.

Intelligence Value of the Collection

~~(TS//SI//NF)~~ As noted, these two collection programs significantly strengthen the Intelligence Community's early warning system for the detection of terrorists and discovery of plots against the homeland. They allow the Intelligence Community to detect phone numbers and e-mail addresses within the United States contacting targeted phone numbers and e-mail addresses associated with suspected foreign terrorists abroad and vice-versa; and connections between entities within the United States tied to a suspected foreign terrorist abroad. NSA needs access to telephony and e-mail transactional information in bulk so that it can quickly identify the network of contacts that a targeted number or address is connected to, whenever there is RAS that the number or address is associated with [REDACTED]

[REDACTED] Importantly, there are no intelligence collection tools that, independently or in combination, provide an equivalent capability.

~~(TS//SI//NF)~~ To maximize the operational utility of the data, the data cannot be collected prospectively once a lead is developed because important connections could be lost in data that was sent prior to the identification of the RAS phone number or e-mail address. NSA identifies the network of contacts by applying sophisticated analysis to the massive volume of metadata. (Communications metadata is the dialing, routing, addressing or signaling information associated with an electronic communication, but not content.). The more metadata NSA has access to, the more likely it is that NSA can identify or discover the network of contacts linked to targeted numbers or addresses. Information discovered through NSA's analysis of the metadata is then provided to the appropriate federal national security agencies, including the FBI, which are responsible for further investigation or analysis of any potential terrorist threat to the United States.

~~(TS//SI//NF)~~ In conclusion, the Section 215 and pen-trap bulk collection programs provide a vital capability to the Intelligence Community. The attacks of 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is required to protect the homeland, and the programs discussed in this paper cover a critical seam in our defense against terrorism. Recognizing that the programs have implications for the privacy interests of U.S. person data, extensive policies, safeguards, and reviews have been enacted by the FISA Court, DOJ, ODNI and NSA.

~~TOP SECRET//COMINT//NOFORN~~

Exhibit 6

DIANNE FEINSTEIN, CALIFORNIA, CHAIRMAN
CHRISTOPHER S. BOND, MISSOURI, VICE CHAIRMAN

JOHN D. ROCKEFELLER IV, WEST VIRGINIA
RON WYDEN, OREGON
EVAN BAYH, INDIANA
BARBARA A. MIKULSKI, MARYLAND
RUSSELL D. FEINGOLD, WISCONSIN
BILL NELSON, FLORIDA
SHELDON WHITEHOUSE, RHODE ISLAND

ORRIN HATCH, UTAH
OLYMPIA J. SNOWE, MAINE
SAXBY CHAMBLISS, GEORGIA
RICHARD BURR, NORTH CAROLINA
TOM COBURN, OKLAHOMA
JAMES E. RISCH, IDAHO

United States Senate

SELECT COMMITTEE ON INTELLIGENCE

WASHINGTON, DC 20510-6475

HARRY REID, NEVADA, EX OFFICIO
MITCH MCCONNELL, KENTUCKY, EX OFFICIO
CARL LEVIN, MICHIGAN, EX OFFICIO
JOHN MCCAIN, ARIZONA, EX OFFICIO

DAVID GRANNIS, STAFF DIRECTOR
LOUIS B. TUCKER, MINORITY STAFF DIRECTOR
KATHLEEN P. MCGHEE, CHIEF CLERK

February 23, 2010

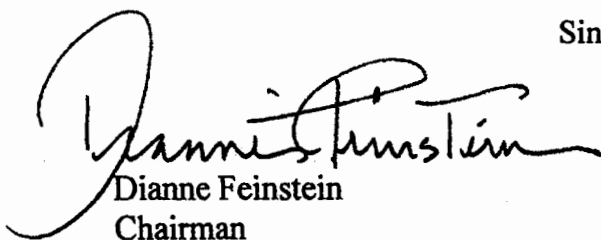
Dear Colleague:

Three provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA) will sunset on February 28, 2010: (1) authority for roving electronic surveillance of targets who take steps to thwart FISA surveillance (Section 206 of the USA PATRIOT Act); (2) authority to compel production of business records and other tangible things with the approval of the FISA Court (Section 215 of the USA PATRIOT Act); and (3) authority to target non-U.S. person "lone wolves" who engage in international terrorist activities but are not necessarily associated with an identified terrorist group (Section 6001 of the Intelligence Reform and Terrorism Prevention Act).

Members of the Select Committee on Intelligence have previously requested that the Executive Branch permit each Member of Congress access to information on the nature and significance of intelligence authority on which they are asked to vote. In response to these requests, the Attorney General and the Director of National Intelligence have provided a classified paper to the House and Senate Intelligence Committees on important intelligence collection made possible by authority that is subject to the approaching sunset, and asked for our assistance in making it available, in a secure setting, directly and personally to any interested Member.

We would like to invite each Member of the Senate to read this classified paper in the Intelligence Committee's offices in 211 Hart Senate Office Building. The Attorney General and DNI have offered to make Department of Justice and Intelligence Community personnel available to meet with any Member who has questions. We will be pleased to make members of our staff available for the same purpose. Please contact our Security Director, James Wolfe, at 224-1751, to arrange for a time.

Sincerely,


Dianne Feinstein
Chairman


Christopher S. Bond
Vice Chairman

Exhibit 7

USA Patriot Act

From: The Permanent Select Committee on Intelligence

Sent By: Khizer.Syed@mail.house.gov

Date: 2/25/2010

February 24, 2010

Dear Colleague:

Three provisions of the USA PATRIOT Act are set to expire on February 28, 2010: (1) authority for roving electronic surveillance of targets who take steps to thwart FISA surveillance; (2) authority to compel production of business records and other tangible things with the approval of the FISA Court; and (3) authority to target non-U.S. person "lone wolves" who engage in international terrorist activities, but are not necessarily associated with an identified terrorist group.

In advance of the anticipated House consideration of a one-year extension of the three provisions described above, the Attorney General and the Director of National Intelligence have provided a classified document to the congressional intelligence committees on important intelligence collection programs made possible by these expiring authorities. They have asked for the Committee's assistance in making that document available to interested members of Congress.

I have agreed to accommodate this request, and Chairman Conyers and I will make Judiciary and Intelligence Committee staff available to meet with any member who has questions. The Attorney General and DNI will also make Department of Justice and Intelligence Community personnel available if needed.

If you are interested in reviewing this classified document, please contact the Committee's scheduler, Stephanie Leaman, at x57690, to set up an appointment in the Committee offices, located in HVC-304.

Sincerely,

/s/

Silvestre Reyes

Chairman

Permanent Select Committee on Intelligence

Exhibit 8

~~TOP SECRET//COMINT//NOFORN~~~~(TS//SI//NF)~~ **Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization**

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED AND ONLY A LIMITED NUMBER OF EXECUTIVE BRANCH OFFICIALS HAVE ACCESS TO IT. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT ALL WHO HAVE ACCESS TO THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

Key Points

- (U) Section 215 of the USA PATRIOT Act, which expires at the end of February 2011, allows the government, upon approval of the Foreign Intelligence Surveillance Court ("FISA Court"), to obtain access to certain business records for national security investigations;
- (U) Section 402 of the Foreign Intelligence Surveillance Act ("FISA"), which is not subject to a sunset, allows the government, upon approval of the FISA Court, to install and use a pen register or trap and trace ("pen/trap") device for national security investigations;
- ~~(TS//SI//NF)~~ These authorities support two sensitive and important intelligence collection programs. These programs are authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls and electronic communications, such as the telephone numbers or e-mail addresses that were communicating and the times and dates but not the content of the calls or e-mail messages themselves;
- ~~(TS//SI//NF)~~ Although the programs collect a large amount of information, the vast majority of that information is never reviewed by any person, because the information is not responsive to the limited queries that are authorized for intelligence purposes;
- ~~(TS//SI//NF)~~ The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the FISA Court and Congress;
- ~~(TS//SI//NF)~~ Although there have been compliance problems in recent years, the Executive Branch has worked to resolve them, subject to oversight by the FISA Court; and
- ~~(TS//SI//NF)~~ The National Security Agency's (NSA) bulk collection programs provide important tools in the fight against terrorism, especially in identifying terrorist plots against the homeland. These tools are also unique in that they can produce intelligence not otherwise available to NSA.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20360101

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~Background

~~(TS//SI//NF)~~ Since the tragedy of 9/11, the Intelligence Community has developed an array of capabilities to detect, identify and disrupt terrorist plots against the United States and its interests. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in that effort. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States.

~~(TS//SI//NF)~~ Prior to the attacks of 9/11, the NSA intercepted and transcribed seven calls from hijacker Khalid al-Mihdhar to a facility associated with an al Qa'ida safehouse in Yemen. However, NSA's access point overseas did not provide the technical data indicating the location from where al-Mihdhar was calling. Lacking the originating phone number, NSA analysts concluded that al-Mihdhar was overseas. In fact, al-Mihdhar was calling from San Diego, California. According to the 9/11 Commission Report (pages 269-272):

"Investigations or interrogation of them [Khalid al-Mihdhar, etc], and investigation of their travel and financial activities could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity did not arise."

~~(TS//SI//NF)~~ Today, under FISA Court authorization pursuant to the "business records" authority of the FISA (commonly referred to as "Section 215"), the government has developed a program to close the gap that allowed al-Mihdhar to plot undetected within the United States while communicating with a known terrorist overseas. This and similar programs operated pursuant to FISA, including exercise of pen/trap authorities, provide valuable intelligence information.

(U) Absent legislation, Section 215 will expire on February 28, 2011, along with the so-called "lone wolf" provision and roving wiretaps (which this document does not address). The pen/trap authority does not expire.

~~(TS//SI//NF)~~ The Section 215 and pen/trap authorities are used by the U.S. Government in selected cases to acquire significant foreign intelligence information that cannot otherwise be acquired either at all or on a timely basis. Any U.S. person information that is acquired is subject to strict, court-imposed restrictions on the retention, use, and dissemination of such information and is also subject to strict and frequent audit and reporting requirements.

~~(TS//SI//NF)~~ The largest and most significant use of these authorities is to support two important and highly sensitive intelligence collection programs under which NSA collects and analyzes large amounts of transactional data obtained from certain telecommunications service providers in the United States. [REDACTED]

Although these programs have been briefed to the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about these two programs when considering reauthorization of the expiring

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

PATRIOT Act provisions. The Executive Branch views it as essential that an appropriate statutory basis remains in place for NSA to conduct these two programs.

Section 215 and Pen-Trap Collection

~~(TS//SI//NF)~~ Under the program based on Section 215, NSA is authorized to collect from certain telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call. There is no collection of the content of any telephone call under this program, and under longstanding Supreme Court precedent the information collected is not protected by the Fourth Amendment. In this program, court orders (generally lasting 90 days) are served on [REDACTED] telecommunications companies [REDACTED]

[REDACTED] The orders generally require production of the business records (as described above) relating to substantially all of the telephone calls handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.

~~(TS//SI//NF)~~ Under the program based on the pen/trap provision in FISA, the government is authorized to collect similar kinds of information about electronic communications – such as “to” and “from” lines in e-mail, certain routing information, and the date and time an e-mail is sent – excluding the content of the e-mail and the “subject” line. Again, this information is collected pursuant to court orders (generally lasting 90 days) and, under relevant court decisions, is not protected by the Fourth Amendment.

~~(TS//SI//NF)~~ Both of these programs operate on a very large scale. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

However, as described below, only a tiny fraction of such records are ever viewed by NSA intelligence analysts.

Checks and Balances

FISA Court Oversight

~~(TS//SI//NF)~~ To conduct these bulk collection programs, the government has obtained orders from several different FISA Court judges based on legal standards set forth in Section 215 and the FISA pen/trap provision. Before obtaining any information from a telecommunications service provider, the government must establish, and the FISA Court must conclude, that the information is relevant to an authorized investigation. In addition, the government must comply with detailed “minimization procedures” required by the FISA Court that govern the retention and dissemination of the information obtained. Before NSA analysts may query bulk records, they must have reasonable articulable suspicion – referred to as “RAS” – that the number or e-mail address they submit is associated with [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

[REDACTED] The RAS requirement is designed to protect against the indiscriminate querying of the collected data so that only information pertaining to one of the foreign powers listed in the relevant Court order [REDACTED]

[REDACTED] is provided to NSA personnel for further intelligence analysis. The bulk data collected under each program can be retained for 5 years.

Congressional Oversight

(U) These programs have been briefed to the Intelligence and Judiciary Committees, through hearings, briefings, and visits to NSA. In addition, the Intelligence and Judiciary Committees have been fully briefed on the compliance issues discussed below.

Compliance Issues

~~(TS//SI//NF)~~ In 2009, a number of technical compliance problems and human implementation errors in these two bulk collection programs were discovered as a result of Department of Justice (DOJ) reviews and internal NSA oversight. However, neither DOJ, NSA, nor the FISA Court has found any intentional or bad-faith violations. [REDACTED]

[REDACTED] In accordance with the Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The FISA Court placed several restrictions on aspects of the business records collection program until the compliance processes were improved to its satisfaction. [REDACTED]

(U) The incidents, and the Court's responses, were also reported to the Intelligence and Judiciary Committees in great detail. The Committees, the Court and the Executive Branch have responded actively to the incidents. The Court has imposed safeguards that, together with greater efforts by the Executive Branch, have resulted in significant and effective changes in the compliance program.

(U) All parties will continue to report to the FISA Court and to Congress on compliance issues as they arise, and to address them effectively.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~Intelligence Value of the Collection

~~(TS//SI//NF)~~ As noted, these two collection programs significantly strengthen the Intelligence Community's early warning system for the detection of terrorists and discovery of plots against the homeland. They allow the Intelligence Community to detect phone numbers and e-mail addresses within the United States that may be contacting targeted phone numbers and e-mail addresses associated with suspected foreign terrorists abroad and vice-versa; and entirely domestic connections between entities within the United States tied to a suspected foreign terrorist abroad. NSA needs access to telephony and e-mail transactional information in bulk so that it can quickly identify and assess the network of contacts that a targeted number or address is connected to, whenever there is RAS that the targeted number or address is associated with [REDACTED]

[REDACTED] Importantly, there are no intelligence collection tools that, independently or in combination, provide an equivalent capability.

~~(TS//SI//NF)~~ To maximize the operational utility of the data, the data cannot be collected prospectively once a lead is developed because important connections could be lost in data that was sent prior to the identification of the RAS phone number or e-mail address. NSA identifies the network of contacts by applying sophisticated analysis to the massive volume of metadata – but always based on links to a number or e-mail address which itself is associated with a counterterrorism target. (Again, communications metadata is the dialing, routing, addressing or signaling information associated with an electronic communication, but not content) The more metadata NSA has access to, the more likely it is that NSA can identify, discover and understand the network of contacts linked to targeted numbers or addresses. Information discovered through NSA's analysis of the metadata is then provided to the appropriate federal national security agencies, including the FBI, which are responsible for further investigation or analysis of any potential terrorist threat to the United States.

~~(TS//SI//NF)~~ In conclusion, the Section 215 and pen/trap bulk collection programs provide an important capability to the Intelligence Community. The attacks of 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is required to protect the homeland, and the programs discussed in this paper cover a critical seam in our defense against terrorism. Recognizing that the programs have implications for the privacy interests of U.S. person data, extensive policies, safeguards, and reviews have been enacted by the FISA Court, DOJ, ODNI and NSA.

~~TOP SECRET//COMINT//NOFORN~~

Exhibit 9

~~TOP SECRET//COMINT//NOFORN~~



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

February 2, 2011

The Honorable Dianne Feinstein
Chairman
The Honorable Saxby Chambliss
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Madam Chairman and Mr. Vice Chairman:

~~(TS)~~ Please find enclosed an updated document that describes the bulk collection programs conducted under Section 215 of the PATRIOT Act (the "business records" provision of the Foreign Intelligence Surveillance Act (FISA)) and Section 402 of FISA (the "pen/trap" provision). The Department and the Intelligence Community jointly prepared the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States.

~~(TS)~~ We believe that making this document available to all Members of Congress, as we did with a similar document in December 2009, is an effective way to inform the legislative debate about reauthorization of Section 215. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the SSCI's plan to make the document available to other Members is subject to the strict rules set forth below.

~~(TS)~~ Like the document provided to the Committee on December 13, 2009, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared SSCI, Judiciary Committee, and leadership staff), in a secure location in the SSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the SSCI regarding review of classified information and non-disclosure agreements. No

~~Classified by: Assistant Attorney General, NSD~~

~~Reason: 1.4(c)~~

~~Declassify on: February 2, 2036~~

~~TOP SECRET//COMINT//NOFORN~~

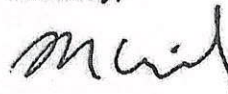
~~TOP SECRET//COMINT//NOFORN~~

The Honorable Dianne Feinstein
The Honorable Saxby Chambliss
Page Two

photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that SSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the House Permanent Select Committee on Intelligence (HPSCI) under similar conditions, so that it may be made available to the Members of the House, as well as cleared leadership, HPSCI and House Judiciary Committee staff.

(U) We look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,



Ronald Weich
Assistant Attorney General

Enclosure

~~TOP SECRET//COMINT//NOFORN~~

Exhibit 10

~~TOP SECRET//COMINT//NOFORN~~



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

February 2, 2011

The Honorable Mike Rogers
Chairman
The Honorable C.A. Dutch Ruppersberger
Ranking Minority Member
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman and Congressman Ruppersberger:

~~(TS)~~ Please find enclosed an updated document that describes the bulk collection programs conducted under Section 215 of the PATRIOT Act (the "business records" provision of the Foreign Intelligence Surveillance Act (FISA)) and Section 402 of FISA (the "pen/trap" provision). The Department and the Intelligence Community jointly prepared the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States.

~~(TS)~~ We believe that making this document available to all Members of Congress, as we did with a similar document in December 2009, is an effective way to inform the legislative debate about reauthorization of Section 215. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the HPSCI's plan to make the document available to other Members is subject to the strict rules set forth below.

~~(TS)~~ Like the document provided to the Committee on December 13, 2009, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared HPSCI, Judiciary Committee, and leadership staff), in a secure location in the HPSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the HPSCI regarding review of classified information and non-disclosure agreements. No

~~Classified by: Assistant Attorney General, NSD~~

~~Reason: 1.4(c)~~

~~Declassify on: February 2, 2036~~

~~TOP SECRET//COMINT//NOFORN~~

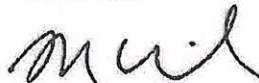
~~TOP SECRET//COMINT//NOFORN~~

The Honorable Mike Rogers
The Honorable C.A. Dutch Ruppersberger
Page Two

photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that HPSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the Senate Select Committee on Intelligence (SSCI) under similar conditions, so that it may be made available to the Members of the Senate, as well as cleared leadership, SSCI and Senate Judiciary Committee staff.

(U) We look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,



Ronald Weich
Assistant Attorney General

Enclosure

~~TOP SECRET//COMINT//NOFORN~~

Exhibit 11

DIANNE FEINSTEIN, CALIFORNIA, CHAIRMAN
SAXBY CHAMBLISS, GEORGIA, VICE CHAIRMAN

JOHN D. ROCKEFELLER IV, WEST VIRGINIA
RON WYDEN, OREGON
BARBARA A. MIKULSKI, MARYLAND
BILL NELSON, FLORIDA
KENT CONRAD, NORTH DAKOTA
MARK UDALL, COLORADO
MARK WARNER, VIRGINIA

OLYMPIA J. SNOWE, MAINE
RICHARD BURR, NORTH CAROLINA
JAMES E. RISCH, IDAHO
DANIEL COATS, INDIANA
ROY BLUNT, MISSOURI
MARCO RUBIO, FLORIDA

SCI#

2011 - 0823

United States Senate

SELECT COMMITTEE ON INTELLIGENCE

WASHINGTON, DC 20510-6475

February 8, 2011

HARRY REID, NEVADA, EX OFFICIO
MITCH MCCONNELL, KENTUCKY, EX OFFICIO
CARL LEVIN, MICHIGAN, EX OFFICIO
JOHN MCCAIN, ARIZONA, EX OFFICIO
DAVID GRANNIS, STAFF DIRECTOR
MARTHA SCOTT POINDEXER, MINORITY STAFF DIRECTOR
KATHLEEN P. MCGHEE, CHIEF CLERK

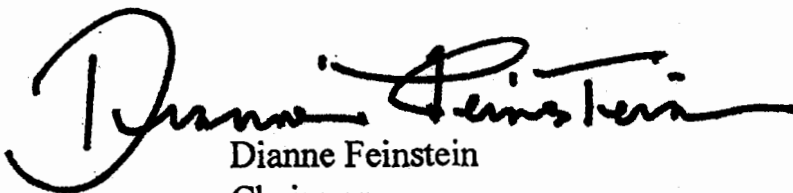
Dear Colleague:

Three provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA) will sunset on February 28, 2011. Two – one on roving authority for electronic surveillance and the other on the acquisition of business records that are relevant to investigations to protect against international terrorism or espionage – were added to FISA by the USA PATRIOT Act. The third, on “lone wolf” authority under FISA, was added by the Intelligence Reform Act of 2004.

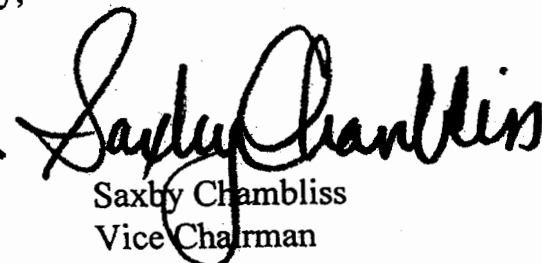
Members of our Committee have previously requested that the Executive Branch permit each Member of Congress access to information on the nature and significance of the intelligence authority on which they are asked to vote. In response, last year the Attorney General and the Director of National Intelligence (DNI) provided a classified report to the House and Senate Intelligence Committees in advance of the previous sunset date of February 28, 2010. At the request of our Committee, the Attorney General and DNI have now provided an updated classified report for review by Members in connection with this year's February 28, 2011 sunset. As was requested last year, they have asked that any interested Member review this report in a secure setting.

We invite each Senator to read this classified report in our committee spaces in Room 211, Hart Senate Office Building. The Attorney General and DNI have offered to make Justice Department and Intelligence Community personnel available to meet with any Member who has questions. We will be pleased to make our staff available for the same purpose. Please contact our Security Director, James Wolfe, at 224-1751, to arrange to read the report.

Sincerely,



Dianne Feinstein
Chairman



Saxby Chambliss
Vice Chairman

Exhibit 12



➤ [113th Congress](#)
(2013-2014)

Press Release of Intelligence Committee

➤ [112th Congress](#)
(2011-2012)

Feinstein, Chambliss Statement on NSA Phone Records Program

➤ [111th Congress](#)
(2009-2010)

Contact: Brian Weiss (Feinstein), (202) 224-9629
Lauren Claffey (Chambliss), (202) 224-3423

➤ [110th Congress](#)
(2007-2008)

Thursday, June 6, 2013

➤ [109th Congress](#)
(2005-2006)

Washington—Senate Intelligence Committee Chairman Dianne Feinstein (D-Calif.) and Vice Chairman Saxby Chambliss (R-Ga.) today released the following joint statement:

➤ [108th Congress](#)
(2003-2004)

"A primary mission of the U.S. intelligence community is to detect and prevent terrorist attacks against the United States, and Congress works closely with the executive branch to ensure that the authorities necessary to keep our country safe are in place. One of these authorities is the 'business records' provision of the Foreign Intelligence Surveillance Act under which the executive branch is authorized to collect 'metadata' concerning telephone calls, such as a telephone number or the length of a call. This law does not allow the government to listen in on the content of a phone call.

➤ [107th Congress](#)
(2001-2002)

"The executive branch's use of this authority has been briefed extensively to the Senate and House Intelligence and Judiciary Committees, and detailed information has been made available to all members of Congress prior to each congressional reauthorization of this law.

"Ensuring security, however, must be consistent with respect for the constitutional rights of all Americans. The alleged FISA Court order contained in the *Guardian* article does not give the government authority to listen in on anyone's telephone call, nor does it provide the government with the content of any communication or the name of any subscriber. As with other FISA authorities, all information the government may receive under such an order would be subject to strict limitations. While our courts have consistently recognized that there is no reasonable expectation of privacy in this type of metadata information and thus no search warrant is required to obtain it, any subsequent effort to obtain the content of an American's communications would require a specific order from the FISA Court.

"The intelligence community has successfully used FISA authorities to identify terrorists and those with whom they communicate, and this intelligence has helped protect the nation. The threat from terrorism remains very real and these lawful intelligence activities must continue, with the careful oversight of the executive, legislative and judicial branches of government."

###

	Search	211 Hart Senate Office Building, Washington, D.C. 20510 Phone: 202-224-1700
----------------------	---------------------------------------	---

Copyright © 2006 United States Senate Select Committee on Intelligence

Exhibit 13

Title Info

Title:

REP. MIKE D. ROGERS HOLDS A HEARING ON SURVEILLANCE PROGRAMS

Date:

June 18, 2013

Location:

WASHINGTON, D.C.

Committee:

Permanent Select Committee on Intelligence. House

Permalink:

[HTTP://congressional.proquest.com/congressional/docview/t65.d40.06180003.u30?accountid=14740](http://congressional.proquest.com/congressional/docview/t65.d40.06180003.u30?accountid=14740)

Speaker

REP. MIKE D. ROGERS

Body

ROGERS: The committee will come to order.

General Alexander, Deputy Attorney General Cole, Chris Inglis, Deputy Director Joyce and Mr. Litt, thank you for appearing before us today, especially on short notice.

The ranking member and I believe it is important to hold an open hearing today, and we don't do a tremendous amount of those, to provide this House and the public with an opportunity to hear directly from you how the government is using the legal authorities that Congress has provided to the executive branch since the terrorist attacks of September 11th, 2001.

I'd also like to recognize the hard work of the men and women of the NSA and the rest of the intelligence community who work day in and day out to disrupt threats to our national security. People at the NSA in particular have heard a constant public drumbeat about a laundry list of nefarious things they are alleged to be doing to spy on Americans -- all of them wrong. The misperceptions have been great, yet they keep their heads down and keep working every day to keep us safe.

ROGERS: And, General Alexander, please convey our thanks to your team for continuing every day, despite much misinformation about the quality of their work. And thank them for all of us for continuing to work to protect America.

I also want to take this moment to thank General Alexander who has been extended as national security adviser in one way or another three different times. That's a patriot.

This is a very difficult job at a very difficult time in our history. And for the general to accept those extensions of his military service to protect this nation, I think with all of the -- the, again, the misinformation out there, I want to thank you for that.

Thank you for your patriotism. Thank you for continuing to serve to protect the United States, again. And you have that great burden of knowing lots of classified information you cannot talk publicly about. I want you to know, thank you on behalf of America for your service to your country.

The committee has been extensively briefed on these efforts over a regular basis as a part of our ongoing oversight responsibility over the 16 elements of the intelligence community and the national intelligence program.

In order to fully understand the intelligence collection programs most of these briefings and hearings have taken place in classified settings. Nonetheless, the collection efforts under the business records provision in Section 702 of the Foreign Intelligence Surveillance Act are legal, court-approved and subject to an extensive oversight regime.

I look forward from hearing from all of the witnesses about the extensive protections and oversight in place for these programs.

General Alexander, we look forward to hearing what you're able to discuss in an open forum about how the data that you have -- you obtain from providers under court order, especially under the business records provision, is used.

And Deputy Attorney General Cole, we look forward to hearing more about the legal authorities themselves and the state of law on what privacy protections Americans have in these business records.

One of the frustrating parts about being a member of this committee, and really challenge, is sitting at the intersection of classified intelligence programs and transparent democracy as representatives of the American people.

The public trusts the government to protect the country from another 9/11-type attack, but that trust can start to wane when they are faced with inaccuracies, half truths and outright lies about the way the intelligence programs are being run.

One of the more damaging aspects of selectively leaking incomplete information is that it paints an inaccurate picture and fosters distrust in our government.

This is particularly so when those of us who have taken the oath to protect information that can damage the national security if released cannot publicly provide clarifying information because it remains classified.

It is at times like these where our enemies with -- our enemies within become almost as damaging as our enemies on the outside.

It is critically important to protect sources and methods so we aren't giving the enemy our play book.

It's also important, however, to be able to talk about how these

programs help protect us so they can continue to be reauthorized. And then we highlight the protections and oversight of which these programs operate under.

General Alexander, you and I have talked over the last week, about the need to -- to be able to publicly elaborate on the success stories these authorities have contributed to without jeopardizing ongoing operations. I know you'll have the opportunity to talk about several of those today.

I place the utmost value in protecting sources and methods. And that's why you've been, I think, so diligent in making sure that anything that's disclosed comports with the need to protect sources and methods. So that, again, we don't make it easier for the bad guys overseas, terrorists in this case, to do harm to United States citizens, and I respect that.

I also recognize that when we are forced into the position of having so publicly discussed intelligence programs due to irresponsible criminal behavior that we also have to be careful to balance the need for secrecy while educating the public.

I think you have struck the right balance between protecting sources and methods and maintaining the public's trust by providing more examples of how these authorities have helped disrupt terrorist plots and connections. I appreciate your efforts in this regard.

For these authorities to continue, they must continue to be available. Without them, I fear we will return to the position where we were prior to the attacks of September 11th, 2001. And that would be unacceptable for all of us.

I hope today's hearing will help answer questions that have arisen as a result of the fragmentary and distorted illegal disclosures over the past several days.

Before recognizing General Alexander for his opening statement, I turn the floor over to the ranking member for any opening statement he'd like to make.

RUPPERSBERGER: Well, I agree with really a lot of what the chairman said.

General Alexander, Chris Inglis, you know, your leadership in NSA has been outstanding. And I just want to acknowledge the people who work at NSA every day. NSA is in my district. I have an occasion to communicate, and a lot of the people who go to work to protect our country, who work hard every day, are concerned that the public think they're doing something wrong. And that's not the case at all.

And the most important thing we can do here today is let the public know the true facts. I know that Chairman Rogers and I and other members have asked you to help declassify what we can, that will not hurt our security, so the public can understand that this important (sic) is legal, why we're doing this program and how it protects us.

We're here today because of the brazen disclosure of critical

classified information that keeps our country safe. This widespread leak by a 29-year-old American systems administrator put our country and our allies in danger by giving the terrorists a really good look at the play book that we use to protect our country. The terrorists now know many of our sources and methods.

There's been a lot in the media about this situation. Some right. A lot wrong. We're holding this open hearing today so we can set the record straight and the American people can hear directly from the intelligence community as to what is allowed and what is not under the law. We need to educate members of Congress also, with the public.

To be clear, the National Security Agency is prohibited from listening in on phone calls of Americans without proper, court-approved legal authorities.

We live in a country of laws. These laws are strictly followed and layered with oversight from three branches of government, including the executive branch, the courts and Congress.

Immediately after 9/11, we learned that a group of terrorists were living in the United States actively plotting to kill Americans on our own soil. But we didn't have the proper authorities in place to stop them before they could kill almost 3,000 innocent people.

Good intelligence is clearly the best defense against terrorism. There are two main authorities that have been highlighted in the press, the business records provision that allows the government to legally collect what is called metadata, simply the phone number and length of call. No content, no conversations. This authority allows our counterterrorism and the law enforcement officials to close the gap on foreign and domestic terrorist activities. It enables our intelligence community to discover whether foreign terrorists have been in contact with people in the U.S. who may be planning a terrorist attack on U.S. soil.

The second authority is known as Section 702 of the FISA Amendment Act. It allows the government to collect the content of e-mail and phone calls of foreigners -- not Americans -- located outside the United States. This allows the government to get information about terrorists, cyber-threats, weapons of mass destruction and nuclear weapons proliferation that threaten America.

This authority prohibits the targeting of American citizens or U.S. permanent residents without a court order, no matter where they are located.

Both of these authorities are legal. Congress approved and reauthorized both of them over the last two years. In fact, these authorities have been instrumental in helping prevent dozens of terrorist attacks, many on U.S. soil.

But the fact still remains that we must figure out how this could have happened. How was this 29-year-old systems administrator able to access such highly classified information and about such sensitive matters? And how was he able to download it and remove it from his

workplace undetected?

We need to change our systems and practices, and employ the latest in technology that would alert superiors when a worker tries to download and remove this type of information. We need to seal this crack in the system.

And to repeat something incredibly important: The NSA is prohibited from listening to phone calls or reading e-mails of Americans without a court order. Period. End of story.

Look forward your testimony.

ROGERS: Again, thank you very much.

Thanks, Dutch, for that.

General Alexander, the floor is yours.

ALEXANDER: Chairman, Ranking Member, thank you for the kind words. I will tell you it is a privilege and honor to serve as the director of the National Security Agency and the commander of the U.S. Cyber Command.

As you noted, we have extraordinary people doing great work to protect this country and to protect our civil liberties and privacy.

Over the past few weeks, unauthorized disclosures of classified information have resulted in considerable debate in the press about these two programs.

The debate had been fueled, as you noted, by incomplete and inaccurate information, with little context provided on the purpose of these programs, their value to our national security and that of our allies, and the protections that are in place to preserve our privacy and civil liberties.

Today, we will provide additional detail and context on these two programs to help inform that debate.

These programs were approved by the administration, Congress and the courts. From my perspective, a sound legal process that we all work together as a government to protect our nation and our civil liberties and privacy.

ALEXANDER: Ironically, the documents that have been released so far show the rigorous oversight and compliance our government uses to balance security with civil liberties and privacy.

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. It is a testament to the ongoing team work of the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency, working with our allies and industry partners, that we have been able to connect the dots and prevent more terrorist attacks.

The events of September 11, 2001 occurred, in part, because of a failure on the part of our government to connect those dots. Some of those dots were in the United States. The intelligence community was not able to connect those domestic dots, phone calls between operatives and the U.S. and Al Qaida terrorist overseas. Following the 9/11 commission, which investigated the intelligence community's failure to detect 9/11, Congress passed the PATRIOT Act.

Section 215 of that act, as it has been interpreted and implied, helps the government close that gap by enabling the detection of telephone contact between terrorists overseas and operatives within the United States. As Director Mueller emphasized last week during his testimony to the -- to the Judiciary Committee, if we had had Section 215 in place prior to 9/11, we may have known that the 9/11 hijacker Mihdhar was located in San Diego and communicating with a known Al Qaida safe house in Yemen.

In recent years, these programs, together with other intelligence, have protected the U.S. and our allies from terrorist threats across the globe to include helping prevent the terrorist -- the potential terrorist events over 50 times since 9/11. We will actually bring forward to the committee tomorrow documents that the interagency has agreed on, that in a classified setting, gives every one of those cases for your review. We'll add two more today publicly we'll discuss. But as the chairman noted, if we give all of those out, we give all the secrets of how we're tracking down the terrorist as a community. And we can't do that. Too much is at risk for us and for our allies. I'll go into greater detail as we go through this testimony this morning.

I believe we have achieved the security and relative safety in a way that does not compromise the privacy and civil liberties of our citizens. We would like to make three fundamental points. First, these programs are critical to the intelligence community's ability to protect our nation and our allies' security. They assist the intelligence community efforts to connect the dots.

Second, these programs are limited, focused, and subject to rigorous oversight. They have distinct purposes in oversight mechanisms. We have rigorous train programs for our analysts and their supervisors to understand their responsibilities regarding compliance.

Third, the disciplined operation of these programs protects the privacy and civil liberties of the American people. We will provide important details about each of those. First, I'd -- I'd ask the Deputy Attorney General Jim Cole to discuss the overarching framework of our authority.

Sir.

COLE: Thank you -- thank you, General.

Mr. Chairman, Mr. Ranking Member, members of the committee, as General Alexander said, and -- and as the chairman and ranking member have said, all of us in the national security area are constantly trying to balance protecting public safety with protecting people's

privacy and civil liberties in this government. And it's a constant job at balancing this.

We think we've done this in these instances. There are statutes that are passed by Congress. This -- this is not a program that's off the books, that's been hidden away. This is part of what government puts together and discusses. Statutes are passed. It is overseen by three branches of our government, the Legislature, the Judiciary, and the Executive Branch. The process of oversight occurs before, during, and after the processes that we're talking about today.

And I want to talk a little bit how that works, what the legal framework is, and what some of the protections are that are put into it. First of all, what we have seen published in the newspaper concerning 215 -- this is the business records provisions of the PATRIOT Act that also modify FISA.

You've seen one order in the newspaper that's a couple of pages long that just says under that order, we're allowed to acquire metadata, telephone records. That's one of two orders. It's the smallest of the two orders. And the other order, which has not been published, goes into, in great detail; what we can do with that metadata; how we can access it; how we can look through it; what we can do with it, once we have looked through it; and what the conditions are that are placed on us to make sure that we protect privacy and civil liberties; and, at the same time, protect public safety.

Let me go through a few of the features of this. First of all, it's metadata. These are phone records. These -- this is just like what you would get in your own phone bill. It is the number that was dialed from, the number that was dialed to, the date and the length of time. That's all we get under 215. We do not get the identity of any of the parties to this phone call. We don't get any cell site or location information as to where any of these phones were located. And, most importantly, and you're probably going to hear this about 100 times today, we don't get any content under this. We don't listen in on anybody's calls under this program at all.

This is under, as I said, section 215 of the PATRIOT Act. This has been debated and up for reauthorization, and reauthorized twice by the United States Congress since its inception in 2006 and in 2011. Now, in order -- the way it works is, the -- there is an application that is made by the FBI under the statute to the FISA court. We call it the FISC. They ask for and receive permission under the FISC under this to get records that are relevant to a national security investigation. And they must demonstrate to the FISC that it will be operated under the guidelines that are set forth by the attorney general under executive order 12333. This is what covers intelligence gathering in the federal government.

It is limited to tangible objects. Now, what does that mean? These are like records, like the metadata, the phone records I've been describing. But it is quite explicitly limited to things that you could get with a grand jury subpoena, those kinds of records. Now, it's important to know prosecutors issue grand jury subpoenas all the time and do not need any involvement of a court or anybody else,

really, to do so.

Under this program, we need to get permission from the court to issue this ahead of time. So there is court involvement with the issuance of these orders, which is different from a grand jury subpoena. But the type of records, just documents, business records, things like that, are limited to those same types of records that we could get through a grand jury subpoena.

Now, the orders that we get last 90 days. So we have to re-up and renew these orders every 90 days in order to do this. Now, there are strict controls over what we can do under the order. And, again, that's the bigger, thicker order that hasn't been published. There's restrictions on who can access it in this order. It is stored in repositories at NSA that can only be accessed by a limited number of people. And the people who are allowed to access it have to have special and rigorous training about the standards under which that they can access it.

In order to access it, there needs to be a finding that there is responsible suspicion that you can articulate, that you can put into words, that the person whose phone records you want to query is involved with some sort of terrorist organizations. And they are defined. It's not everyone. They are limited in the statute. So there has to be independent evidence, aside from these phone records, that the person you're targeting is involved with a terrorist organization.

COLE: If that person is a United States person, a citizen, or a lawful permanent resident, you have to have something more than just their own speeches, their own readings, their own First Amendment-type activity. You have to have additional evidence beyond that that indicates that there is reasonable, articulable suspicion that these people are associated with specific terrorist organizations.

Now, one of the things to keep in mind is under the law, the Fourth Amendment does not apply to these records. There was a case quite a number of years ago by the Supreme Court that indicated that toll records, phone records like this, that don't include any content, are not covered by the Fourth Amendment because people don't have a reasonable expectation of privacy in who they called and when they called. That's something you show to the phone company. That's something you show to many, many people within the phone company on a regular basis.

Once those records are accessed under this process and reasonable articulable suspicion is found, that's found by specially trained people. It is reviewed by their supervisors. It is documented in writing ahead of time so that somebody can take a look at it. Any of the accessing that is done is done in an auditable fashion. There is a trail of it. So both the decision and the facts that support the accessing and the query is documented. The amount that was done, what was done -- all of that is documented and reviewed and audited on a fairly regular basis.

There are also minimization procedures that are put into place so

that any of the information that is acquired has to be minimized. It has to be limited and its use is strictly limited. And all that is set out in the terms of the court order. And if any U.S. persons are involved, there are particular restrictions on how any information concerning a U.S. person can be used in this.

Now, there is extensive oversight and compliance that is done with these records and with this process. Every now and then, there may be a mistake -- a wrong phone number is hid or a person who shouldn't have been targeted gets targeted because there is a mistake in the phone record, something like that.

Each of those compliance incidents, if and when they occur, have to be reported to the FISA court immediately. And let me tell you, the FISA court pushes back on this. They want to find out why did this happen, what were the procedures and the mechanisms that allowed it to happen, and what have you done to fix it. So whenever we have a compliance incident, we report it to the court immediately and we report it to Congress. We report it to the Intelligence Committees of both houses and the Judiciary Committees of both houses.

We also provide the Intelligence and Judiciary Committees with any significant interpretations that the court makes of the 215 statute. If they make a ruling that is significant or issue an order that is significant in its interpretation, we provide those, as well as the applications we made for those orders, to the Intelligence Committee and to the Judiciary Committee.

And every 30 days, we are filing with the FISC, with the court, a report that describes how we implement this program. It includes a discussion of how we're applying the reasonable, articulable suspicion standard. It talks about the number of approved queries that we made against this database, the number of instances that the query results and contain a U.S. person information that was shared outside of NSA. And all of this goes to the court.

At least once every 90 days and sometimes more frequently, the Department of Justice, the Office of the Director of National Intelligence, and the NSA meet to assess NSA's compliance with all of these requirements that are contained in the court order. Separately, the Department of Justice meets with the inspector general for the National Security Agency and assesses NSA's compliance on a regular basis.

Finally, there is by statute reporting of certain information that goes to Congress in semiannual reports that we make on top of the periodic reports we make if there's a compliance incident. And those include information about the data that was required and how we are performing under this statute.

So once again keeping in mind, all of this is done with three branches of government involved: oversight and initiation by the executive branch with review by multiple agencies; statutes that are passed by Congress, oversight by Congress; and then oversight by the court.

Now, the 702 statute under the FISA Amendments Act is different.

Under this, we do get content, but there's a big difference. You are only allowed under 702 to target for this purpose non-U.S. persons who are located outside of the United States. So if you have a U.S. permanent resident who's in Madrid, Spain, we can't target them under 702. Or if you have a non-U.S. person who's in Cleveland, Ohio, we cannot target them under 702. In order to target a person, they have to be neither a citizen nor a permanent U.S. resident, and they need to be outside of the United States while we're targeting them.

Now, there's prohibitions in this statute. For example, you can't reverse-target somebody. This is where you target somebody who's out of the United States, but really your goal is to capture conversations with somebody who is inside the United States. So you're trying to do indirectly what you couldn't do directly. That is explicitly prohibited by this statute. And if there is ever any indication that it's being done, because again, we report the use that we make of this statute to the court and to the Congress, that is seen.

You also have to have a valid foreign intelligence purpose in order to do any of the targeting on this. So you have to make sure, as it was described, that it's being done for defined categories of weapons of mass destruction, foreign intelligence, things of that nature. These are all done pursuant to an application that is made by the attorney general and the director of national intelligence to the FISC. The FISC gives a certificate that allows this targeting to be done for a year period. It then has to be renewed at the end of that year in order for it to be re-upped.

Now, there's also there is a requirement that, again, there is reporting. You cannot under the terms of this statute have and collect any information on conversations that are wholly within the United States. So you're targeting someone outside the United States. If they make a call to inside the United States, that can be collected, but it's only because the target of that call outside the United States initiated that call and went there. If the calls are wholly within the United States, we cannot collect them.

If you're targeting a person who is outside of the United States and you find that they come into the United States, we have to stop the targeting right away. And if there's any lag and we find out that we collected information because we weren't aware that they were in the United States, we have to take that information, purge it from the systems, and not use it.

Now, there's a great deal of minimization procedures that are involved here, particularly concerning any of the acquisition of information that deals or comes from U.S. persons. As I said, only targeting people outside the United States who are not U.S. persons. But if we do acquire any information that relates to a U.S. person, under limited criteria only can we keep it.

If it has to do with foreign intelligence in that conversation or understanding foreign intelligence, or evidence of a crime or a threat of serious bodily injury, we can respond to that. Other than that, we have to get rid of it. We have to purge it, and we can't use it. If we inadvertently acquire any of it without meaning to, again, once that's discovered, we have to get rid of it. We have to purge it.

The targeting decisions that are done are, again, documented ahead of time, reviewed by a supervisor before they're ever allowed to take place in the beginning. The Department of Justice and the Office of the Director of National Intelligence conduct on-site reviews of each targeting that is done. They look at them to determine and go through the audit to determine that they were done properly. This is done at least every 60 days and many times done more frequently than that.

In addition, if there's any compliance issue, it is immediately reported to the FISC. The FISC, again, pushes back: How did this happen? What are the procedures? What are the mechanisms you're using to fix this? What have you done to remedy it? If you acquired information you should (sic) have, have you gotten rid of it as you're required? And in addition, we're providing Congress with all of that information if we have compliance problems.

We also report quarterly to the FISC concerning the compliance issues that have arisen during that quarter, on top of the immediate reports and what we've done to fix it and remedy the ones that we reported.

COLE: We also to Congress under this program, the Department of Justice and the Office of the Director of National Intelligence provide a semiannual report to the FISC and to Congress assessing all of our compliance with the targeting and minimization procedures that are contained in the court order. We also provide a semi-annual report to the FISC and Congress concerning the implementation of the program, what we've done and what we've found. And we also provide to Congress, documents that contain again, how we're dealing with the minimization procedures, any significant legal interpretations that the FISC makes concerning these statutes, as well as the orders and the applications that would relate to that.

And on top of all of this, annually the inspector general for NSA does an assessment, which he provides to Congress that reports on compliance, the number of disseminations under this program that relate to U.S. persons, the number of targets that were reasonably believed at the time to be outside the United States who were later determined to be in the United States, and when that was done. So in short, there is, from before, during and after the involvement of all three branches of the United States government, on a robust and fairly intimate way. I'd like to make one other observation, if I may, on this. We have tried to do this in as thorough, as protective, and as transparent a way as we possibly can, considering it is the gathering of intelligence information.

Countries and allies of ours all over the world collect intelligence. We all know this. And there have recently been studies about how transparent our system is in the United States, compared to many of our partners, many in the E.U. Countries like France, the U.K., Germany, who we work with regularly. And a report that was just recently issued in May of this year found that the FISA Amendments Act, the statute that we're talking about here, and I will quote, "Imposes at least as much, if not more, due process and oversight on foreign intelligence surveillance than other countries." And this

includes E.U. countries. And it says under this, the U.S. is more transparent about its procedures, requires more due process protections in its investigations that involve national security, terrorism and foreign intelligence.

The balance is always one we seek to strive to -- to achieve. But I think as I've laid out to you, we have done everything we can to achieve it. And I think part of the proof of what we've done is this report that came out just last month, indicating our system is as good, and frankly better, than all of our allies and liaison partners. Thank you Mr. Chairman.

ALEXANDER: Mr. Chairman, I will now switch to the value of the program, and talk about some statistics that we're putting together. As we stated, these programs are immensely valuable for protecting our nation, and security the security of our allies. In recent years, the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world. FAA 702 contributed in over 90 percent of these cases. At least 10 of these events included homeland-based threats. In the vast majority, business records, FISA reporting contributed as well. I would also point out that it is a great partnership with the Department of Homeland Security in those with a domestic nexus.

But the real lead for domestic events is the Federal Bureau of Investigation. It has been our honor and privilege to work with Director Mueller, and Deputy Directory Joyce who -- I'll turn it now over to Sean?

JOYCE: Thank you General. Thank you chairman and ranking member, and members of the committee for the opportunity to be here today. NSA and the FBI have a unique relationship, and one that has been invaluable since 9/11. And I just want to highlight a couple of the instances. In the fall of 2009, NSA using 702 authority intercepted an e-mail from a terrorist located in Pakistan. That individual was talking with an individual located inside the United States, talking about perfecting a recipe for explosives. Through legal process, that individual was identified as Najibullah Zazi. He was located in Denver, Colorado.

The FBI followed him to New York City. Later we executed search warrants with the New York Joint Terrorism Task Force and NYPD and found bomb-making components in backpacks. Zazi later confessed to a plot to bomb the New York subway system with backpacks. Also working with FISA business records, the NSA was able to provide a previously unknown number of one of the co-conspirators -- co-conspirators, Adis Medunjanin. This was the first core Al Qaida plot since 9/11 directed from Pakistan. Another example, NSA utilizing 702 authority was monitoring a known extremist in Yemen. This individual was in contact with an individual in the United States named Khalid Ouazzani. Ouazzani and other individuals that we identified through a FISA that the FBI applied for through the FISC were able to detect a nascent plotting to bomb the New York Stock Exchange.

Ouazzani had been providing information and support to this plot. The FBI disrupted and arrested these individuals. Also David Headley, a U.S. citizen living in Chicago. The FBI received intelligence

regarding his possible involvement in the 2008 Mumbai attacks responsible for the killing of over 160 people. Also, NSA through 702 coverage of an Al Qaida affiliated terrorist found that Headley was working on a plot to bomb a Danish newspaper office that had published the cartoon depictions of the Prophet Mohammed. In fact, Headley later confessed to personally conducting surveillance of the Danish newspaper office. He, and his co-conspirators were convicted of this plot.

Lastly, the FBI had opened an investigation shortly after 9/11. We did not have enough information, nor did we find links to terrorism and then we shortly thereafter closed the investigation. However, the NSA using the business record FISA tipped us off that this individual had indirect contacts with a known terrorist overseas. We were able to reopen this investigation, identify additional individuals through a legal process, and were able to disrupt this terrorist activity. Thank you. Back to you, General?

ALEXANDER: So that's four cases total that we've put out publicly. What we're in the process of doing with the inter-agency is looking at over 50 cases that were classified, and will remain classified, that will be provided to both of the Intel Committees of the Senate and the House, to all of you. Those 50 cases right now have been looked at by the FBI, CIA and other partners within the community, and the National Counterterrorism Center is validating all of the points so that you know that what we've put in there is exactly right. I believe the numbers from those cases is something that we can publicly reveal, and all publicly talk about.

What we are concerned, as the chairman said, is to going into more detail on how we stopped some of these cases, as we are concerned it will give our adversaries a way to work around those, and attack us, or our allies. And that would be unacceptable. I have concerns that the intentional and irresponsible release of classified information about these programs will have a long, and irreversible impact on our nation's security, and that of our allies. This is significant. I want to emphasize that the Foreign Intelligence is the best -- the Foreign Intelligence Program that we're talking about, is the best counterterrorism tools that we have to go after these guys.

We can't lose those capabilities. One of the issues that has repeatedly come up, well how do you then protect civil liberties and privacy? Where is the oversight? What are you doing on that? We have the deputy director of the National Security Agency, Chris Inglis, will now talk about that and give you some specifics about what we do, and how we do it with these programs.

INGLIS: Thank you, General Alexander.

Chairman, Ranking Member, members of the committee, I'm pleased to be able to briefly describe the two programs as used by the National Security Agency with a specific focus on the internal controls and the oversight provided. Now first to remind these two complimentary, but distinct programs are focused on foreign intelligence. That's NSA's charge. The first program executed under Section 215 of the Patriot Act authorizes the collection of telephone metadata only. As you've heard before, the metadata is only the

telephone numbers, and contact, the time and date of the call, and the duration of that call.

INGLIS: This authority does not, therefore, allow the government to listen in on anyone's telephone calls, even that of a terrorist. The information acquired under the court order from the telecommunications providers does not contain the content of any communications, what you are saying during the course of the conversation, the identities of the people who are talking, or any cell phone locational information. As you also know this program was specifically developed to allow the U.S. government to detect communications between terrorists operating outside the U.S., who are themselves communicating with potential operatives inside the U.S., a gap highlighted by the attacks of 9/11.

The controls on the use of this data at NSA are specific, rigorous, and designed to ensure focus on counter-terrorism. To that end, the metadata acquired and stored under this program may be queried only when there is a reasonable suspicion based on specific and documented facts that an identifier, like a telephone number, is associated with specific foreign terrorist organizations.

This determination is formally referred to as the "reasonable articulable suspicion standard." During all 2012, the 12 months of 2012, we at NSA approved fewer than 300 unique numbers, which were then used to initiate a query of this data set.

The second program, authorized under Section 702 of the Foreign Intelligence Surveillance Act, authorizes targeting only for communications of foreigners who are themselves not within the United States for foreign intelligence purposes, with the compelled assistance of an electronic communications service provider.

As I noted earlier, NSA being a foreign intelligence agency, foreign intelligence for us is information related to the capabilities, intentions, or activities of foreign governments, foreign organizations, foreign persons, or international terrorists. Let me be very clear. Section 702 cannot be and is not used to intentionally target any U.S. citizen or any U.S. person, any person known to be in the United States, a person outside the United States if the purpose is to acquire information from a person inside the United States. We may not do any of those things using this authority.

The program is also key in our counter-terrorism efforts, as you've heard. More than 90 percent of the information used to support the 50 disruptions mentioned earlier was gained from this particular authority. Again, if you want to target the content of a U.S. person anywhere in the world, you cannot use this authority. You must get a specific court warrant.

I'd like to now describe in further details some of the rigorous oversight for each of these programs. First, for the Section 215 program, also referred to as business records FISA, controls and (ph) determine how we manage and use the data are explicitly defined and formally approved by the Foreign Intelligence Surveillance Court.

First, the metadata segregated from other data sets held by NSA and all queries against the data base are documented and audited. As defined in the orders of the court, only 20 analysts at NSA and their two managers, for a total of 22 people, are authorized to approve numbers that may be used to query this database. All of those individuals must be trained in the specific procedures and standards that pertain to the determination of what is meant by reasonable, articulable suspicion.

Every 30 days, NSA reports to the court the number of queries and disseminations made during that period. Every 90 days, the Department of Justice samples all queries made across the period and explicitly reviews the basis for every U.S. person, or every U.S. identity query made. Again, we do not know the names of the individuals of the queries we might make.

In addition, only seven senior officials at NSA may authorize the dissemination of any information we believe that might be attributable to a U.S. person. Again, we would not know the name. It would only be the telephone number. And that dissemination in this program would only be made to the Federal Bureau of Investigation at determining that the information is related to and necessary to understand a counter-terrorism initiative.

The Foreign Intelligence Surveillance court reviews the program every 90 days. The data that we hold must be destroyed within five years of its acquisition. NSA and the Department of Justice briefed oversight committees on the employment of the program. We provide written notification of all significant developments within the program. The Department of Justice provides oversight committees with all significant foreign intelligence surveillance courts' opinions regarding the program.

Turning my attention to the 702 program, the Foreign Intelligence Surveillance Court annually reviews certification, which are required by law, that are jointly submitted by the attorney general and the director of national intelligence. These certifications define the categories of foreign actors that may be appropriately targeted and, by law, must include specific targeting and minimization procedures that the attorney general and the court both agree are consistent with the law and the Fourth Amendment of the Constitution. These procedures require that a communication of or concerning a U.S. person must be promptly destroyed after it's identified, either as clearly not relevant to the authorized purpose, or as not containing evidence of a crime.

The statute further requires a number of reports to be provided to both the court and the oversight committees. A semi-annual assessment by the Department of Justice and the Office of the Director of National Intelligence, regard in (ph) compliance with the targeting and minimization procedures an annual I.G. assessment that reports compliance with procedural requirements laid out within the order -- the number of disseminations that may refer to U.S. persons, the number of targets later found to be in the United States, and whether the communications of such targets were ever reviewed.

An annual director of NSA report is also required to describe the compliance efforts taken by NSA and address the number of U.S. person identities disseminated in NSA reporting. Finally, Foreign Intelligence Surveillance Court procedures require NSA to inform the court of any novel issues of law or technology relevant to an authorized activity and any non-compliance to include the Executive Branch's plan for remedying that same event. In addition to the procedures I've just described, the Department of Justice conducts on-site reviews at NSA to sample NSA's 702 targeting and tasking decisions every 60 days.

And, finally, I would conclude with my section to say that in July of 2012, the Senate Select Committee on Intelligence, in a report reviewing the progress over the four years of the law's life at that point in time, said that across the four-year history of the program, the committee had not identified a single willful effort by the Executive Branch to violate the law.

ALEXANDER: So to wrap up, Chairman, first I'd like to just hit on -- when we say seven officials, that's seven positions that -- at NSA can disseminate U.S. persons data. Today, there are 10 people in those positions. One of those is our -- SIGINT operations officer. Every one of those have to be -- credentialed. Chris and I are two of those officials.

I do want to hit a couple of key points. First, with our industry partners, under the 702 program, the U.S. government does not unilaterally obtain information from the servers of U.S. companies. Rather, the U.S. companies are compelled to provide these records by U.S. law, using methods that are in strict compliance with that law.

Further, as the deputy attorney general noted, virtually all countries have lawful intercept programs under which they compel communication providers to share data about individuals they believe represent a threat to their societies. Communication providers are required to comply with those programs in the countries in which they operate. The United States is not unique in this capability.

The U.S., however, operates its program under the strict oversight and compliance regime that was noted above with careful oversights by the courts, Congress, and the administration. In practice, U.S. companies have put energy and focus and commitment into consistently protecting the privacy of their customers around the world, while meeting their obligations under the laws of U.S. and other countries in which they operate. And I believe they take those seriously.

Our third and final point, as Americans, we value our privacy and our liberty -- our civil liberties. Americans -- as Americans, we also value our security and our safety. In the 12 years since the attacks on September 11th, we have lived in relative safety and security as a nation. That security is a direct result of the intelligence community's quiet efforts to better connect the dots and learn from the mistakes that permitted those attacks to occur on 9/11.

In those 12 years, we have thought long and hard about oversight

and compliance and how we minimize the impact on our fellow citizens' privacy. We have created and implemented and continue to monitor -- monitor a comprehensive mission compliance program inside NSA. This program, which was developed based on industry best practices and compliance works to keep operations and technology aligned with NSA's externally approved procedures.

Outside of NSA, the officer of the -- the Office of the Director of National Intelligence, Department of Justice, and the Foreign Intelligence Surveillance Court provide robust oversight as well as this committee. I do believe we have that balance right.

In summary, these programs are critical to the intelligence community's ability to protect our nation and our allies' security. They assist the intelligence community's efforts to connect the dot. Second, these programs are limited, focused, and subject to rigorous oversight. They have distinct purposes and oversight mechanisms. Third, the disciplined operation of these programs protects the privacy and civil liberties of the American people.

As you noted, Chairman, the people of NSA take these responsibilities to heart. They protect our nation and our allies as part of a bigger team. And they protect our civil liberties and privacy. It has been an honor and privilege to lead these great Americans. I think Bob Litt has a couple of comments to make, and then we'll turn it back to you, Chairman.

LITT: Yes, Mr. Chairman, Mr. Ranking Member, members of the committee, I just want to speak very briefly and address a couple of additional misconceptions that the public has been fed about some of these programs.

The first is that collection under Section 702 of the FISA Amendments Act is somehow a loosening of traditional standards because it doesn't require individualized warrants. And, in fact, exactly the opposite is the case. The kind of collection that is done under Section 702, which is collecting foreign intelligence information for foreigners outside of the United States historically was done by the executive branch under its own authority without any kind of supervision whatsoever.

And as a result of the FISA Amendments Act, this has now been brought under a judicial process with the kind of restrictions and limitations that have been described by the other witnesses here. So, in fact, this is a tightening of standards from what they were before.

The second misconception is that the FISA court is a rubber stamp for the executive branch. And people point to the fact that the FISA court ultimately approves almost every application that the government submits to it.

But this does not recognize the actual process that we go through with the FISA court. The FISA court is judges, federal district judges appointed from around the country who take this on in addition to their other burdens. They're all widely respected and experienced judges. And they have a full-time professional staff that works only

on FISA matters.

When we prepare an application for -- for a FISA, whether it's under one of these programs or a traditional FISA, we first submit to the court what's called a "read copy," which the court staff will review and comment on.

And if -- and they will almost invariably come back with questions, concerns, problems that they see. And there is an iterative process back and forth between the government and the FISA court to take care of those concerns so that at the end of the day, we're confident that we're presenting something that the FISA court will approve. That is hardly a rubber stamp. It's rather extensive and serious judicial oversight of this process.

The third point, the third misconception that I want to make is that the process we have here is one that simply relies on trust for individual analysts or individual people at NSA to obey the rules.

And I just -- I -- I won't go into detail as to the oversight, because I think it's been adequately described by the others. But the point is, there is a multilayered level of oversight, first within NSA, then involving my agency, the Office of the Director of National Intelligence and the Department of Justice and ultimately involving the FISA court and the Congress to ensure that these rules are complied with.

And the last point that I'd -- the last misconception I want to address is that this information shouldn't have been classified and it was classified only to -- to conceal it from the American people and that the leaks of this information are not damaging.

And, Mr. Chairman and Mr. Ranking Member, you both made this point. These are, as General Alexander said, extremely important collection programs to protect us not only from terrorists, but from other threats to our national security, a wide variety.

And they have produced a huge amount of valuable intelligence over the years. We are now faced with a situation that because this information has been made public, we run the risk of losing these collection capabilities. We're not gonna know for many months whether these leaks in fact have caused us to lose these capabilities. But if -- if they -- if they do have that effect, there is no doubt that they will cause our national security to be affected.

Thank you, Mr. Chairman.

ROGERS: Thank you all, very much. I appreciate that. I just have a couple of quick questions. I know members have lots of questions here and I want to get to them.

Mr. Inglis, just for the record, you -- can you describe quickly your civilian role as the deputy? You serve as that role in a civilian capacity. Is that correct?

INGLIS: Yes, sir. Across the history of NSA, there has always been a senior serving military officer, that's the director of the

National Security Agency, and at the same time a senior serving civilian authority, and that would be the deputy director, and that's my role.

ROGERS: All right, and -- but you have also had military service. Is that correct?

INGLIS: Sir, I did. I served for a period of 13 years on active duty in the United States Air Force, and then transitioned to the National Security Agency.

ROGERS: So you rose to the rank of -- of?

INGLIS: I was brigadier general in the Air National Guard. As in all things, it's complicated.

(CROSSTALK)

ROGERS: Yeah. But I just wanted to get on the record that you do have -- you have military service as well as your civilian service.

(CROSSTALK)

INGLIS: I do, sir. As I transitioned from the active Air Force to the National Security Agency, I retained my affiliation with the reserve components and was pleased and proud to be able to serve in the Air National Guard for another 20 years.

ROGERS: Great. Well, thank you for that service.

You mentioned in "queries of less than 300," what does -- what does that mean?

INGLIS: In each of those cases, sir, there was a determination made an analyst at NSA that there was a reasonable, describable, articulable suspicion that an number of interest, a telephone number of interest, might be associated with a connected plot of a specific terrorist plot overseas, and therefore a desire to see whether that plot had a connection into the United States.

The process they go through then is as described, one where they make a -- a...

(CROSSTALK)

ROGERS: Well, describe the inquiry -- it's not put -- you don't put in a name?

INGLIS: We do not, sir.

ROGERS: So you put in...

(CROSSTALK)

INGLIS: The only thing we get from the providers are numbers. The only thing we could possibly then bounce against that data set are numbers, themselves.

ROGERS: Right. So there are no names and no addresses affiliated with these phone numbers.

INGLIS: No, there are not, sir.

ROGERS: OK. Just phone numbers.

INGLIS: That's right, sir.

ROGERS: OK. Go ahead.

INGLIS: So an analyst would then try to determine whether there was a describable, it must be written, documentation that would say that there is a suspicion that this is attributed to a foreign terrorist plot and there might be a U.S. nexus. After having made that determination, they would make a further check to determine whether it is possible to discern that this might be associated with a U.S. person. The way you would infer that is you might look at the area code and say that area code could likely be in the United States. We all know that within this area, that if you see an area code that begins with 301, that would be Maryland. That would be your only insight into whether or not this might be attributable to a U.S. person.

If that were to be the case, then the case for a reasonable, articulable suspicion must get a further review to ensure that this is not a situation where somebody is merely expressing their First Amendment rights.

If that's all that was, if they were merely expressing their First Amendment rights, however objectionable any person might find that, that is not a basis to query the database.

If it gets through those checks, then at that point, it must be approved by one of those 20 plus two individuals -- 20 analysts, specially-trained analysts, or their two managers -- such that it might then be applied as a query against the data set. Again, the query itself would just be a number, and the query against the data set would then determine whether that number exists in the database. That's how that query is formed. And, again...

(CROSSTALK)

ROGERS: So the response is not a name; it's an address. It's a phone number.

INGLIS: It cannot be. If it were to be a name or if it were to be an address, there would be no possibility that the database would return any meaningful results, since none of that information is in the database.

ROGERS: Just a phone number pops back up.

INGLIS: Just a phone number. What comes back if you query the database are phone numbers that were in contact, if there are any, with that number. And, again, the other information in that database would indicate when that call occurred and what the duration of that

call were -- were to be.

ROGERS: Again, I just want to make very clear, there are no names and no addresses in that database.

INGLIS: There are not, sir.

ROGERS: OK. And why only less than 300 queries of phone numbers into that database?

INGLIS: Sir, only less than 300 numbers were actually approved for query against that database. Those might have been applied multiple times, and therefore, there might be a number greater than that of actual queries against the database. But the reason there are so few selectors approved is that the court has determined that there is a very narrow purpose for this -- this use. It can't be to prosecute a greater understanding of a simply domestic plot. It cannot be used to do anything other than terrorism. And so, therefore, there must be very well-defined describable written determinations that this is -- is a suspicion of a connection between a foreign plot and a domestic nexus. If it doesn't meet those standards...

(CROSSTALK)

ROGERS: Are those queries reported to the court?

INGLIS: Those queries are all reported to the Department of Justice, reviewed by the Department of Justice. The number of those queries are reported to the court. And any time that there is a dissemination associated with a U.S. person...

(CROSSTALK)

ROGERS: Is there a court-approved process in order to make that query into that information of only phone numbers?

INGLIS: Yes, sir. The court explicitly approves the process by which those determinations were made, and the Department of Justice provides a rich oversight auditing of that capability.

ROGERS: Great. Thank you.

General Alexander, is the NSA on private company's servers as defined under these two programs?

ALEXANDER: We are not.

ROGERS: Is -- is the NSA have the ability to listen to Americans' phone calls or read their e-mails under these two programs?

ALEXANDER: No, we do not have that authority.

ROGERS: Does the technology exist at the NSA to flip a switch by some analyst to listen to Americans' phone calls or read their e-mails?

ALEXANDER: No.

ROGERS: So the technology does not exist for any individual or group of individuals at the NSA to flip a switch to listen to Americans' phone calls or read their e-mails?

ALEXANDER: That is correct.

ROGERS: When -- Mr. Joyce, if you could help us understand that, if you get a piece of a number, there's been some public discussion that, gosh, there's just not a lot of value in what you might get from a program like this that has this many levels of oversight. Can you talk about how that might work into an investigation to help you prevent a terrorist attack in the United States?

JOYCE: Investigating terrorism is not an exact science. It's like a mosaic. And we try to take these disparate pieces and bring them together to form a picture. There are many different pieces of intelligence. We have assets. We have physical surveillance. We have electronic surveillance through a legal process; phone records through additional legal process; financial records.

Also, these programs that we're talking about here today, they're all valuable pieces to bring that mosaic together and figure out how these individuals are plotting to attack the United States here or whether it's U.S. interests overseas.

So, every dot, as General Alexander mentioned, we hear the cliché frequently after 9/11 about connecting the dots. I can tell you as a team, and with the committee and with the American public, we come together to put all those dots together to form that picture to allow us to disrupt these activities.

ROGERS: Thank you.

Given the large number of questions by members, I'm going to move along.

Mr. Ruppertsberger, for a brief...

RUPPERSBERGER: Firstly, I want to thank all the witnesses for your presentation, especially Mr. Cole -- a very good presentation. I think you explained the law in a very succinct way.

You know, it's unfortunate sometimes when we have incidents like this that a lot of negative or false information gets out. I think, though, that those of us who work in this field, in the intelligence field every day, know what the facts are and we're trying to now present those facts through this panel. That's important.

But I would say that I weren't in this field and if I were to listen to the media accounts of what occurred in the beginning, I would be concerned, too. So, this is very important that we get the message out to the American public that what we do is legal and we're doing it to protect our national security from attacks from terrorists.

Now, there are -- one area that, Mr. Litt, you -- you addressed this -- but I think it's important to just reemphasize the FISA court. You know, again, it's unfortunate, when people disagree with you, they attack you. They say things that aren't true. We know that these are federal judges in the FISA court. They have integrity, and that they will not approve anything that they feel is wrong. We have 90-day periods where the court looks at this issue.

I want to ask you, though, General Alexander, do you feel in any way that the FISA court is a rubber-stamp based on the process? Our forefathers created a great system of government, and that's checks and balances. And that's what we are. That's what we do in this country to follow our Constitution. It's unfortunate that these federal judges are being attacked.

ALEXANDER: I do not. I believe, as you have stated, the federal judges on that court are superb. Our nation would be proud of what they do and the way they go back and forth to make sure we do this exactly right.

And every time we make a mistake, how they work with us to make sure it is done correctly to protect our civil liberties and privacy and go through the court process. They have been extremely professional. There is, from my perspective, no rubber-stamp.

It's kind of interesting. It's like saying you just ran a 26-mile marathon; somebody said, "Well, that was just a jog." Every time we work with the court, the details and the specifics of that that go from us up through the FBI, through the Department of Justice and through the court on each one of those orders that we go to the court. There is tremendous oversight, compliance and work. And I think the court has done a superb job.

More importantly, if I could, what we worked hard to do is to bring all of these -- all these under court supervision for just this reason. I mean, we've done the right thing, I think, for our country here.

Thank you.

RUPPERSBERGER: Thank you for that answer.

The second area I want to get into, General Alexander, the public are saying, "Well, how did this happen?" We have -- we have rules. We have regulations. We have individuals that work in intelligence go through being -- persistently being classified. And yet here we have a technical person who had lost some jobs; had a background that wouldn't always would be considered the best.

We have to learn from mistakes how they've occurred. What system are you or the director of national intelligence of the administration putting into effect now to make sure what happened in this situation, that if another person were to -- to turn against his or her country, that we would have an alarm system that would not put us in this position right now?

ALEXANDER: So, this is a very difficult question, especially when that person is a system administrator and they get great access...

RUPPERSBERGER: Why don't you say what a system administrator is?

ALEXANDER: Well, a system administrator is one that actually helps operate, run, set the conditions, the auditing and stuff on a system or a portion of the network. When one of those persons misuses their authorities, this is a huge problem.

So working with the director of national intelligence, what we are doing is working to come up with a two-person rule and oversight for those, and ensure that we have a way of blocking people from taking information out of our system. This is work in progress. We're working with the FBI on the investigation. We don't have all the facts yet. We've got to get those. And as we're getting those facts, we are working through our system. Director Clapper has asked us to do that and providing that feedback back to the rest of the community.

RUPPERSBERGER: OK. Thank you.

I yield back.

ROGERS: (OFF-MIKE)

THORNBERRY: Thank you, Mr. Chairman.

And thank you all for being here, and for making some additional information available to the public. I know it's frustrating for you, as it is for us, to have these targeted narrow leaks and not be able to talk about the bigger picture.

General Alexander, you mentioned that you're going to send us tomorrow 50 cases that have been stopped because of these programs, basically. Four have been made public to this point. And I think there are two new ones that you are talking about today. But I would invite you to explain to us both of those two new cases -- Mowlin (ph) and the Operation WiFi case. And one of them starts with a 215; one of them starts with a 702.

And so I think it's important for you to provide the information about how these programs stopped those terrorist attacks.

ALEXANDER: OK. I'm going to defer this, because the actual guys who actually do all the work and (inaudible) is the FBI, and get it exactly right. I'm going to have Sean do that. Go ahead, Sean.

JOYCE: So, Congressman, as I mentioned previously, NSA on the Op WiFi, which is Khalid Ouazzani out of Kansas City. That was the example that I referred to earlier. NSA, utilizing 702 authority, identified an extremist located in Yemen. This extremist located in Yemen was talking with an individual located inside the United States in Kansas City, Missouri. That individual was identified as Khalid Ouazzani.

The FBI immediately served legal process to fully identify Ouazzani. We went up on electronic surveillance and identified his co-conspirators. And this was the plot that was in the very initial stages of plotting to bomb the New York Stock Exchange. We were able to disrupt the plot. We were able to lure some individuals to the United States. And we were able to effect their arrest. And they were convicted for this terrorist activity.

THORNBERRY: OK. Just so I -- on that plot, it was under the 702, which is targeted against foreigners, that some communication from this person in Yemen back to the United States was picked up. And then they turned it over to you at the FBI to serve legal process on this person in the United States.

JOYCE: That is absolutely correct. And if you recall, under 702, it has to be a non-U.S. person outside the United States, and then also one of the criteria is linked to terrorism.

THORNBERRY: OK. Would you say that this -- their intention to blow up the New York Stock Exchange was a serious plot? Or is this something that they kind of dreamed about, you know, talking among their buddies?

JOYCE: I think the jury considered it serious, since they were all convicted.

THORNBERRY: OK. And -- and what about the other plot? October, 2007, that started I think with a 215?

JOYCE: I refer to that plot. It was an investigation after 9/11 that the FBI conducted. We conducted that investigation and did not find any connection to terrorist activity. Several years later, under the 215 business record provision, the NSA provided us a telephone number only, in San Diego, that had indirect contact with an extremist outside the United States.

We served legal process to identify who was the subscriber to this telephone number. We identified that individual. We were able to, under further investigation and electronic surveillance that we applied specifically for this U.S. person with the FISA court, we were able to identify co-conspirators and we were able to disrupt this terrorist activity.

THORNBERRY: I'm sorry. Repeat for me again what they were plotting to do.

JOYCE: He as actually -- he was providing financial support to an overseas terrorist group that was a designated terrorist group by the United States.

THORNBERRY: But there was some connection to suicide bombings that they were talking about, correct?

JOYCE: Not in the example that I'm citing right here.

THORNBERRY: Oh, I'm sorry, the group in Somalia to which he was

financing, that's what they -- that's what they do do in Somalia, correct?

JOYCE: That is correct, and as you know, as part of our classified hearings regarding the American presence in -- in that area of the world.

THORNBERRY: OK. OK, thank you.

Chairman (OFF-MIKE)

ALEXANDER: If I could, Congressman, just -- just hit a couple key points. It's over 50 cases. And the reason I'm not giving a specific number is we want the rest of the community to actually beef those up and make sure that (inaudible) we have there is exactly right. I'd give you the number 50X. But if somebody says, "Well, not this one." Actually, what we're finding out is there are more. They said, "You missed these three or four." So those are being added to the packet.

On the top of that packet we'll have a summary of all of these, the listing of those. I believe those numbers are things that we can make public, that you can use, that we can use. And we'll try to give you the numbers that apply to Europe, as well, as well as those that had a nexus in the United States.

The issue on terms of releasing more on the specific overseas cases is (inaudible) our -- it's our concern that in some of those -- now, going into further details of exactly what we did and how we did it may prevent us from disrupting a future plot.

So that's something that work in progress. Our intent is to get that to the committee tomorrow for both -- both Intel Committees for the Senate and House.

THORNBERRY: Great. Thank you.

ROGERS: Mr. Thompson?

THOMPSON: Thank you, Mr. Chairman.

Thank you all very much for being here and for your testimony and for your service to our country.

Mr. Litt, before going to a hearing, does or has the FISA court ever rejected a case that's been brought before it?

LITT: I believe the answer to that is yes, but I would defer that to the deputy attorney general.

COLE: It has happened. It's not often, but it does happen.

THOMPSON: Thank you.

Mr. Cole, what kinds of records comprise the data collected under the business records provision?

COLE: There's a couple of different kinds. The shorthand -- and it's required under the statute -- is the kinds of records you could get with a grand jury subpoena. These are business records that already exist. It could be a contract. It could be something like that.

In this instance that we're talking about for this program, these are telephone records. And it's just like your telephone bill. It'll show a number called, the date the number was called, how long the call occurred; a number that called back to you. That's all it is, not even identifying who the people are that's involved.

THOMPSON: Have you previously collected anything else under that authority?

COLE: Under the 215 authority?

THOMPSON: Correct.

COLE: I'm not sure beyond the 215 and the 702 that -- answering about what we have and haven't collected has been declassified to be talked about.

THOMPSON: OK.

It was said that there's been cases where there was data inadvertently or mistakenly collected and then subsequently destroyed. Is that...

COLE: That's correct.

THOMPSON: And -- and there actually has been data that has been inadvertently collected and it was destroyed, nothing else was done with it?

COLE: That's correct. The -- this is a very strict process that we go through in that regard. You can get a wrong digit on a phone number and you collect the wrong number, something like that. And when that's discovered, that's taken care of in that way.

THOMPSON: And who does the checking? Who -- who determines if something has been inadvertently collected and then decides that it's -- needs to be destroyed?

COLE: Well, I'll -- I'll refer over to NSA in the first instance, because they do a very robust and vigorous check internally themselves. But then as an after-the-fact, the Department of Justice and ODNI and the inspector general for NSA also do audits and make sure that we understand all the uses. And if there's any compliance problems that they're identified, that they're given to the court, they're given to the Congress, and they're fixed.

THOMPSON: I -- I don't think I need anything more than -- than that.

General Alexander, can you tell us what Snowden meant during this chat thing that he did when he said that NSA provides Congress with,

and I quote, "a special immunity to its surveillance"?

ALEXANDER: I have no idea.

THOMPSON: Anybody else?

ALEXANDER: I'm not sure I understand the context of the special immunity.

THOMPSON: I -- I don't either. That's why...

(CROSSTALK)

ALEXANDER: We treat you with special respect.

(LAUGHTER)

THOMPSON: He said with a "special immunity to its surveillance."

ALEXANDER: I -- I have no idea. I think it may be in terms of disseminating any information, let's say, not in this program but in any program that we have, if we have to disseminate U.S. persons data or a threat to a U.S. member of Congress, we're not allowed to say the name unless it's valuable to one of the investigations or (inaudible).

So we can't just put out names and stuff in our things (ph). So part of the minimization procedures protects the who.

Did you want to add to that?

INGLIS (?): No, I would simply have said that your status as U.S. persons gives you a special status, as we've described throughout this hearing.

THOMPSON: If you -- if that does surface and you do figure that out you'll get that information to us?

Also the president kind of suggested, I guess, in his television interview the other night that the New York subway bomber could not have been or would not have been caught without PRISM. Is that true?

JOYCE: Yes, that is accurate. Without the 702 tool we would not have identified Najibullah Zazi.

THOMPSON: Thank you. I have no further question.

I yield back the balance of my time.

ROGERS: Mr. Miller?

MILLER: Thank you, Mr. Chairman.

General Alexander, which agency actually presents the package to the FISA court for them to make their decision?

ALEXANDER: Well, it's actually -- business records, FISA, it's the FBI (inaudible).

Go ahead.

JOYCE: The FBI is part of the process. It then goes over to the Department of Justice. And they are the ones -- if the DAG wants to comment on that.

COLE: The formal aspect of the statute allows the director of the FBI to make an application to the court. The Justice Department handles that process. We make the -- put all the paperwork together. And it must be signed off on before it goes to the court by either the attorney general, myself, or if we have a confirmed assistant attorney general in charge of the National Security Division, that person is authorized. But it has to be one of the three of us to sign it before it goes.

MILLER: The court is a single judge?

COLE: The judges sit kind of in -- in rotation in the court presiding over it. These are all Article 3 judges. They have lifetime appointments. They have their districts that they deal with, and they are selected by the chief justice to sit on the FISA court for a period of time. And so they will rotate through and be the duty judges that are required for this.

MILLER: I guess the crux of my question is, would there be a way that if you did not get the answer that you wanted from a certain judge could you go to another FISA court judge and ask for another opinion?

COLE: I -- I think that would be very, very difficult to do, because the staff at the FISA court does a great deal of the prep work and they're gonna recognize when they've thrown something back that if you're coming back and you haven't made any changes to correct the deficiencies that caused them to throw it back, my guess is they'll throw it back again.

MILLER: And I think one of the things that a lot of people don't understand -- and it was alluded to by Mr. Litt; and I think, Mr. Cole, you have also discussed it -- and that's the read-ahead document that the court gets, the opportunity. A lot of focus has been made on the fact that as my colleague, Mr. Thompson said, court's a rubberstamp. But they do have an opportunity to review the documents prior to rendering a decision.

COLE: They do. And it's by no means as a rubber stamp. They push back a lot. And when they see something -- these are very thick applications that have a lot in them. And when they see anything that raises an issue, they will push back and say, "We need more information about this area. We need more information about that legal issue. We need more information about your facts in certain areas."

This is by no means a rubberstamp. There is an enormous amount of work. And they make sure -- they're the ones to make sure that the privacy and the civil liberty interests of United States' citizens are honored. They're that bulwark in this process. So they -- they have to be satisfied.

MILLER: There's been some discussion this morning on the inadvertent violation of a court order where data has been collected and then destroyed. But has there ever been any disciplinary action taken on somebody who inadvertently violated an order?

COLE: Not that I'm aware of. And I think one of the statistics that Mr. Inglis had included in his comment was that in the history of this, there has never been found an intentional violation of any of the provisions of the court order, or any of the collection in that regard. So the -- the nature of the kinds of anomalies that existed were technical errors, were typographical errors, things of that nature as opposed to anything that was remotely intentional. So there would be in those instances, no reason for discipline. There may be reason to make sure our systems are fixed so that a technical violation, or technical error doesn't exist again because we've identified it. But nothing intentional.

LITT: Can I just add one thing to that point? An important part of the oversight process that the Department of Justice, and the ODNI engage in is when compliance problems are identified, and the vast majority of them are self-identified by NSA, but when a compliance issue is identified, we go and look at it and say, OK are there changes that need to be made in the system so that this kind of mistake doesn't happen again? It's a constantly improving process to prevent problems from occurring.

MILLER: Thank you. I yield back.

ROGERS: Ms. Schakowsky?

SCHAKOWSKY: Thank you Mr. Chairman. General Alexander, do you feel that this open hearing today jeopardizes in any way our national security?

ALEXANDER: I don't think the sharing itself jeopardizes it. I think the damage was done in the release of the information already. I think today what we have the opportunity is (sic) so where it makes sense, provide additional information on the oversight, the compliance and some of the -- the statistics, without jeopardizing it. So to answer your question, no. We're being very careful to do that, and I appreciate what the committee has done on that.

SCHAKOWSKY: How many people were in the same position as Snowden was, as a systems manager to have access to this information that could be damaging if released?

ALEXANDER: Well, there are system administrators throughout NSA and in our -- all our complexes around the world. And there is on the order of a thousand system administrators, people who actually run the networks that have, in certain sections, that -- that level of authority and ability to interface with...

SCHAKOWSKY: How many of those are outside contractors, rather than...

ALEXANDER: The majority are contractors. As you may know, as

you may recall, about 12-13 years ago as we tried to downsize our government work force, we pushed more of our information technology workforce or system administrators to the contract arena. That's consistent across the intelligence community.

SCHAKOWSKY: I would -- I would argue that this conversation that we're having now could have -- could have happened unlike what you said Mr. Litt. And perhaps we disagree also, General Alexander, that the erosion of trust, the misconceptions and the misunderstandings that resulted and why would assume that when there's 1,000 -- are there any more than 1,000 by the way?

ALEXANDER: Well, we're actually counting all of those positions. I'll get you an accurate number.

SCHAKOWSKY: That -- that some of this information would not have become public. And that the effort that has to convince the American public of the necessity of this program, I think would suggest that we would have been better off at having a discussion of vigorous oversight, the legal framework, et cetera up front, and how this could prevent perhaps another 9/11, and in fact, 50 or so, attacks. Let me ask you this, Mr. Cole, you know you -- you were talking about transparency, and you were saying that -- essentially that while the Verizon phone records order looked bad on its face, that there are other FISA court orders that talk in more depth about the legal rationale, about -- about what we're -- what we're doing.

So, will you release those court opinions with the necessary redactions, of course? And if not, why?

COLE: Well, I'm going to refer that over to Mr. Litt because the classifying authority on that would be DNI.

LITT: As you may know, we have been working for some time on trying to declassify opinions of the FISA court. It's been a very difficult task, because like most legal opinions, you have facts intermingled with legal discussion. And the facts frequently involve classified information, sensitive sources and methods. And what we've been discovering is that when you remove all of the information that needs to be classified, you're left with something that looks like Swiss cheese, and is not really very comprehensible. Having said that, I think as -- as General Alexander said, there's information out in the public domain now. There's -- the director of national intelligence declassified certain information about these programs last week.

And as a result of that, we are going back, taking another look at these opinions to see whether, in light of that declassification, there's now -- we can make a more comprehensible release of the opinion. So the answer to that is, we are looking at that and -- and frankly we would like to release it to the public domain, as much of this as we can, without compromising national security.

SCHAKOWSKY: I think -- General Alexander, so what other types of -- of records are collected under this Section 215? Can -- can you talk about that at all?

ALEXANDER: Yeah, for NSA the only -- the only records that are

collected under business records 215 is this telephony data. That's all.

SCHAKOWSKY: And is there authorization to collect more?

ALEXANDER: Under 215 for us? No, this is the only -- that we do. Now it gets into other authorities, but it's not ours. And I don't now if the -- I'll pass that to the attorney general because you're asking me now outside of NSA.

COLE: 215 is generally -- is a general provision that allows the acquisition of business records if its relevant to a national security investigation. So that showing has to be made to the court to allow that subpoena to issue that there is a relevance, and a connection. And that can be any -- any number of different kinds of records that a business might maintain; customer records, purchase orders, things of that nature. Somebody buys materials that they could buy an explosive out of, you could go to a company that sells those and get records of the purchase. Things of that nature.

SCHAKOWSKY: What about e-mails?

COLE: E-mails would not be covered by business records in that regard. You would have to -- under the Electronic Communications Privacy Act, you get specific court authorization for e-mails, that's stored content. If you're going to be looking at them in real time while they're going, you're going to have a separate FISA court order that would allow you to do that. It wouldn't be covered by the business records.

SCHAKOWSKY: Thank you Mr. Chairman.

ALEXANDER: Could I just make sure -- one clear part on the system administrator versus -- so what you get access to is helping to run the network, and the web servers that are on that network that are publicly available. To get to any data, like the business records 215 data that we're talking about, that's in an exceptionally controlled area. You would have to have specific certificates to get into that. I am not aware that he had -- he, Snowden, had any access to that. And on the reasonable articulable suspicion numbers and on what we're seeing there, I don't know of any inaccurate RAS numbers that have occurred since 2009.

There are rigorous controls that we have from a technical perspective that once the numbers can -- is considered RAS-approved, that you put that number in. You can't make a mistake because the system helps correct that now. So that -- that is a technical control that we have put in there.

SCHAKOWSKY: Thank you. I yield back.

CONAWAY: Well, thank you gentlemen. General Alexander thank you for your long service. Mr. Cole and Mr. Inglis went through -- through a very extensive array of the oversight and internal controls that are associated with -- with what's going on. In a business environment, Sarbanes-Oxley requires that companies go through their entire system to make sure that, not only do the details trees work,

but that the forest works as well. Is there any one at -- in the vast array of what you guys are doing that steps back and says, all right, we're -- the goal is to protect privacy and our civil liberties and we're doing the very best we can.

Is there a -- an internal control audit, so to speak that looks at the entire system that says, we've got the waterfront covered? And we're doing what we need to do?

COLE: I'll start. I mean there are these periodic reviews that I've described that audit everything that is done under both of these programs by both NSA and the Department of Justice, and the Office of the Director of National Intelligence, and we report to the court, and we report to Congress. So all of that is done looking at the whole program at the same time.

CONAWAY: I guess I -- Mr. Cole I'm looking at the -- the program of that. I understand that those pieces work really well, and that that's their design to -- to go at it and create the -- that kind of audit process. But is there an overall look at -- at everything that is done to say, we've got it all covered? Or -- and if we don't, and there are suggestions that we need to improve it, where do those suggestions get vetted? And have we had suggestions for improvement that we said, no, we don't need to do that?

LITT: Mr. Conaway if I might speak on that, there are at least two levels at which that takes place.

One is by statute within the Office of the Director of National Intelligence, there is -- there is a civil liberties protection officer -- his name is Alex Joel, who's an incredibly capable person whose job it is to take exactly that kind of look at our programs and make suggestions for the protection of civil liberties.

Outside of -- of the intelligence community, there...

(CROSSTALK)

CONAWAY: And that person would have the requisite clearances to know all the details?

(CROSSTALK)

LITT: Absolutely. He is -- he is, in fact, part of this audit process as well, his office is.

The second thing is that -- is that outside of the intelligence community, the president's Civil Liberties Oversight Board, which has -- has five confirmed members is also charged with evaluating the impact of our counterterrorism programs on privacy and civil liberties.

They also have full clearances. They have the ability to get full visibility into this program. In fact, they have recently been briefed on these programs, and I know they are, in fact, looking at them to make exactly that kind of assessment.

(CROSSTALK)

CONAWAY: And who -- who do they report to? Is that report public?

LITT: It's the president's board. I suspect that to the extent they're making a classified report, it would not be public. To the extent that they can make an unclassified report, it's up to them whether or not it becomes public.

CONAWAY: Several of you mentioned the term "minimization" and then also five-year destruction, rolling five-year window on the -- on the business record issues. You've used the word "purge," "get rid of," "destroy."

In an electronic setting, can you help us understand exactly what that means? I understand when I shred a piece of paper into the thousand-and-one pieces, that's one thing. But given the number of times you back up data and all the other, can a citizen feel like that once the minimization worked, that this electronically, we have in fact deleted all these things that are -- that we're supposed to delete?

INGLIS: So I'll start at that. Yes, sir, I believe that we can. We have a fairly comprehensive system at NSA that whenever we collect anything, whether it's under this authority or some other, we actually bind to that communication where we got it, how we got it, what authority we got it under so that we know precisely whether we can retain it for some fixed period of time.

And if it simply ages off, as in the case of the B.R. FISA data we talked about, at the expiration of those five years, it is automatically taken out of the system. Literally just deleted from the system.

CONAWAY: OK. And it's mechanically overwritten and all of the back-up copies of that are done away with, and...

INGLIS: Yes, sir.

CONAWAY: OK.

INGLIS: It's -- it gets fairly complicated very quickly, but we have what are called source systems of record within our architecture, and those are the places that we say if it -- if the data element has the right to exist, it's attributable to one of those. And if it doesn't have the right to exist, you can't find it in there.

And we have very specific lists of information that determine what the provenance of data is, how long that data can be retained. We have on the other side of the coin purge lists that if we were authorized -- if we were required to purge something, that item would show up explicitly on that list. And we regularly run that against our data sets to make sure that we've checked and double-checked that those things that should be purged have been purged.

CONAWAY: All right.

One quick one: Any indication that the -- the FISA court has a problem with resources necessary to run its oversight piece?

INGLIS: Not that I'm aware of right now. But, obviously, the courts are suffering under sequestration, like everybody else. So I don't know what's gonna hit them as we go forward.

CONAWAY: Thank you, sir,

I yield back.

ROGERS: Mr. Conaway.

Mr. Langevin?

LANGEVIN: Thank you, Mr. Chairman.

And gentlemen, I want to thank you all for your testimony here today and for your service to our -- our country.

I'm -- as members of the committee, I have been briefed on the program, and -- and I know the excess of due diligence you've gone through to make sure that this is done right.

So I think it's important that this discussion is being had this morning. And hopefully it's gonna give greater confidence to the American people that all the agencies involved have dotted their i's and crossed their t's.

I especially think it's helpful that we have the discussion about the FISA court today and -- and how detailed the -- the requests have to be before they get approval and it's made clear that these are not just one-page documents that are presented to a FISA judge and then it's rubber stamped.

It actually goes through excessive due diligence, and -- and before it even gets to the point where the judge sees it. And, obviously, if the -- if all the criteria have been met, then it gets -- it gets approved, and if it's -- if the criteria have not been met, it's gonna be rejected.

So, I won't belabor that point, excepting that's been had -- been a very fruitful discussion.

But can you talk further about the -- again the role of the I.G. and go into that -- that -- that process a little more so that the -- the amount of review the I.G. does, once a query has been made in terms of the range of queries that have been made, I think that's -- would be important to clarify.

INGLIS: I would just start with that, and then defer to the ODNI and the attorney general -- deputy attorney general for some followup.

And so, at NSA, any analyst that wants to form a query, regardless of whether it's this -- this authority or any other, essentially has a two-person control rule. They would determine

whether this query should be applied, and there's someone who provides oversight on that.

We've already learned that under the metadata records that are captured by the B.R. FISA program, that there's a very special court-defined process by which that's done.

Those are all subject to the I.G., the inspector general's review on a periodic basis, such that we can look at the procedures as defined, the procedures as executed, reconcile the two and ensure that internal to NSA, that that's done exactly right. There are periodic reports that the I.G. has to produce on these various programs, and they are faithfully reported.

But I think the real checks and balances within the executive branch happen between NSA and the Department of Justice, the Office of the Director of National Intelligence. And because NSA also has a foot within the Department of Defense, the Department of Defense enters into that as well. They have intelligence oversight mechanisms.

And between those four components, there is rich and rigorous oversight which varies in terms of the things that they look for, based upon the authorities. B.R. FISA is a particularly rigorous authority. But they all have checks and balances to transcend just NSA.

LANGEVIN: OK.

COLE (?): And, Congressman, if I -- if I could add to that, and I refer you to a recent review by the DOJ inspector general on the 702 program that was highly complimentary of all the checks and balances that were in place.

LANGEVIN: Thank you.

So let me turn my attention now to -- I know these programs primarily target non-U.S. persons, but can you -- and this is probably a question for you, Mr. Joyce, just to clarify, you've said that if a U.S. person or a -- the overseas or the United States or a non-U.S. person living in the United States, that if they're -- we become aware that they may be involved in terrorist activity that they are served -- processed.

Can you go into that level of detail of what then happens and how the courts are involved with -- if we become aware that a U.S. person is involved?

JOYCE: So -- so I think either -- maybe I misspoke or -- or you misspoke. We -- we -- we are not looking at all at U.S. persons. The 702 is anyone outside the United States. And even if a U.S. person is outside of the United States, it does not include it in the 702 coverage.

OK, so it's a non-U.S. person outside the United States, and it has to have -- there's three different criteria it goes through. One of those links is terrorism. So that is where specifically only certain individuals are targeted. Those ones, one of the criteria,

linked to terrorism.

On numerous occasions, as I've outlined in some of the examples, those individuals outside the United States were discovered communicating with someone inside the United States.

We then -- that is, being tipped from the NSA. We then go through the legal process here, the FBI does, regarding that U.S. person. So we go and we have to serve what's called a national security letter to identify the subscriber. It's much like a subpoena.

Following that, if we want to pursue electronic surveillance, we have to make a specific application regarding that person with the FISA court here.

LANGEVIN: That's what I was looking for. So thank you very much.

I yield back.

(OFF-MIKE)

ALEXANDER: Sir, if I could, just to follow on and -- and to clarify, 'cause as we're going through this, I want to make sure that everything we say is exactly right -- from from my perspective. And so, as Sean said, NSA may not target the phone calls or e-mails of any U.S. person anywhere in the world without individualized court orders.

LANGEVIN (?): OK. Thank you.

ROGERS: That's an important point we can't make enough.

Mr. Lobiondo?

LOBIONDO: Thank you. Thank you, Mr. Chairman.

General Alexander and team, thank you for helping -- helping us understand in so many closed sessions and hopefully helping the nation understand what we're doing, why we're doing it, and how we're doing it.

I want to focus a little bit more on 702, if we could.

And, General Alexander, could you -- could you explain what happens if a target of surveillance is communicating with a U.S. person in the United States?

ALEXANDER: So, under 702, I think the best case is some that Sean Joyce made. If we see, if we're tracking a known terrorist in another country, say Pakistan, Yemen or someplace, and we see them communicating with someone in the United States, and it has a terrorism nexus, focused on doing something in the United States, we tip that to the FBI.

So our job is to identify, see the nexus of it. It could be in another country as well. So sometimes, we'd see somebody in that --

one of those countries planning something in Europe or elsewhere. We would then share that through intelligence meetings to those countries.

But when it comes into the United States, our job ends. We're the outside and we provide that to the inside FBI to take it from there. So they, then, take it and say, "Does this make sense?" They'll go up, as Sean explained, look at the process for getting additional information to see if this is a lead worth following.

LOBIONDO: And what does the government have to do if it wants to target a U.S. person under FISA when they're located abroad -- when they're not here? What -- what would be the process for the government?

COLE: That would be the -- a full package going to the FISA court, identifying that person; identifying the probable cause to believe that that person is involved in either terrorism or foreign intelligence activities; and indicating that we have then the request to the court to allow us to intercept their communications because we've made the showing that they're involved in terrorist or foreign intelligence activities.

So we'd have to make a formal application targeting that person specifically, whether they're inside or outside of the United States.

LOBIONDO: And what if you...

(CROSSTALK)

INGLIS: And, sir, if I might. And again, that could not be done under 702. There's a separate section of the Foreign Intelligence Surveillance Act that would allow that, but it would not be doable under 702.

LOBIONDO: And -- and what if you want to monitor someone's communication in the United States?

COLE: Same thing. Again, a different provision of FISA, but we would have to show that that person is in fact with probable cause involved in foreign terrorist activities or foreign intelligence activities on behalf of a terrorist organization or a foreign power. We'd have to lay out to the court all of those facts to get the court's permission to then target that person.

LOBIONDO: So, I just want to reemphasize that. You -- you have to specifically go to the FISA court and make your case as to why this information is necessary to be accessed.

COLE: That's correct.

LOBIONDO: And without that, you have no authority and cannot do it and do not do it.

COLE: That's correct.

LOBIONDO: OK. Thank you.

I yield back, Mr. Chairman.

ROGERS: Great. Thank you very much.

Mr. Schiff?

SCHIFF: Thank you, Mr. Chairman.

And thank you, gentlemen, for your work.

On the business records program, the general FISA court order allows you to get the metadata from the communications providers. Then when there are reasonable and articulable facts, you can go and see if one of the numbers has a match in the metadata.

On those 300 or so occasions when you do that, does that require separate court approval? Or does the general FISA court order allow you, when your analysts have the reasonable, articulable facts, to make that query? In other words, every time you make the query, does that have to be approved by the court?

COLE: We do not have to get separate court approval for each query. The court sets out the standard that must be met in order to make the query, in its order. And that's in the primary order. And then that's what we audit in a very robust way in any number of different facets through both executive branch and then give it to the court, and give it to the Congress.

So we're given that 90-day period with these parameters and restrictions to access it. We don't go back to the court each time.

SCHIFF: And does the court scrutinize after you present back to the court, "these are the occasions where we found reasonable articulable facts," do they scrutinize your basis for conducting those queries?

COLE: Yes, they do.

SCHIFF: General Alexander, I wanted to ask you. I raised this in closed session, but I'd like to raise it publicly as well. What are the prospects for changing the program such that rather than the government acquiring the vast amounts of metadata, the telecommunications retain the metadata, and then only on those 300 or so occasions where it needs to be queried, you're querying the telecommunications providers for whether they have those business records related to a reasonable articulable suspicion of foreign terrorist connection?

ALEXANDER: I think jointly the FBI and NSA are looking at the architectural framework of how we actually do this program and what are the advantages and disadvantages of doing each one. Each case, as you know from our discussions, if you leave it at the service providers, you have a separate set of issues in terms of how you actually get the information, then how you have to go back and get that information, and how you follow it on and the legal authority for them to compel them to keep these records for a certain period of time.

So what we're doing is we're going to look at that and come back to the director of national intelligence, the administration and then to you all, and give you recommendations on that for both the House and the Senate. I do think that that's something that we've agreed to look at and that we'll do. It's just going to take some time. We want to do it right.

And I think, just to set expectations, the -- the concern is speed in crisis. How do we do this? And so that's what we need to bring back to you, and then I think have this discussion here and let people know where we are on it.

Anything that you wanted to add?

SCHIFF: I would -- I would strongly encourage us to vigorously investigate that potential restructuring. Even though there may be attendant inefficiencies with it, I think that the American people may be much more comfortable with the telecommunications companies retaining those business records, that metadata, than the government acquiring it, even though the government doesn't query it except on very rare occasions.

ALEXANDER: So it may be something like that that we'd bring back and look at. So we are going to look at that. And we have already committed to doing that and we will do that, and go through all the details of that.

SCHIFF: Mr. Litt, I wanted to ask you about the FISA court opinions. This week, I'm going to be introducing the House companion to the bipartisan Merkley bill that would require disclosure of certain FISA court opinions, again, in a form that doesn't impair our national security.

I recognize the difficulty that you described earlier in making sure those opinions are generated in a way that doesn't compromise the programs. You mentioned that you're doing a review, and I know one's been going on for sometime. In light of how much of the programs have now been declassified, how soon do you think you can get back to us about whether you're going to be able to declassify some of those FISA court opinions?

LITT: I'm hesitant to answer any question that begins "how soon," partly because there are a lot of agencies with equities in this, partly because there's a lot else going on in this area. My time has not been quite as free-up to address this topic as I would have liked over the last week-and-a-half.

I can tell you that -- that I've asked my staff to work with the other agencies involved and try to press this along as quickly as possible. We're trying to identify those opinions where we think there's the greatest public interest in having them declassified, and start with those. And we'd like to push the process through as quickly as possible at this point.

SCHIFF: And I would just encourage in the last second that beyond the two programs at issue here, to the degree you can

declassify other FISA court opinions, I think it's in the public interest.

LITT: Yes, I think that's part of what we're doing.

SCHIFF: Thank you, Mr. Chairman.

COLE: Congressman Schiff, I just wanted to correct a little bit one of the things I said. The FISC does not review each and every reasonable, articulable suspicion determination. What does happen is they are given reports every 30 days in the aggregate. And if there are any compliance issues, if we found that it wasn't applied properly, that's reported separately to the court.

ROGERS: Do you have a followup?

SCHIFF: Thank you, Mr. Chairman. I just want to make sure I understood what you just said. A prior court approval is not necessary for a specific query. But when you report back to the court about how the order has been implemented, you do set out those cases where you found reasonable articulable facts and made a query. Do you set out those with specificity or do you just say "on 15 occasions, we made a query"?

COLE: It's more the latter -- the aggregate number where we've made a query. And if there's any problems that have been discovered, then we with specificity report to the court those problems.

SCHIFF: It may be worth considering providing the basis of the reasonable and articulable facts and having the court review that as a -- as a further check and balance. I'd just make that suggestion.

ROGERS: Mr. Cole, my understanding, though, is that every access is already preapproved; that the way you get into the system is court-approved. Is that correct?

COLE: That's correct.

The court sets out the standards which have to be applied to allow us to make the query in the first place. Then the application -- the implementation of that standard is reviewed by NSA internally at several levels before the actual implementation is done. It's reviewed by the Department of Justice. It's reviewed by the Office of the Director of National Intelligence. It's reviewed by the inspector general for the National Security Agency. So there's numerous levels of review of the application of this. And if there are any problems with those reviews, those are then reported to the court.

ROGERS: And -- and just to be clear, so if they don't follow the court-approved process, that would be a variation, that would have to be reported to the court?

COLE: That's correct.

ROGERS: OK. But you are meeting the court-approved process with every query?

COLE: That's correct.

INGLIS: And sir, if I might add to that that every one of those query is audited, those are all reviewed by the Department of Justice. Those are the reviews that we spoke about -- spoke about at 30 and 90 days. And there's a very specific focus on those that we believe are attributable to U.S. persons despite the fact that in (inaudible) FISA we don't know the identities of those persons. And so the court gets all of those reports.

SCHIFF: Thank you, Mr. Chairman.

I -- I just point out, all those internal checks are valuable, but they're still internal checks. And it may be worthwhile having the court, if not prospectively at least after the fact review those determinations.

Thank you, Mr. Chairman.

NUNES: Thank you, Mr. Chairman.

Mr. Cole, really what's happened here is that the totality of many problems within the executive branch has now tarnished the fine folks at the NSA and the CIA. And I just made a short list here, but, you know, right after Benghazi there was -- there's lies after Benghazi, four dead Americans. Fast and Furious, the Congress still is missing documents. We have dead Americans and dead Mexican citizens. You at least tapped into or got phone records from AP reporters, Fox News reporters, including from the House Gallery right here within this building.

Last week, as you know, A.G. Holder has been -- is being accused by the Judiciary Committee of possibly lying to the committee.

And then to top it all off, you have, you know, an IRS official who with other officials ran like a covert media operation on a Friday to help, you know, try to release documents to think that this would just go away about the release of personal data from U.S. citizens from the IRS.

So now -- you know, I understand when my constituents ask me, "Well, if the IRS is leaking personal data" -- General Alexander, this question's for you -- "how do I know for sure that the NSA and the -- and (inaudible) people that are trying to protect this country aren't leaking data?"

So Mr. -- Mr. Rogers asked the question about, you know, how do we know that -- that someone from the White House just can't go turn a switch and begin to listen to their phone conversations?

So General, I think if you could clarify the -- kind of the difference in what the people that are trying to protect this country are doing and what they go through, the rigorous standards. I think it would help, I think, fix this mess for the American people.

ALEXANDER: Thank you, Congressman.

I think the key -- the key facts here. When we disseminate data, everything that we disseminate and all the queries that are made into the database are 100 percent auditable. So they are audited by not only the analysts who's actually doing the job but the overseers that look and see, did he do that right or she do that right.

In every case that we have seen so far we have not seen one of our analysts willfully do something wrong like what you just said. That's where disciplinary action would come in.

What I have to overwrite -- underwrite is when somebody makes an honest mistake. These are good people. If they transpose two letters in typing something in, that's an honest mistake. We go back and say, now how can we fix it? The technical controls that you can see that we're adding in help fix that. But is -- it is our intent to do this exactly right.

In that, one of the things that we have is tremendous training programs for our people that they go through. How to protect U.S. persons data? How to interface with the business record FISA? The roles and responsibilities under FAA 702. Everyone, including myself, at NSA has to go through that training to ensure that we do it right.

And we take that very seriously. I believe the best in the world at (ph) terms of protecting our privacy. And I would just tell you, you know, the other thing that's sometimes confused here is that, "Well, then they're getting everybody else in the world." But our -- our approach is foreign intelligence -- you know, it's the same thing in Europe. We're not interested in -- in -- well, one, we don't have the time. And, two, ours is to protect our country and our allies. I think we do that better than anyone else.

Now, Chris, anything -- if you want to add to that?

INGLIS: No, I think that's exactly right. When somebody comes to work at NSA, just like elsewhere in the government, they take an oath to the Constitution not to NSA, not to some particular mission but to the Constitution and the entirety of that Constitution. Covers the issues importantly that we're discussing here today: national security and the protection of civil liberties. There's no distinction for us. They're all important.

NUNES: So I want to -- I want to switch gears a little bit here, General Alexander -- and perhaps this is a good question for Mr. Joyce. But I just find it really odd that right before the Chinese president comes to this country that all of these leaks happen and this guy has fled to -- to Hong Kong, this Snowden. And I'm really concerned that just -- the information that you presented us last week. This is probably gonna be the largest leak in American history -- and there's still probably more to come out. Can you just explain to the American people the seriousness of this leak and the damage -- you said earlier that it's damaged national security. Can you go into a few of those specifics?

JOYCE: Very -- no. Really, I can comment very little other than

saying it's and ongoing criminal investigation. I can tell you, as we've all seen, these are egregious leaks -- egregious. It has affected -- we are revealing in front of you today methods and techniques. I have told you, the examples I gave you, how important they have been. The first core Al Qaida plot to attack the United States post-9/11 we used one of these programs. Another plot to bomb the New York Stock Exchange, we used these programs. And now here we are talking about this in front of the world. So I think those leaks affect us.

NUNES: General?

ALEXANDER: It also -- it also affects our partnership with our allies, because the way it comes out -- and with industry. I mean, it's damaged all of those. Industry's trying to do the right thing, and they're compelled by the courts to do it. And we use this to also protect our allies and our interests abroad.

And so I think the way it's come out and the way it looks is that we're willfully doing something wrong when in fact we're using the courts, Congress and the administration to make sure that everything we do is exactly right. And as Chris noted, we all take an oath to do that, and we take that oath seriously.

NUNES: And in fact, just in closing here, Mr. Chairman, we know from the Mandiant report that came out that other governments are busy doing this and expanding their cyber warfare techniques. And I just want to say that, you know, it is so vital, as the chairman's pointed out many times, for the folks and the work that you're doing at NSA and all of your folks, how important that is to not only today's security but tomorrow's security.

So thank you for your service, General.

I yield back.

ROGERS: I -- I would just dispute the fact that other governments do it any -- any way, shape or form close to having any oversight whatsoever of their intelligence gathering programs.

Ms. Sewell?

SEWELL: Thank you, Mr. Chairman.

I also want to thank all of our witnesses today for your service to this country and for helping to maintain our national security.

I'd like to talk a little bit about the security practices. You've spent a lot of time really explaining to the American people the various levels of complexity in which you have judicial oversight and congressional oversight. How did this happen? How did a relatively low level administrator -- service systems administrator I think you said, General Alexander -- have classified information? And is it an acceptable risk?

I get that you have 1,000 or so system administrators. It is extremely frightening that you would go through such measures to do

the balancing act internally to make sure that we're balancing protection and security and -- and privacy, and yet internally in your own controls, there are system administrators that can go rogue. Is it an acceptable risk? How did it happen? And is there oversight to these system administrators?

ALEXANDER: Well, there is oversight. What we are now looking at is where that broke down and what happened. And that's gonna be part of the investigation that we're working with the FBI on.

I would just come back to 9/11. One of the key things was we went from the need to know to the need to share. And in this case, what the system administrator had access to is what we'll call the public web forums that NSA operates. And these are the things that talk about how we do our business, not necessarily what's been collected as a results of that; nor does it necessarily give them the insights of the training and the other issues that -- training and certification process and accreditation that our folks go through to actually do this.

ALEXANDER: So those are in separate programs that require other certificates to get into. Those are all things that we're looking at. You may recall that the intelligence community looked at a new information technology environment that reduces the number of system administrators.

If we could jump to that immediately, I think that would get us a much more secure environment and would reduce this set of problems. It's something that the DNI is leading and that we're supporting, as you know, across the community. I think that is absolutely vital to get to. And there are -- there are mechanisms that we can use there that will help secure this.

Please.

SEWELL: So the -- to be clear, Snowden did not have the certificates necessarily -- necessary to lead that public forum?

ALEXANDER: So each -- each set of data that we would have -- and, in this case, let's say the business records, FISA -- you have to have specific certificates -- because this is a cordoned off. So that would be extremely difficult for him -- you'd have to get up to NSA, get into that room.

Others require certificates for you to be working in this area to have that. It -- he would have to get one of those certificates to actually enter that area. Does that make sense? In other words, it's a key.

SEWELL: Well, I think that -- I would encourage us to figure out a way that we can declassify more information. I thank you for giving us two additional examples of -- of -- of terrorist attacks that we have thwarted because of these programs. But I think that providing us with as much information as you can on FISA courts' opinions -- how -- how that goes -- would help the American public de-mystify what we're doing here. I think that the examples -- the additional

examples that you gave today were great.

But I also am concerned that we have contractors doing -- I get that we cannot -- that there was a move at some point to -- to not have as many government employees, and so we sort of out-sourced it. But given the sensitivity of the information and the access, even for -- for relatively low-level employees, do you see that being a problem? And -- and how do we go about...

ALEXANDER: So we do have significant concerns in this area. And it is something that we need to look at. The mistakes of one contractor should not tarnish all the contractors because they do great work for our nation, as well. And I think we have to be careful not to throw everyone under the bus because of one person.

But you -- you raised two great points that I think we -- we will look at. One, how do we provide the oversight and compliance? And I talked to our technology director about the two-person control for system administrators to make any change. We are going to implement that. And I think, in terms of what we release to the public, I am for releasing as much as we can. But I want to weigh that with our national security, and I think that's what you expect. That -- that's what the American people...

SEWELL: Absolutely.

ALEXANDER: ... expect us. So that's where I need to really join that debate on this side to make sure that what we do is exactly right. I think on things like how we minimize data, how we run this program, the -- those kinds of things, I think we can -- we -- we're trying to be -- that's why Chris went through those great details.

I think those are things that the American people should know. Because what they find out is -- shoot, look at the oversight, the compliance, and the training that are people are going through. This is huge. This isn't some rogue operation that a group of guys up at NSA are running. This is something that have oversight by the committees, the courts, the administration in a 100 percent auditable process on a business record FISA.

You know, that's extraordinary oversight. And I think when the American people look at that, they say, "Wow, for less than 300 selectors, that amount of oversight --" and that's what we jointly agreed to do. I think that's tremendous.

SEWELL: I do too. I -- I -- I applaud the efforts. I just -- I think that, given the nature of this leak, you know, we don't want our efforts to be for naught, if, in fact, what happens is that the -- the leaks get the American people so concerned that they -- we roll back on these programs, and therefore increase our vulnerability as a nation. I think that all of us -- that's not in anyone's best interest.

Going back to sort of the difference between private contractors and government employees, is there a difference in the level of security clearance that...

ALEXANDER: Same level of security clearance and the same process for securing them.

SEWELL: OK.

Thank you. I yield back the rest of my time.

ROGERS: Thank you.

Mr. Westmoreland.

WESTMORELAND: Thank you, Mr. Chairman.

Mr. Cole, as Mr. Nunes had mentioned about some of the other things that have come out about leaks and so forth, could you -- because my constituents ask me the difference and maybe what the attorney general did in going to the court to -- on the Rosen case saying that he was an unindicted co-conspirator, because that was actually about a leak also. What type of process or internal review did y'all go over before you asked for those phones to be tapped? And, to make it perfectly clear, that was not in a FISA court. Is that correct?

COLE: Number one, that was not a FISA court. In the Rosen case, there were no phones being tapped. It was just to acquire a couple of e-mails. And there is a very, very robust system. It's set out in regulations that the Department of Justice follows of the kinds of scrubbing and review that must be done before any subpoena like that can be issued.

You have to make sure that you've exhausted all other reasonable avenues of investigation that -- that's done before you even get to the decision about whether or not such a -- a process should be used. You have to make sure that the information you're looking at is very, very tailored and only necessary -- truly necessary to be able to move the investigation forward in a significant way.

There has -- there are restrictions on what can be done with the information. And it goes through a very long process of review from the U.S. attorney's office through the United States attorney him or herself, into the, usually, the criminal division of the Justice Department, through the assistant attorney general of the criminal division, through the deputy attorney general's office and up, ultimately, to the attorney general signing it. It gets a lot of review before that's done under the criteria that we have in our guidelines and our CFR.

WESTMORELAND: So -- so the DOJ didn't -- because -- (inaudible) a security leak, the DOJ didn't contact the FBI or the NSA, or there was no coordination with that? It was strictly a DOJ criminal investigation?

COLE: Well, the FBI does criminal investigation with...

WESTMORELAND: I understand.

COLE: ... the Department of Justice. And they were contacted in that regard. But it was not part of the FISA process. It did not

involve the NSA.

WESTMORELAND: And I think that's what we need to be clear of, is...

COLE: Correct.

WESTMORELAND: ... that it was absolutely not part of the FISA -- process. And that is a lot more detailed and a lot more scrutinized as far as getting information than what this was. Is that correct?

COLE: Well, they're both very detailed and very scrutinized processes. They're -- they have different aspects to them. But they're both very unusually, frankly, detailed and scrutinized, both of those processes.

WESTMORELAND: Thank you.

And, General, going back to what Ms. Sewell had asked about the difference of clearance that you would have with a contractor or a government employee, when you have 1,000 different contractors -- I mean, I know the -- from my experience on having had one of my staff go through a security clearance, it's pretty -- it's a -- it's a pretty detailed operation. And I know that this gentleman had previously, I believe, heard that he had worked for the CIA. Had there been any further clearance given to this individual when he became a contractor after he left the employee of the CIA?

ALEXANDER: No additional clearance. He had what's needed to work at NSA or one of our facilities, the top secret special intelligence clearance. And that goes through a series of processes and reviews. The director of national intelligence is looking at those processes to make sure that those are all correct. And -- and he stated he's taken that on. We support that objective.

But to work at NSA, whether you're a contract, a government civilian, or a military, you have to have that same level of clearance.

WESTMORELAND: Does it bother you that this general had only been there for a short period of time? Or is there any oversight or review or whatever of the individuals are that carrying out this work? Is there any type of probation time or -- or anything? Because, you know, it seems that he was there a -- a very short period of time.

ALEXANDER: So he had worked in a couple of positions. He had just moved into the Booz Allen position in March. But he had worked in a information technology position for the 12 months preceding that at NSA Hawaii. So he'd actually been there 15 months. He moved from one contract to another.

WESTMORELAND: So would he have been familiar with these programs at his previous job?

ALEXANDER: Yes. And I believe that's where -- going out on what we call, the public classified web servers that help you understand

parts of NSA, that he gained some of the information, and -- and took some of that. I can't go into more detail.

LITT: Mr. Westmoreland, if I just might...

WESTMORELAND: Yes?

LITT: ... make one point there? When you say, would he have become familiar with these programs? I think part of the problem that we're having these days is that he wasn't nearly as familiar with these programs as he's portrayed himself to be. And thus -- this is what happens when somebody, you know sees a tiny corner of things and thinks that it gives them insight and viability into the program.

WESTMORELAND: Thank you. I yield back.

HIMES: Thank you Mr. Chairman and I too would like to thank the panel for appearing here today and for your service to the country. I think I've told each of you that in my limited time on this committee, I've been heartened by your competence, and by the competence of the agencies in which you work. I'll also add that I've seen nothing in the last week, week and a half to suggest that any of these programs that are being discussed, are operating in any way outside the law. And I would add that the controls that appear to be in place on these programs seem -- seem solid. I'll also say that I don't know that there's any way to do oversight without a posture of skepticism on the part of the overseers.

And so I hope you'll take my observations and questions in that spirit. And I'd like to limit my questions and observations purely to Section 215 and the Verizon disclosures, which quite frankly, trouble me. They trouble me because of the breadth and the scope of the information collection. They trouble me because I think this is historically unprecedented in the extent of the data that is being collected on potentially all American citizens. And the controls which you've laid out for us, notwithstanding, I think new (sic) for this country. We know that when a capability exists, there's a potential for abuse. Mr. Nunes ran through a lot of current issues going back to J. Edgar Hoover bugging the hotel rooms of Martin Luther King, to Nixon, to concerns around the IRS.

If a capability exists, from time to time it will be abused. And one of the things that I'm concerned about is this individual who I -- who's resume would I think make him -- make it unlikely that he would get an unpaid internship in my office, he had access to some of the most sensitive information that we have. And perhaps he could have, or someone like him, could have chosen a different path. Could have accessed phone numbers and -- though we spent a lot of time on the fact that you don't get names, we all know that with a phone number and Google, you can get a name pretty quickly.

He could have chosen to make a point about Congressman Himes making 2:00 am phone calls out of a bar in Washington. Or the CEO of Google making phone calls. Or anything really. Information that we hold to be private. So I guess -- I've got two questions. I guess I direct this one on 215 to Mr. Litt and then Mr. Cole. Where do we draw the line? So in other words, so long as the information is not

information to which I have a reasonable expectation of privacy under Maryland v. Smith and under Section 215 powers, where do we draw the line?

Could you, for example have video data? As I walk around Washington my -- I suppose that you could probably reconstruct my day with video that is captured on third-party cameras. Could you keep that in a way that is analogous to what you're doing with phone numbers? And again with all of the careful guards and what not, could you not reconstruct my day because I don't have a reasonable expectation of privacy around -- I know that's a hypothetical, but I'm trying to identify where the line is?

COLE: Well, I think the -- the real issue here is how it's accessed? What it can be used for? How you can actually...

HIMES: I -- I -- I'm stipulating that that system, even though we know it's not perfect, I'm stipulating that that system is perfect. And I'm asking, where is the limit as to what you can keep in the tank?

COLE: I -- I think some of it is a matter for the United States Congress to decide as policy matters, and the legislating that you do surrounding these acts, as to where you're going to draw those lines. Certainly the courts have looked at this and determined that under the statutes we have, there is a relevance requirement, and they're not just saying out of whole cloth you're allowed to gather these things. You have to look at it all together. And they're only saying that you can gather this volume under these circumstances, under these restrictions, with these controls. Without those circumstances and controls and restrictions, the court may well not have approved the orders under 215 to allow that collection to take place.

So you can't separate that out, one from the other and say, just the acquisition, what can we do? Because the acquisition comes together with the restrictions on access.

HIMES: And if those restrictions and controls are adequate, there's theoretically no restriction on your ability to store information on anything for which I do not have the reasonable expectation for privacy?

COLE: I'll refer back to NSA...

(CROSSTALK)

HIMES: Let me...

(CROSSTALK)

HIMES: ... I do have one more question.

(CROSSTALK)

HIMES: Yeah, this is the conversation -- I do have one more -- much more...

ALEXANDER: Can I...

HIMES: ... specific question.

ALEXANDER: ... can I hit...

HIMES: Yeah.

ALEXANDER: ... if I could. I'll ask for more time if I could, because I do think what you've asked is very important. So your question is, could somebody get out and get your phone number and see that you were at a bar last night? The answer is no. Because first in our system, somebody would have had to approve, and there's only 22 people that can approve, a reasonable articulable suspicion on a phone number. So first, that has to get input. Only those phone numbers that are approved could then be queried. And so you have to have one of those 22 break a law. Then you have to have somebody go in and break a law. And the system is 100 percent auditable, so it will be caught.

There is no way to change that. And so on that system, whoever did that would have broken the law. That would be willful. And then that person would be found by the court to be in violation of a court order, and that's much more serious. We have never had that happen.

HIMES: Yeah. No, I -- I thank you. I appreciate that, and I -- I sort of -- I think it's really important to explore these -- these bright lines about what you can keep and what you can't. Again, I don't see anything about the control systems that are troubling, but I do have one last quick question if the chairman will indulge me in. General, this is I guess for you and it's -- it's something that I asked you in closed session. As we weigh this, because obviously we're weighing security against privacy and what not, as we weigh this, I think it's really important that we understand exactly the national security benefit. And I limit myself to 215 here. 50 episodes. I don't think it's adequate to say that 702 and 215 authorities contributed to our preventing 50 episodes. I think it's really essential that you grade the importance of that contribution. The question I asked you, and -- and you can answer now, or I'd really like to get into this. How many of those 50 episodes would have occurred, but for your ability to use the Section 215 authorities as disclosed in the Verizon situation? How essential, not just contributing to, but how essential are these authorities to stopping which terrorist attacks?

ALEXANDER: OK. For clarity over 50. And in 90 percent of those cases FAA 702 contributed, and in 50 percent I believe they were critical. We will send that to the committee.

HIMES: This is 702 you're talking about?

ALEXANDER: This is 702.

HIMES: OK.

ALEXANDER: Now, shifting to the business record FISA, and I'll do a Mutt and Jeff here, I'm not sure which one I am. There's just

over 10 that had a domestic. And the vast majority...

HIMES: 10 of the 50 were section...

ALEXANDER: Just over 10.

(CROSSTALK)

HIMES: And how many would you say were critical.

ALEXANDER: No. No, you're...

HIMES: I'm sorry.

ALEXANDER: ... let me finish.

HIMES: Did I get it wrong?

ALEXANDER: Yeah, you do. Over -- just slightly over 10, and I don't want to pin that number until the community verifies it, so just a little over 10 were a domestic -- had a domestic nexus. And so business records FISA could only apply to those? So, see the ones in other countries, it couldn't apply to because the data is not there and it doesn't come into the U.S. So if we now look at that, the vast majority of those had a contribution by business record FISA. So, I think we have to be careful that you don't try to take the whole world and say, oh well you only did those that were in the United States and only, you know some large majority of that.

I do think this, going back to 9/11, we didn't have the ability to connect the dots. This adds one more capability to help us do that. And from my perspective, what we're doing here with the civil liberties and privacy oversight, and bringing together, does help connect those dots. Go ahead, Sean?

HIMES: If I could just -- I -- I'm out of time, but I think this point is really important. If my constituents are representative of the broader American public, they're more concerned frankly with the Section 215 gathering of American data than they are with the foreign data. And so I really hope you'll elucidate for us specifically case by case how many stopped terrorist attacks were those programs, 215, essential to?

JOYCE: I would just add to General Alexander's comments.

And I -- and I think you asked an almost impossible question to say, how important each dot was.

What I can tell you is, post 9/11 I don't recognize the FBI I came into 26 years ago. Our mission is to stop terrorism, to prevent it. Not after the fact, to prevent it before it happens in the United States. And I can tell you every tool is essential and vital. And the tools as I outlined to you and their uses today have been valuable to stopping some of those plots. You ask, "How can you put the value on an American life?" And I can tell you, it's priceless.

HIMES: Thank you, Mr. Chairman.

ROGERS: (OFF-MIKE)

BACHMANN: Thank you, Mr. Chair, for holding this important hearing today.

I just have a series of short questions. My first one is, you had mentioned earlier in your testimony that data must be destroyed within five years of acquisition. I believe that's in section 215 phone records. Is that -- that's true, within five years?

INGLIS: That is true. It's destroyed when it reaches five years of age.

BACHMANN: And how long do the phone companies on their own maintain data?

INGLIS: That varies. They don't hold that data for the benefit of the government. They hold that for their own business internal processes. I don't know the specifics. I know that it is variable. I think that it ranges from six to 18 months and the data that they hold is, again, useful for their purposes, not necessarily the government's.

BACHMANN: So then my question is, did the FISA orders give the United States companies a choice in whether to participate in the NSA business records or in the PRISM programs? Were these -- was this voluntarily -- voluntary compliance on the part of these companies?

INGLIS: No, these are court orders that require their compliance with the terms of the court order.

BACHMANN: So let me just for the record state, is NSA spying today or have you spied on American citizens?

INGLIS: We -- we do not target U.S. persons anywhere in the world without a specific court warrant.

BACHMANN: And does the NSA listen to the phone calls of American citizens?

INGLIS: We do not target or listen to the telephone calls of U.S. persons under that targeting without a specific court warrant.

BACHMANN: Does the NSA read the e-mails of American citizens?

INGLIS: Same answer, ma'am.

BACHMANN: Does the NSA read the text messages of American citizens?

INGLIS: Again, we do not target the content of U.S.-person communications without a specific warrant anywhere on the earth.

BACHMANN: Has the NSA ever tracked any political enemies of the administration, whether it's a Republican administration or Democrat administration? Have either of the administrations -- you said you're

100 percent auditable, so you would know the answer to this question -- have you ever tracked the political enemies of an administration?

INGLIS: In my time at NSA, no, ma'am.

BACHMANN: Does the government keep the video data, like Mr. Himes had just questioned? Does the government have a database with video data in it, tracking movements of the American people?

INGLIS: No, ma'am.

(CROSSTALK)

BACHMANN: I'm sorry. That's not -- the microphone isn't on.

INGLIS: NSA does not hold such data.

ALEXANDER: Yeah, and we don't know of any data -- anybody that does. So I think those are held, as you see from Boston, by individual shop owners and (inaudible).

BACHMANN: But -- but does the federal government have a database with video data in it tracking the whereabouts of the American people?

JOYCE: The FBI does not have such a database, nor am I aware of one.

BACHMANN: Do we -- does the American government have a database that has the GPS location whereabouts of Americans, whether it's by our cell phones or by any other tracking device? Is there a known database?

INGLIS: NSA does not hold such a database.

BACHMANN: Does the NSA have a database that you maintain that holds the content of Americans' phone calls? Do you have recordings of all of our calls? So if we're making phone calls, is there a national database that has the content of our calls?

ALEXANDER: We're not allowed to do that, nor do we do that, unless we have a court order to do that. And it would be only in specific cases and almost always that would be an FBI lead, not ours.

BACHMANN: So do we maintain a database of all of the e-mails that have ever been sent by the American people?

ALEXANDER: No. No, we do not.

BACHMANN: Do we -- is there a database from our government that maintains a database of the text messages of all Americans?

ALEXANDER: No -- none that I know of, and none at NSA.

BACHMANN: And so I think what you have told this committee is that the problem is not with the NSA, that is trying to keep the American people safe. You've told us that you have 100 percent auditable system that has oversight both from the court and from

Congress.

It seems to me that the problem here is that of an individual who worked within the system, who broke laws, and who chose to declassify highly sensitive classified information. It seems to me that's where our focus should be, on how there could be a betrayal of trust and how a traitor could do something like this to the American people. It seems to me that's where our focus must be and how we can prevent something like that from ever happening again.

Let me ask your opinion: How damaging is this to the national security of the American people that this trust was violated?

ALEXANDER: I think it was irreversible and significant damage to this nation.

BACHMAN:: Has this helped America's enemies?

ALEXANDER: I believe it has. And I believe it will hurt us and our allies.

BACHMANN: I yield back, Mr. Chair.

ROONEY: Thank you, Mr. Chairman.

I want to thank the panel.

You know, one of the negatives about being so low on the totem pole up here is basically all the questions that I wanted to address have been asked.

And I think I'm really proud of this committee because on both sides of the aisle, a lot of the questions were very poignant. And I hope that the American people and those that are in the room have learned a lot about what happened here and learned a lot about the people on the panel.

I can say specifically, General Alexander, my time on the Intelligence Committee, I have more respect for you. And I'm glad that you're the one up there testifying so the American people can see despite what they're -- what's being portrayed and the suspicions that are out there, that there is nobody better to articulate what happened and what we're trying to do than yourself.

So I want to thank you for that.

We -- we -- I'll ask a couple basic questions that I think that might help clear some things up.

Mr. Cole, you talked about how the -- the Fourth Amendment isn't applicable under the business records exception and the Patriot Act Section 215, applicable case law, Maryland v. Smith, et cetera. And then we heard about how to -- to be able to look at the data under 215, there has to be very specific suspicion that is presented to a court, and that court is not a rubber stamp in allowing us to basically look at metadata which is strictly phone records.

One of, I think, problems that people have out there is that it was such a large number of phone numbers. And when you testify, when everybody testifies, that it's very specific and only a limited number of people are able to -- to basically articulate who we should be looking at and then you hear this number, millions, from Verizon, can you -- can you help clear that up?

COLE: Certainly. First of all we -- as we said, we don't give the reasonable suspicion to the court ahead of time. They set out the standards for us to use.

But the analogy, and I've heard it used several times is, if you're looking for a needle in the haystack, you have to get the haystack first. And that's why we have the ability under the court order to acquire -- and the key word here is acquire -- all of that data.

We don't get to use all of that data necessarily. That is the next step, which is you have to be able to determine that there is reasonable, articulable suspicion to actually use that data.

So if we want to find that there is a phone number that we believe is connected with terrorist organizations and terrorist activity, we need to have the rest of the haystack, all the other numbers, to find out which ones it was in contact with.

And, as you heard Mr. Inglis say, it's a very limited number of times that we make those queries because we do have standards that have to be met before we can even make use of that data. So while it sits there, it is used sparingly.

ROONEY: Did you or anybody that you know at the NSA break the law in trying to obtain this information?

COLE: I am aware of nobody who has broken the law at the NSA in obtaining the information in the lawful sense. There's other issues that we have with the leaks that have gone on here.

ROONEY: And maybe this question is for General Alexander: Based on everything that we've heard today, do you see any problems with either 702 or 215 that you think should be changed by this body?

ALEXANDER: Not right now. But this is something that we have agreed that we would look at, especially the structure of how we do it.

I think Congressman Schiff brought up some key points, and we are looking at all of those. And what we have to bring back to you is the agility, how we do it in the oversight, is there other ways that we can do this.

But at the end of the day, we need these tools and we just got to figure out the right way to do it or the next step from my perspective, having the court, this body of Congress and the administration do oversight.

I think if the American people were to step through it, they would agree that what we're doing is exactly the right way.

ALEXANDER: So those are the steps that we will absolutely they'll go back and -- and look at the entire architecture and that's a commitment that FBI and NSA has made to the administration and to this committee.

ROONEY: Final question, Mr. Joyce, what's next for Mr. Snowden we can expect?

JOYCE: Justice.

ROONEY: I yield back, Mr. Chairman. Thank you.

(CROSSTALK)

POMPEO: Great. Thank you, Mr. Chairman.

Thank you all for being here today. You know, this has been -- this has been a great hearing. I think the American people will have gotten a chance to hear from folks who are actually executing this program in an important way, and they'll have a choice whether to believe Mr. Inglis and General Alexander or a felon who fled to communist China.

For me, there's an easy answer to that.

There are those who talk about the war on terror winding down, they say we're toward the end of this, these programs were created post-9/11 to counter the terrorist threat, but for the soldiers fighting overseas and our allies and for us in the States.

General Alexander, Mr. Joyce, do you think these programs are just as much needed today as they were in the immediate aftermath of 9/11?

ALEXANDER: I do.

JOYCE: I do, too. And I would just add, I think the environment has become more challenging. And I think the more tools you have to be able to fight terrorism, the more we're gonna be able to protect the American people.

POMPEO: Thank you.

We've talked a lot about the statutory basis for Section 215 and Section 702. We've talked a lot on all the process that goes with them. And I want to spend just a minute talking about the constitutional boundaries and where they are.

We've got FISA court judges, Article 3. Mr. Litt, these are just plain old Article 3 judges, in the sense of life time tenure, nominated by a president, confirmed by the United States Senate. They have the same power, restrictions and authority as all Article 3 judges do. Is that correct?

LITT: Yes, that's correct.

POMPEO: We have Article 2 before us here today and we've got Article 1 oversight taking place this morning.

I want to talk about Article 1's involvement. There have been some members who talked about the fact that they didn't know about these programs. General Alexander or maybe Mr. Inglis, can you talk about the briefings that you've provided for members of Congress, both recently and as this set of laws was developed -- set of laws were developed?

INGLIS: So 702 was recently reauthorized at the end of 2012. In the runup to that, NSA in the companionship with the Department of Justice, FBI, the DNI, made a series of presentations across the Hill some number of times and talked in very specific details at the classified level about the setup of those programs, the controls on those programs and the success of those programs.

The reauthorization of Section 215 of the Patriot Act came earlier than that, but there was a similar set of briefings along those lines.

At the same time, we welcome and continue to welcome any and all Congress persons or senators to come to NSA or we can come to you and at the classified level brief any and all details, That's a standing offer. And some number have, in fact taken us up on that offer.

POMPEO: Do you have something to add, General?

ALEXANDER: That's exactly right. In fact, anyplace, anytime we can help, we will do it.

POMPEO: Good. I appreciate that. I've been on the committee only a short time. I learned about these programs actually before I came on the committee, so I know that members outside of this committee also had access to the information. And I think that's incredibly important.

As -- as committee oversight members, that's one thing, but I think it's important that all the members of Congress understand the scope of these programs. And I appreciate the fact that you've continued to offer that assistance for all of us.

A couple of just clean-up details, going last. I want to make sure I have this right.

General Alexander, from the data under Section 215 that's collected, can you -- can you figure out the location of the person who made a particular phone call?

ALEXANDER: Not beyond the area code.

POMPEO: Do you have any information about the signal strength or tower direction? I've seen articles that talk about you having this information. I want to...

(CROSSTALK)

ALEXANDER: No, we don't.

POMPEO: ... we've got that right.

ALEXANDER: We don't have that in the database.

POMPEO: And then, lastly, Mr. Litt, you made a reference to Section 702. You talked about it being a restriction on Article 230, not an expansion. That is, Article 2, the presidents of both parties believed they had the -- the powers that are being exercised under Section 702 long before that statutory authority was granted.

So is it the case that you view Section 702 as a control and a restriction on Article 2?

LITT: Yes.

POMPEO: Great.

Mr. Chairman, I yield back.

(OFF-MIKE)

KING: Thank you, Mr. Chairman. I'll make this brief.

I want to first of all thank all witnesses for their testimony, for their service, and for all you've done to strengthen and maintain this program.

My question, General Alexander, is -- is to you and also perhaps to Mr. Joyce,

Several times in your testimony you referenced 9/11 and how -- and I recall after September 11th there was a -- was a loud challenge to the intelligence community to do a better job of connecting the dots, be more aggressive, be -- you know, be more forward thinking, try to anticipate what's going to happen, think outside the box, all those cliches we heard at the time.

And as I see it, this is a very legitimate and legal response to that request.

I would ask you, General Alexander, or you, Mr. Joyce, I believe referenced the case, after September 11th where there was a phone interception from Yemen which enabled you to foil the New York Stock Exchange plot,

It's also my understanding that prior to 9/11, there was phone messages from Yemen which you did not have the capacity to follow through on which perhaps could have prevented the 9/11 attack.

Could either General Alexander or Mr. Joyce or both of you explain how the attack could have been prevented? Or if you believe it could have been prevented?

JOYCE: I don't know, Congressman, if the attack could have been prevented. What I can tell you is that is a tool that was not

available to us at the time of 9/11. So when there was actually a call made from a known terrorist in Yemen to Khalid Mihdhar in San Diego, we did not have that tool or capability to track that call.

Now, things may have been different, and we will never know that, unfortunately.

So that is the tool that we're talking about today that we did not have at the time of 9/11.

Moving forward, as you mentioned about the -- the stock exchange, here we have a similar thing except this was under, again, the 702 program, where NSA tipped to us that a known extremist in Yemen was talking or conversing with an individual inside the United States, we later identified as Khalid Ouazzani.

And then we were able to go up on our legal authorities here in the United States on Ouazzani, who was in Kansas City and were able to identify two additional co-conspirators.

We found through electronic surveillance they were actually in the initial stages of plotting to bomb the New York Stock Exchange.

So, as -- to really summarize, as I mentioned before, all of these tools are important.

And as Congressman Schiff mentioned, we should have this dialogue. We should all be looking for ways, as you said, thinking outside the box of how to do our business.

But I sit here before you today humbly and say that these tools have helped us.

KING: General?

ALEXANDER: If I could, I think on Mihdhar case, Mihdhar was the terrorist -- the A.Q. terrorist from the 9/11 plot in California that was actually on American Airlines Flight 77 that crashed into the Pentagon -- what -- what we don't know going back in time is the phone call between Yemen and there, if we would have had the reasonable, articulable suspicion standard, so we'd have to look at that.

But assuming that we did, if we had the database that we have now with the business records FISA and we searched on that Yemen number and saw it was talking to someone this California, we could have then tipped that to the FBI.

Another step, and this an assumption, but let me play this out because we will never be able to go all the way back and redo all the figures from 9/11, but this is why some of these programs were put in was to help that.

Ideally going from Mihdhar, we would have been able to find the other teams, the other three teams in the United States and/or one in Germany or some other place.

So the ability to use the metadata from the business record FISA

would have allowed us, we believe, to see some.

Now, so it's hypothetical. There are a lot of conditions that we can put -- that we could put on there. You'd have to have this right. You'd have to have the RAS right.

But we didn't have that ability. We couldn't connect the dots because we didn't have the dots.

And so, I think what we've got here is that one additional capability, one more tool to help us work together as a team to stop future attacks. And as -- as Sean has laid out, you know, when you look at this, you know, the New York City -- two and others, I think from my perspective, you know, those would have been significant events for our nation. And so, I think what we've jointly done with Congress is helped set this program up correctly.

KING: I'll just close, General, by saying in your opening statement you said that you'd rather be testifying here today on this issue rather than explaining why another 9/11 happened.

So I want to thank you for your service in preventing another 9/11 and there's the Zazi case. And I know some -- you're very close with your knowledge of that. And I want to thank all of you for the effort that was done to prevent that attack.

Mr. Chairman, I yield back.

ROGERS: Just a couple of clarifying things here to -- to wrap it up.

Mr. Joyce, you've been in the FBI for 26 years. You've conducted criminal investigations as well.

Sometimes you get a simple tip that leads to a broader investigation. Is that correct?

JOYCE: That is correct, Chairman.

ROGERS: And so, without that initial tip, you might not have found the other very weighty evidence that happened subsequent to that tip. Is that correct?

JOYCE: Absolutely.

ROGERS: So, in the case of -- of Malalin (ph) in 2007, the very fact that under the business 215 records, there was a simple tip that was, we have someone that is known with ties to Al Qaida's east African network calling a phone number in San Diego. That's really all you got, was a phone number in San Diego. Is that correct?

JOYCE: That is correct.

ROGERS: And -- and according to -- in the unclassified report that tip ultimately led to the FBI's opening of a full investigation that resulted in the February 2013 conviction. Is that correct?

JOYCE: Yes, it is, Chairman.

ROGERS: So without that first tip, you would have had -- you -- you weren't up on his electronics communications. You didn't really -- you were not -- he was not a subject of any investigation prior to that tip from the National Security Agency.

JOYCE: No, actually, he was the subject to a prior investigation...

ROGERS: That was closed.

JOYCE: ... several years earlier that was closed...

ROGERS: Right.

JOYCE: ... because we could not find any connection to terrorism.

ROGERS: Right.

JOYCE: And then, if we did not have the tip from NSA, we would not have been able to reopen...

ROGERS: Reopen the case. But at the time, you weren't investigating him?

JOYCE: Absolutely not. It was based on...
(CROSSTALK)

ROGERS: Right, and when they -- when they dipped that number into the -- to the business records, the preserved business records from the court order -- they dipped a phone number in, and a phone number came out in San Diego. Did you know who that person was when they gave you that phone number?

JOYCE: No, we did not. So we had to serve legal process to identify that subscriber and then corroborate it. And then we later went up on electronic surveillance with an order through the FISC.

ROGERS: And -- and when you went up on the electronic surveillance, you used a court order, a warrant...

JOYCE: That is correct.

ROGERS: ... a subpoena? What did you use?

JOYCE: We used a FISA court order.

ROGERS: All right. So you had to go back. You had to prove a standard of probable cause to go up on this individual's phone number. Is that correct?

JOYCE: That's right. And as been mentioned, hopefully several times today, anyone inside the United States, a U.S. person, whether they're inside or outside, we need a specific court order regarding

that person.

ROGERS: All right.

And Mr. Cole, I just -- just for purposes of explanation, if you were going to have a -- an FBI agent came to you for an order to preserve business records, do they need a court order? Do they need a warrant for that in a criminal investigation?

COLE: No, they do not. You can just get a grand jury's subpoena, and, separate from preserving it, you can acquire them with a grand jury subpoena. And you don't need to go to a court to do that.

ROGERS: Right, so that is a lower-legal standard in order to obtain information on a U.S. citizen on a criminal matter.

COLE: That's correct, Mr. Chairman.

ROGERS: So the -- when we -- and I think this is an important point to make. When we -- the system is set up on this foreign collection -- and I argue we need this high standard because it is in a classified -- or used to be in a classified setting -- you need to have this high standard. So can you describe the difference?

If I were going to do a criminal investigation -- getting the same amount of information the -- the legal standard would be much lower if I were working an embezzlement case in Chicago than trying to catch a counter-terrorist -- counter -- excuse me, a terrorist operating overseas trying to get back into the United States to conduct a plot.

COLE: Some of the standards might be similar, but the process that you have to go through is much greater in the FISA context. You actually have to go to a -- a court, the FISA court ahead of time and set out facts that will explain to the court why this information is relevant to the investigation that you're doing, why it's a limited type of investigation that is allowed to be done under the statute and under the rules. And then the court has to approve that ahead of time, along with all of the rules and restrictions about how you can use it, how you can access it, what you can do with it, and who you can disseminate it to.

There is a much different program that goes on in a normal grand jury -- situation. You have restrictions on who you can disseminate to under secrecy grounds, but even those are much broader than they would be under the FISA grounds.

ROGERS: Right.

COLE: And you don't need a court ahead of time.

ROGERS: So -- so, in total, this is a much more overseen -- and, by the way, on a criminal embezzlement case in Chicago, you wouldn't brief that to Congress, would you?

COLE: No, we would not, not as a normal course.

ROGERS: Yeah, and so you have a whole nother layer of legislative oversight on this particular program. And, again, I argue the necessity of that because it is a -- as I said, used to be a classified program of which you additional oversight. You want members of the legislature making sure we're (ph) on track that you don't necessarily need in a criminal matter domestically.

COLE: That's correct. In a normal criminal embezzlement case in Chicago, you would have the FBI and the Justice Department involved. And that's about it.

ROGERS: Right.

COLE: In this, you've got the National Security -- Agency. You've got the ODNI. You've got the inspectors general. You've got the Department of Justice. You have the court monitoring what you're doing, if there's any mistakes that were made. You have Congress being briefed on a regular basis. There is an enormous amount of oversight in this compared to a grand jury situation. Yet the records that can be obtained are of the same kind.

ROGERS: Right, thanks. And I just want a couple of clarifying questions.

Mr. Joyce, if you will, does China have an -- an adversarial intelligence service directed at the United States?

JOYCE: Yes, they do.

ROGERS: Do they perform economic espionage activities targeted at U.S. companies in the United States?

JOYCE: Yes, they do.

ROGERS: Do they conduct espionage activities toward military and intelligent services, both here and abroad, that belong to the United States of America?

JOYCE: Yes, they do.

ROGERS: Do they target policy makers and decision makers, Department of State and other -- other policy makers that might engage in foreign affairs when it comes to the United States?

JOYCE: Yes.

ROGERS: Would you -- how would you rate them as an adversarial intelligence service given the other intelligence services that we know are adversarial, the Russians, the Iranians, the others?

JOYCE: They are one of our top adversaries.

ROGERS: Yeah. And you have had a string of successes recently in prosecutions for Chinese espionage activities in the United States. Is that correct?

JOYCE: That is correct.

ROGERS: And so, that has been both economic, and, if I understand it, as well as the military efforts. So they've been very aggressive in their espionage activities toward the United States. Is it -- would you -- is that a fair assessment?

JOYCE: I think they have been very aggressive against United States interests.

ROGERS: General Alexander, do they -- how would you describe, in an unclassified way, the Chinese cyber efforts for both espionage and their military capability to conduct disruptive attacks toward the United States?

ALEXANDER: Very carefully.

(LAUGHTER)

With a lot of legal oversight. I -- I think one of the things that -- you know, it's public knowledge out there about the cyber activities that we're seeing. But I also think that what's missing, perhaps, in this conversation with the Chinese is what's -- what's acceptable practices here. And I think the president has started some of that in the discussions with the -- the new president of China.

And I think that's some of the stuff that we actually have to have. This need not be an adversarial relationship. I think our country does a lot of business with China, and we need to look at, how can we improve the relations with China in such a way that both our countries benefit? Because we can. And I think that's good for everybody.

What concerns me is now this program and what we're talking about with China, as got -- I think we've got to solve this issue with China and then look at ways to move -- to move forward. And I think we do have to have that discussion on cyber. What is -- what are the right standards, have that discussion both privately and publicly. And it's not just our country. It's all the countries of the world, as well as China.

ROGERS: All right, and I -- I appreciate you drawing the line, but would you say that China engages in economic -- cyber economic espionage against intellectual property to steal intellectual property in the United States?

ALEXANDER: Yes.

ROGERS: Would you argue that they engage in cyber activities to steal both military and intelligence secrets of the United States?

ALEXANDER: Yes.

ROGERS: I -- I just -- I think this is important that we put it in context for several things that I think Americans want to know about the relationship between Mr. Snowden and -- and where he finds home today, and that we know that we're doing a full investigation

into possible connections with any nation state who might take advantage of this activity.

And the one thing I disagree with Mr. Litt today, that they haven't seen anything of any changes. And I would dispute that based on information I've seen recently and would ask anyone to comment. Do you believe that Al Qaida elements have -- have just historically, when they've been -- when issues have been disclosed, changed the way they operate to target both soldiers abroad in their terrorist-plotting activities, movements, financing, weaponization, and training.

LITT: To -- to be clear, what I -- what I intended to say -- and if I wasn't clear, I apologize -- was we know that they've seen this. We know they've commented on it. What we don't know yet is over the long term what impact it's going to have on our collection capabilities. But you're absolutely right. We know they watch us. And they -- they -- they modify their behavior based on what they learn.

ROGERS: And -- and we also know that in some cases in certain countries they have modified their behavior, including the way they target U.S. troops based on certain understandings of communications. Is that correct?

LITT: I think that's -- that's correct.

ROGERS: I'll guarantee it's absolutely correct. And that's what's so concerning about this.

I do appreciate your being here. I know how difficult it is to come and talk.

General, did you want to say something before...

(CROSSTALK)

ALEXANDER: Yeah, I -- I wanted to say, if I could, just a couple things, because they didn't come up in -- in this testimony. But, first, thanks to this committee, the administration and others, in the summer of 2009 we set up the director -- Directorate of Compliance. Put some of our best people in it to ensure that what we're doing is exactly right. And this committee was instrumental in helping us set that up. So that's one point.

When we talk about oversight and compliance, people think it's just once in a while, but there was rigorous actions by you and this entire committee to set that up.

The second is, in the open press there's this discussion about pattern analysis -- they're out there doing pattern analysis on this. That is absolutely incorrect. We are not authorized to go into the data, nor are we data mining or doing anything with the data other than those queries that we discuss, period. We're not authorized to do it. We aren't doing it. There are no automated processes running in the background pulling together data trying to figure out networks.

The only time you can do pattern analysis is, once you start the query on that query and where you go forward. You can't go in and try to bring up -- you know, I have four daughters and 15 grandchildren. I can't supervise them with this database. It is not authorized, and our folks do not do it.

And so that's some of the oversight and compliance you and the rest of the Oversight Committee see, but I think it's important for the American people to know that it's limited. In this case, for 2012, less than 300 selectors were looked at, and they had an impact in helping us prevent potential terrorist attacks, they contributed. And I think when you look at that and you -- you balance those two, that's pretty good.

ROGERS: And I do appreciate it. And I want to commend -- the folks from the NSA have always -- we've never had to issue a subpoena. All that information has always -- readily provided. You meet with us regularly. We have staff and investigators at the NSA frequently. We have an open dialogue when problems happen; we do deal with them in a classified way, in -- in a way I think that Americans would be proud that their elected representatives deal with issues.

And I'm not saying that there are some hidden issues out there; there are not.

I know this has been difficult to come and talk about very sensitive things in a public way. In order to preserve your good work and the work on behalf of all the patriots working to defend America, I still believe it was important to have a meeting where we could at least, in some way, discuss and reassure the level of oversight and redundancy of oversight on a program that we all recognize needed an extra care and attention and lots of sets of eyes. I hope today in this hearing that we've been able to do that.

I do believe that America has the responsibility to keep some things secret as we serve to protect this country. And I think you all do that well. And the darndest thing is that we may have found that it is easier for a systems analyst -- or a systems administrator to steal the information than it is for us to access the program in order to prevent a terrorist attack in the United States. And we'll be working more on those issues.

And we have had great dialogue about what's coming on some other oversight issues.

Again, thank you very, very much. Thank you all for your service. And I wish you all well today.

END