

1 STUART F. DELERY
 Assistant Attorney General
 2 JOSEPH H. HUNT
 Director, Federal Programs Branch
 3 ANTHONY J. COPPOLINO
 Deputy Branch Director
 4 JAMES J. GILLIGAN
 Special Litigation Counsel
 5 MARCIA BERMAN
 Senior Trial Counsel
 6 marcia.berman@usdoj.gov
 BRYAN DEARINGER
 7 Trial Attorney
 RODNEY PATTON
 8 Trial Attorney
 U.S. Department of Justice, Civil Division
 9 20 Massachusetts Avenue, NW, Rm. 7132
 Washington, D.C. 20001
 10 Phone: (202) 514-2205; Fax: (202) 616-8470

11 *Attorneys for the Government Defs. in their Official Capacity*

12 **UNITED STATES DISTRICT COURT**
 13 **NORTHERN DISTRICT OF CALIFORNIA**
SAN FRANCISCO DIVISION

14	FIRST UNITARIAN CHURCH OF LOS)
15	ANGELES, <i>et al.</i> ,)
16	Plaintiffs,)
17	v.)
18	NATIONAL SECURITY AGENCY, <i>et al.</i> ,)
19	Defendants.)

Case No. 3:13-cv-03287-JSW

DECLARATION OF JAMES J. GILLIGAN IN SUPPORT OF GOVERNMENT DEFENDANTS' MOTION TO DISMISS AND OPPOSITION TO PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT

21 I, James J. Gilligan, hereby declare:

22 1. I am the Special Litigation Counsel for the United States Department of Justice, Civil
 23 Division, Federal Programs Branch, and attorney of record for the official capacity Government
 24 Defendants in the above-captioned cases. The statements made herein are based on my personal
 25 knowledge, and on information made available to me in the course of my duties and
 26 responsibilities as counsel for the official capacity Government Defendants in these cases.

1 2. Filed with this declaration, as Exhibits A through P in support of the “Government
2 Defendants’ Motion to Dismiss and Opposition to Plaintiffs’ Motion for Partial Summary
3 Judgment,” are true and correct copies of the following documents:

- 4 a. Exhibit A, Declaration of Teresa H. Shea, Signals Intelligence Director, National
5 Security Agency, dated Dec. 5, 2013;
- 6 b. Exhibit B, Declaration of Joshua Skule, Acting Assistant Director,
7 Counterterrorism Division, Federal Bureau of Investigation, dated Dec. 5, 2013;
- 8 c. Exhibit C, Amended Memorandum Opinion, *In re Application of the FBI for an*
9 *Order Requiring the Production of Tangible Things from [Redacted]*, Dkt. No.
10 BR13-109, Foreign Intelligence Surveillance Court, dated Aug. 29, 2013;
- 11 d. Exhibit D, Memorandum Opinion, *In re Application of the FBI for an Order*
12 *Requiring the Production of Tangible Things from [Redacted]*, Dkt. No. BR 13-
13 158, Foreign Intelligence Surveillance Court, dated Oct. 11, 2013;
- 14 e. Exhibit E, Primary Order, *In re Application of the FBI for an Order Requiring the*
15 *Production of Tangible Things From [Redacted]*, Dkt. No. BR 13-80, Foreign
16 Intelligence Surveillance Court, dated Apr. 25, 2013 (“Primary Order”);
- 17 f. Exhibit F, Secondary Order, *In re Application of the FBI for an Order Requiring*
18 *the Production of Tangible Things [etc.]*, Dkt. No. BR13-80, Foreign Intelligence
19 Surveillance Court, dated Apr. 25, 2013 (“Secondary Order”);
- 20 g. Exhibit G, Letter from Ronald Weich to Rep. Silvestre Reyes, dated Dec. 14,
21 2009;
- 22 h. Exhibit H, Report on the National Security Agency’s Bulk Collection Programs
23 for USA PATRIOT Act Reauthorization;
- 24 i. Exhibit I, Letter from Sens. Diane Feinstein and Kit Bond to Colleagues, dated
25 Feb. 23, 2010;
- 26 j. Exhibit J, Letter from Rep. Silvestre Reyes to Colleagues, dated Feb. 24, 2010;
- 27 k. Exhibit K, Letter from Ronald Weich to Sens. Diane Feinstein and Saxby
28 Chambliss, dated Feb. 2, 2011;

- 1 l. Exhibit L, Letter from Ronald Weich to Reps. Mike Rogers and C.A. Dutch
2 Ruppertsberger, dated Feb. 2, 2011;
- 3 m. Exhibit M, Report on the National Security Agency's Bulk Collection Programs
4 for USA PATRIOT Act Reauthorization, dated Feb. 2, 2011;
- 5 n. Exhibit N, Letter from Sens. Feinstein and Chambliss to Colleagues, dated Feb. 8,
6 2011;
- 7 o. Exhibit O, Press Release of Senate Select Committee on Intelligence, dated June
8 6, 2013;
- 9 p. Exhibit P, *How Disclosed NSA Programs Protect Americans, and Why Disclosure*
10 *Aids Our Adversaries: Hearing Before the House Perm. Select Comm. on*
11 *Intelligence*, 113th Cong., 1st Sess. (2013) (statements of Reps. Rogers,
12 Langevin, and Pompeo), dated June 18, 2013; and
- 13 q. Exhibit Q, *[Redacted]*, Dkt. No. PR/TT [redacted], Opinion and Order, Foreign
14 Intelligence Surveillance Court, dated [redacted], declassified and released on
15 Nov. 18, 2013;
- 16 r. Exhibit R, *In re Prod. of Tangible Things from [Redacted]*, Dkt. No. BR 08-13,
17 Supplemental Opinion, Foreign Intelligence Surveillance Court, dated Dec. 12,
18 2008.

19
20 I declare under penalty of perjury under the laws of the United States of America that the
21 foregoing is true and correct. Executed on December 6, 2013, at Washington, D.C.

22
23 /s/ James J. Gilligan
24 JAMES J. GILLIGAN
25 Special Litigation Counsel
26 james.gilligan@usdoj.gov
27 U.S Department of Justice
28 Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470

EXHIBIT A

1 STUART F. DELERY
 2 Assistant Attorney General
 3 JOSEPH H. HUNT
 4 Director, Federal Programs Branch
 5 ANTHONY J. COPPOLINO
 6 Deputy Branch Director
 7 tony.coppolino@usdoj.gov
 8 JAMES J. GILLIGAN
 9 Special Litigation Counsel
 10 james.gilligan@usdoj.gov
 11 MARCIA BERMAN
 12 Senior Trial Counsel
 13 marcia.berman@usdoj.gov
 14 BRYAN DEARINGER
 15 Trial Attorney
 16 bryan.dearinger@usdoj.gov
 17 RODNEY PATTON
 18 Trial Attorney
 19 rodney.patton@usdoj.gov
 20 U.S. Department of Justice, Civil Division
 21 20 Massachusetts Avenue, NW, Rm. 7132
 22 Washington, D.C. 20001
 23 Phone: (202) 514-2205; Fax: (202) 616-8471

24
25 *Attorneys for the Government Defs. in their Official Capacity*

26
27 **IN THE UNITED STATES DISTRICT COURT**
 28 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
 29 **SAN FRANCISCO DIVISION**
 30

31
32 _____)
 33 FIRST UNITARIAN CHURCH OF)
 34 LOS ANGELES, *et al.*,)
 35)
 36 Plaintiffs,)
 37)
 38 v.)
 39)
 40 NATIONAL SECURITY AGENCY, *et al.*,)
 41)
 42 Defendants.)
 43 _____)

Case No. 3:13-cv-03287 JSW

DECLARATION OF TERESA H. SHEA, SIGNALS INTELLIGENCE DIRECTOR, NATIONAL SECURITY AGENCY

1 I, Teresa H. Shea, do hereby state and declare as follows:
2
3

4 (U) Introduction and Summary
5

6 1. I am the Director of the Signals Intelligence Directorate (SID) at the National Security
7 Agency (NSA), an intelligence agency within the Department of Defense (DoD). I am
8 responsible for, among other things, protecting NSA Signals Intelligence activities, sources, and
9 methods against unauthorized disclosures. Under Executive Order No. 12333, 46 Fed. Reg.
10 59941 (1981), as amended on January 23, 2003, 68 Fed. Reg. 4075 (2003), and August 27, 2004,
11 69 Fed. Reg. 53593 (2004), and August 4, 2008, 73 Fed. Reg. 45325, the NSA is responsible for
12 the collection, processing, and dissemination of Signals Intelligence (SIGINT) information for
13 the foreign intelligence purposes of the U.S. I have been designated an original TOP SECRET
14 classification authority under Executive Order (E.O.) 13526, 75 Fed. Reg. 707 (Jan. 5, 2010),
15 and Department of Defense Directive No. 5200.1-R, Information Security Program Regulation,
16 32 C.F.R. 159a.12 (2000).

17 2. My statements herein are based upon my personal knowledge of SIGINT collection
18 and NSA operations, the information available to me in my capacity as SID Director, and the
19 advice of counsel.

20 3. The NSA was established by Presidential Directive in 1952 as a separately organized
21 agency within the DOD under the direction, authority, and control of the Secretary of Defense.
22 The NSA's foreign intelligence mission includes the responsibility to collect, process, analyze,
23 produce, and disseminate SIGINT information for (a) national foreign intelligence purposes, (b)
24 counterintelligence purposes, and (c) to support national and departmental missions. See E.O.
25 12333, section 1.7(c), as amended.

1 this effort. It is imperative that we have the capability to rapidly detect any terrorist threat inside
2 the U.S.

3 7. One method that the NSA has developed to accomplish this task is analysis of
4 metadata associated with telephone calls within, to, or from the U.S. The term “telephony
5 metadata” or “metadata” as used here refers to data collected under the program that are about
6 telephone calls—such as the initiating and receiving telephone numbers, and the time and
7 duration of the calls—but does not include the substantive content of those calls or any
8 subscriber identifying information.

9 8. By analyzing telephony metadata based on telephone numbers associated with
10 terrorist activity, trained expert intelligence analysts can work to determine whether known or
11 suspected terrorists have been in contact with individuals in the U.S.

12 9. Foreign terrorist organizations use the international telephone system to communicate
13 with one another between numerous countries all over the world, including calls to and from the
14 U.S. When they are located inside the U.S., terrorist operatives also make domestic U.S.
15 telephone calls. The most analytically significant terrorist-related communications are those
16 with one end in the U.S., or those that are purely domestic, because those communications are
17 particularly likely to identify suspects in the U.S. whose activities may include planning attacks
18 against the homeland.

19 10. The telephony metadata collection program was specifically developed to assist the
20 U.S. Government in detecting such communications between known or suspected terrorists who
21 are operating outside of the U.S. and who are communicating with others inside the U.S., as well
22 as communications between operatives who are located within the U.S.

1 11. Detecting and linking these types of communications was identified as a critical
2 intelligence gap in the aftermath of the September 11, 2001 attacks. One striking example of this
3 gap is that, prior to those attacks, the NSA intercepted and transcribed seven calls made by
4 hijacker Khalid al-Mihdhar, then living in San Diego, California, to a telephone identifier
5 associated with an al Qaeda safe house in Yemen. The NSA intercepted these calls using
6 overseas signals intelligence capabilities, but those capabilities did not capture the calling party's
7 telephone number identifier. Because they lacked the U.S. telephone identifier, NSA analysis
8 mistakenly concluded that al-Mihdhar was overseas and not in California. Telephony metadata
9 of the type acquired under this program, however, would have included the missing information
10 and might have permitted NSA intelligence analysts to tip FBI to the fact that al-Mihdhar was
11 calling the Yemeni safe house from a U.S. telephone identifier.

12 12. The utility of analyzing telephony metadata as an intelligence tool has long been
13 recognized. As discussed below, experience also shows that telephony metadata analysis in fact
14 produces information pertinent to FBI counterterrorism investigations, and can contribute to the
15 prevention of terrorist attacks.

16 13. Beginning in May 2006 and continuing to this day, pursuant to orders obtained from
17 the Foreign Intelligence Surveillance Court ("FISC"), under the "business records" provision of
18 the Foreign Intelligence Surveillance Act ("FISA"), enacted by Section 215 of the USA
19 PATRIOT Act, codified at 50 U.S.C. § 1861 (Section 215), NSA has collected and analyzed bulk
20 telephony metadata from telecommunications service providers to close the intelligence gap that
21 allowed al-Mihdhar to operate undetected within the U.S. while communicating with a known
22 terrorist overseas.

1 14. Pursuant to Section 215, the FBI obtains orders from the FISC directing certain
2 telecommunications service providers to produce all business records created by them (known as
3 call detail records) that contain information about communications between telephone numbers,
4 generally relating to telephone calls made between the U.S. and a foreign country and calls made
5 entirely within the U.S. By their terms, those orders must be renewed approximately every 90
6 days. Redacted, declassified versions of a recent FISC “Primary Order” and “Secondary Order,”
7 directing certain telecommunications service providers to produce telephony metadata records to
8 NSA, and imposing strict conditions on the Government’s access to and use and dissemination of
9 the data, are attached, respectively, as Exhibits A and B hereto. At least 15 different FISC judges
10 have entered a total of 35 orders authorizing NSA’s bulk collection of telephony metadata under
11 Section 215, most recently on October 11, 2013.

12 15. Under the terms of the FISC’s orders, the information the Government is authorized
13 to collect includes, as to each call, the telephone numbers that placed and received the call, other
14 session-identifying information (e.g., International Mobile Subscriber Identity (IMSI) number,
15 International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone
16 calling card number, and the date, time, and duration of a call. The FISC’s orders authorizing
17 the collection do not allow the Government to collect the content of any telephone call, nor the
18 names, addresses, or financial information of parties to any call. The metadata collected by the
19 Government pursuant to these orders also does not include cell site locational information.

20 16. The NSA, in turn, stores and analyzes this information under carefully controlled
21 circumstances, and refers to the FBI information about communications (e.g., telephone
22 numbers, dates of calls, etc.) that the NSA concludes have counterterrorism value, typically

1 information about communications between known or suspected terrorist operatives and persons
2 located within the U.S.

3 17. Under the FISC's orders, the Government is prohibited from accessing the metadata
4 for any purpose other than obtaining counterterrorism information relating to telephone numbers
5 (or other identifiers) that are reasonably suspected of being associated with specific foreign
6 terrorist organizations or rendering the metadata useable to query for such counterterrorism
7 related information.

8 18. Pursuant to Section 215 and the FISC's orders, the NSA does not itself in the first
9 instance record any metadata concerning anyone's telephone calls. Nor is any non-governmental
10 party required by Section 215, the FISC or the NSA to create or record the information that the
11 NSA obtains pursuant to Section 215 and FISC orders. Rather, pursuant to the FISC's orders,
12 telecommunications service providers turn over to the NSA business records that the companies
13 already generate and maintain for their own pre-existing business purposes (such as billing and
14 fraud prevention).

15 **QUERY AND ANALYSIS OF METADATA**

16 19. Under the FISC's orders authorizing the NSA's bulk collection of telephony
17 metadata, the NSA may access the data for purposes of obtaining counterterrorism information
18 only through queries (term searches) using metadata "identifiers," e.g., telephone numbers, that
19 are associated with a foreign terrorist organization.

20 20. Specifically, under the terms of the FISC's Primary Order, before an identifier may
21 be used to query the database there must be a "reasonable articulable suspicion" (RAS), based on
22 the factual and practical considerations of everyday life on which reasonable and prudent persons
23 act, that the identifier is associated with one of the identified international terrorist organizations

1 that are subjects of FBI counterterrorism investigations. The RAS requirement ensures an
2 ordered and controlled querying of the collected data; it is also designed to prevent any general
3 browsing of data. Further, when the identifier is reasonably believed to be used by a U.S. person,
4 the suspicion of association with a foreign terrorist organization cannot be based solely on
5 activities protected by the First Amendment. An identifier used to commence a query of the data
6 is referred to as a “seed.”

7 21. Information responsive to an authorized query could include telephone numbers that
8 have been in contact with the terrorist-associated number used to query the data, plus the dates,
9 times, and durations of the calls. Query results do not include the identities of the individuals
10 associated with the responsive telephone numbers, because that is subscriber information that is
11 not included in the telephony metadata.

12 22. Under the FISC’s orders, the NSA may also obtain information concerning second
13 and third-tier contacts of the identifier, also known as “hops.” The first “hop” refers to the set of
14 identifiers directly in contact with the seed identifier. The second “hop” refers to the set of
15 identifiers found to be in direct contact with the first “hop” identifiers, and the third “hop” refers
16 to the set of identifiers found to be in direct contact with the second “hop” identifiers.

17 23. Although bulk metadata are consolidated and preserved by the NSA pursuant to
18 Section 215, the vast majority of that information is never seen by any person. Only the tiny
19 fraction of the telephony metadata records that are responsive to queries authorized under the
20 RAS standard are extracted, reviewed, or disseminated by NSA intelligence analysts, and only
21 under carefully controlled circumstances.

22 24. For example, although the number of unique identifiers has varied over the years, in
23 2012, fewer than 300 met the RAS standard and were used as seeds to query the data after

1 meeting the standard. Because the same seed identifier can be queried more than once over time,
2 can generate multiple responsive records, and can be used to obtain contact numbers up to three
3 “hops” from the seed identifier, the number of metadata records responsive to such queries is
4 substantially larger than 300, but it is still a very small percentage of the total volume of
5 metadata records.

6 25. There is no typical number of records responsive to a query of the metadata—the
7 number varies widely depending on how many separate telephone numbers (or other identifiers)
8 the “seed” identifier has been in direct contact with, how many separate identifiers those in the
9 first-tier contact, and so forth.

10 26. The NSA does not disseminate metadata information that it has not determined to be
11 of counterterrorism value, regardless of whether it was obtained at the first, second, or third hop
12 from a seed identifier. Rather, NSA intelligence analysts work to ascertain which of the results
13 are likely to contain foreign intelligence information, related to counterterrorism, that would be of
14 investigative value to the FBI (or other intelligence agencies). For example, analysts may rely
15 on SIGINT or other intelligence information available to them, or chain contacts within the
16 query results themselves, to inform their judgment as to what information should be passed to the
17 FBI as leads or “tips” for further investigation. As a result, during the three-year period
18 extending from May 2006 (when the FISC first authorized NSA’s telephony metadata program
19 under Section 215) through May 2009, NSA provided to the FBI and/or other intelligence
20 agencies a total of 277 reports containing approximately 2,900 telephone identifiers that the NSA
21 had identified.

22 27. It is not accurate, therefore, to suggest that the NSA can or does “track” or “search”
23 all Americans’ calls or that it engages in “surveillance,” under Section 215. Rather, by the terms

1 of the FISC's orders, the NSA can only access metadata information within, at most, three
2 "hops" of an approved seed identifier that is reasonably suspected of being associated with a
3 foreign terrorist organization specified in the FISC's orders.

4 28. Even when the NSA conducts authorized queries of the database, it does not use the
5 results to provide the FBI, or any other agency, with complete profiles on suspected terrorists or
6 comprehensive records of their associations. Rather, the NSA applies the tools of SIGINT
7 analysis to focus only on those identifiers which, based on the NSA's experience and judgment,
8 and other intelligence available to it, may be of use to the FBI in detecting persons in the U.S.
9 who may be associated with a specified foreign terrorist organization and acting in furtherance of
10 their goals. Indeed, under the FISC's orders, the NSA is prohibited from disseminating any
11 U.S.-person information derived from the metadata unless one of a very limited number of senior
12 NSA officials determines that the information is in fact related to counterterrorism information,
13 and is necessary to understand the counterterrorism information or assess its importance. The
14 NSA disseminates no information derived from the metadata about persons whose identifiers
15 have not been authorized as query terms under the RAS standard, or whose metadata are not
16 responsive to other queries authorized under that standard.

17 **MINIMIZATION PROCEDURES AND OVERSIGHT**

18 29. The NSA's access to, review, and dissemination of telephony metadata collected
19 under Section 215 is subject to rigorous procedural, technical, and legal controls, and receives
20 intensive oversight from numerous sources, including frequent internal NSA audits, Justice
21 Department and Office of the Director of National Intelligence (ODNI) oversight, and reports to
22 the FISC and to the Congressional intelligence committees.

1 30. In accordance with the requirements of Section 215, “minimization procedures” are
2 in place to guard against inappropriate or unauthorized dissemination of information relating to
3 U.S. persons. First among these procedures is the requirement that the NSA store and process
4 the metadata in repositories within secure networks, and that access to the metadata be permitted
5 only for purposes allowed under the FISC’s order, specifically database management and
6 authorized queries for counterterrorism purposes under the RAS standard. In addition, the
7 metadata must be destroyed no later than five years after their initial collection.

8 31. Second, under the FISC’s orders no one other than twenty-two designated officials in
9 the NSA’s Homeland Security Analysis Center and the Signals Intelligence Directorate can make
10 findings of RAS that a proposed seed identifier is associated with a specified foreign terrorist
11 organization. For identifiers believed to be associated with U.S. persons, the NSA’s Office of
12 General Counsel must also determine that a finding of RAS is not based solely on activities
13 protected by the First Amendment. And, as noted above, the minimization requirements also
14 limit the results of approved queries to metadata within three hops of the seed identifier.

15 32. Third, while the results of authorized queries of the metadata may be shared, without
16 minimization, among trained NSA personnel for analysis purposes, no results may be
17 disseminated outside of the NSA except in accordance with the minimization and dissemination
18 requirements and established NSA procedures. Moreover, prior to dissemination of any U.S.
19 person information outside of the NSA, one of a very limited number of NSA officials must
20 determine that the information is in fact related to counterterrorism information, and is necessary
21 to understand the counterterrorism information or assess its importance.

22 33. Fourth, in accordance with the FISC’s orders, the NSA has imposed stringent and
23 mutually reinforcing technological and personnel training measures to ensure that queries will be

1 made only as to identifiers about which RAS has been established. These include requirements
2 that intelligence analysts receive comprehensive training on the minimization procedures
3 applicable to the use, handling, and dissemination of the metadata, and technical controls that
4 prevent NSA intelligence analysts from seeing any metadata unless as the result of a query using
5 an approved identifier.

6 34. Fifth, the telephony metadata collection program is subject to an extensive regime of
7 oversight and internal checks and is monitored by the Department of Justice (DOJ), the FISC,
8 and Congress, as well as the Intelligence Community. Among these additional safeguards and
9 requirements are audits and reviews of various aspects of the program, including RAS findings,
10 by several entities within the Executive Branch, including the NSA's legal and oversight offices
11 and the Office of the Inspector General, as well as attorneys from DOJ's National Security
12 Division and the Office of the Director of National Intelligence.

13 35. Finally, in addition to internal oversight, any compliance matters in the program
14 identified by the NSA, DOJ, or ODNI are reported to the FISC. Applications for 90-day renewals
15 must report information on how the NSA's authority to collect, store, query, review and
16 disseminate telephony metadata was implemented under the prior authorization. Significant
17 compliance incidents are also reported to the Intelligence and Judiciary Committees of both
18 houses of Congress.

19 **COMPLIANCE INCIDENTS**

20 36. Since the telephony metadata collection program under Section 215 was initiated,
21 there have been a number of significant compliance and implementation issues (described below)
22 that were discovered as a result of internal NSA oversight and of DOJ and ODNI reviews. Upon

1 discovery, these violations were reported by the Government to the FISC and Congress, the NSA
2 remedied the problems, and the FISC reauthorized the program.

3 37. For example, beginning in mid-January 2009, the Government notified the FISC that
4 the NSA employed an "alert list" consisting of counterterrorism telephony identifiers to provide
5 automated notification to signals intelligence analysts if one of their assigned foreign
6 counterterrorism targets was in contact with a telephone identifier in the U.S., or if one of their
7 targets associated with foreign counterterrorism was in contact with a foreign telephone
8 identifier. The NSA's process compared the telephony identifiers on the alert list against
9 incoming Section 215 telephony metadata as well as against telephony metadata that the NSA
10 acquired pursuant to its Executive Order 12333 SIGINT authorities. Reports filed with the FISC
11 incorrectly stated that the NSA had determined that each of the telephone identifiers it placed on
12 the alert list were supported by facts giving rise to RAS that the telephone identifier was
13 associated with a foreign terrorist organization as required by the FISC's orders, i.e., was RAS
14 approved. In fact, however, the majority of telephone identifiers included on the alert list had
15 not gone through the process of becoming RAS approved, even though the identifiers were
16 suspected of being associated with a foreign terrorist organization. The NSA shut down the
17 automated alert list process and corrected the problem.

18 38. Following this notification, the Director of the NSA ordered an end-to-end system
19 engineering and process review of its handling of the Section 215 metadata. On March 2, 2009,
20 the FISC ordered the NSA to seek FISC approval to query the Section 215 metadata on a case-
21 by-case basis, except where necessary to protect against an imminent threat to human life. The
22 FISC further ordered the NSA to file a report with the FISC following the completion of the end-
23 to-end review discussing the results of the review and any remedial measures taken. The report

1 filed by the NSA discussed all of the compliance incidents, some of which involved queries of
2 the Section 215 metadata using non-RAS approved telephone identifiers, and how they had been
3 remedied. The compliance incidents, while serious, generally involved human error or complex
4 technology issues related to the NSA's compliance with particular aspects of the FISC's orders.
5 Subsequently, the FISC required a full description of any incidents of dissemination outside of
6 the NSA of U.S. person information in violation of court orders, an explanation of the extent to
7 which the NSA had acquired foreign-to-foreign communications metadata pursuant to the court's
8 orders and whether the NSA had complied with the terms of court orders in connection with any
9 such acquisitions, and certification as to the status of several types of data to the extent those data
10 were collected without authorization.

11 39. The U.S. Government completed these required reviews and reported to the FISC in
12 August 2009. In September 2009, the FISC entered an order permitting the NSA to once again
13 assess RAS without seeking pre-approval from the FISC subject to the minimization and other
14 requirements that remain in place today.

15 40. In fact, in an August 2013 Amended Memorandum Decision discussing the Court's
16 reasons for renewing the continued operation of the Section 215 telephony metadata program for
17 a 90-day period, the FISC stated, "The Court is aware that in prior years there have been
18 incidents of non-compliance with respect to the NSA's handling of produced information.
19 Through oversight by this Court over a period of months, those issues were resolved." *In re*
20 *Application of the Federal Bureau of Investigation for an Order Requiring the Production of*
21 *Tangible Things From [Redacted]*, Case No. BR 13-109, Amended Memorandum Opinion at 5
22 n.8 (FISC, released in redacted form September 17, 2013; *available at*

1 <http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf> (last visited December
2 2, 2013).

3 41. These incidents, including the FISC's related opinions, were also reported to
4 Congress in 2009.

5 42. Having received these reports and having been informed that the Government
6 interpreted Section 215 to authorize the bulk collection of telephony metadata, Congress has
7 twice reauthorized Section 215, without relevant modification, in 2010 and again in 2011.

8 43. In sum, the factors giving rise to compliance incidents discussed in this section have
9 been remedied. Moreover, even the most serious incidents, in which non-RAS approved
10 selectors were used to query the database, would not have allowed the NSA to establish the
11 "database of the associations of plaintiffs and their members" about which plaintiffs speculate.
12 That type of analysis is simply not possible from the raw telephony metadata that is collected
13 under the program, as it does not identify who is calling whom and for what purpose.

14 **BENEFITS OF METADATA COLLECTION**

15 44. Among other benefits, the bulk collection of telephony metadata under Section 215
16 has an important value to NSA intelligence analysts tasked with identifying potential terrorist
17 threats to the U.S. homeland, in support of FBI, by enhancing their ability to detect, prioritize,
18 and track terrorist operatives and their support networks both in the U.S. and abroad. By
19 applying the FISC-ordered RAS standard to telephone identifiers used to query the metadata,
20 NSA intelligence analysts are able to: (i) detect domestic identifiers calling foreign identifiers
21 associated with one of the foreign terrorist organizations and discover identifiers that the foreign
22 identifiers are in contact with; (ii) detect foreign identifiers associated with a foreign terrorist
23 organization calling into the U.S. and discover which domestic identifiers are in contact with the

1 foreign identifiers; and (iii) detect possible terrorist-related communications occurring between
2 communicants located inside the U.S.

3 45. Although the NSA possesses a number of sources of information that can each be
4 used to provide separate and independent indications of potential terrorist activity against the
5 U.S. and its interests abroad, the best analysis occurs when NSA intelligence analysts can
6 consider the information obtained from each of those sources together to compile and
7 disseminate to the FBI as complete a picture as possible of a potential terrorist threat. While
8 telephony metadata is not the sole source of information available to NSA counterterrorism
9 personnel, it provides a component of the information NSA intelligence analysts rely upon to
10 execute this threat identification and characterization role.

11 46. An advantage of bulk metadata analysis as applied to telephony metadata, which are
12 interconnected in nature, is that it enables the Government to quickly analyze past connections
13 and chains of communication. Unless the data is aggregated, it may not be feasible to detect
14 chains of communications that cross communication networks. The ability to query accumulated
15 telephony metadata significantly increases the NSA's ability to rapidly detect persons affiliated
16 with the identified foreign terrorist organizations who might otherwise go undetected.

17 47. Specifically, when the NSA performs a contact-chaining query on a terrorist
18 associated telephone identifier, it is able to detect not only the further contacts made by that first
19 tier of contacts, but the additional tiers of contacts, out to a maximum of three "hops" from the
20 original identifier, as authorized by the applicable FISC order. The collected metadata thus holds
21 contact information that can be immediately accessed as new terrorist-associated telephone
22 identifiers are identified. Multi-tiered contact chaining identifies not only the terrorist's direct

1 associates but also indirect associates, and, therefore provides a more complete picture of those
2 who associate with terrorists and/or are engaged in terrorist activities.

3 48. Another advantage of the metadata collected in this matter is that it is historical in
4 nature, reflecting contact activity from the past. Given that terrorist operatives often lie dormant
5 for extended periods of time, historical connections are critical to understanding a newly
6 identified target, and metadata may contain links that are unique, pointing to potential targets that
7 may otherwise be missed.

8 49. Bulk metadata analysis under Section 215 thus enriches NSA intelligence analysts'
9 understanding of the communications tradecraft of terrorist operatives who may be preparing to
10 conduct attacks against the U.S. This analysis can be important considering that terrorist
11 operatives often take affirmative and intentional steps to disguise and obscure their
12 communications.

13 50. Furthermore, the Section 215 metadata program complements information that the
14 NSA collects via other means and is valuable to NSA, in support of the FBI, for linking possible
15 terrorist-related telephone communications that occur between communicants based solely inside
16 the U.S.

17 51. As a complementary tool to other intelligence authorities, the NSA's access to
18 telephony metadata improves the likelihood of the Government being able to detect terrorist cell
19 contacts within the U.S. With the metadata collected under Section 215 pursuant to FISC orders,
20 the NSA has the information necessary to perform the call chaining that enables NSA
21 intelligence analysts to obtain a much fuller understanding of the target and, as a result, allows
22 the NSA to provide FBI with a more complete picture of possible terrorist-related activity
23 occurring inside the U.S.

1 52. The value of telephony metadata collected under Section 215 is not hypothetical.

2 While many specific instances of the Government's use of telephony metadata under Section 215
3 remain classified, a number of instances have been disclosed in declassified materials.

4 53. An illustration of the particular value of the bulk metadata program under Section
5 215—and a tragic example of what can occur in its absence—is the case of 9/11 hijacker Khalid
6 al-Mihdhar, which I have described above. The Section 215 telephony metadata collection
7 program addresses the information gap that existed at the time of the al-Mihdhar case. It allows
8 the NSA to rapidly and effectively note these types of suspicious contacts and, when appropriate,
9 to tip them to the FBI for follow-on analysis or action.

10 54. Furthermore, once an identifier has been detected, the NSA can use bulk telephony
11 metadata along with other data sources to quickly identify the larger network and possible co-
12 conspirators both inside and outside the U.S. for further investigation by the FBI with the goal of
13 preventing future terrorist attacks.

14 55. As the case examples in the FBI declaration accompanying this declaration
15 demonstrate, Section 215 bulk telephony metadata is a resource not only in isolation, but also for
16 investigating threat leads obtained from other SIGINT collection or partner agencies. This is
17 especially true for the NSA-FBI partnership. The Section 215 telephony metadata program
18 enables NSA intelligence analysts to evaluate potential threats that it receives from or reports to
19 the FBI in a more complete manner than if this data source were unavailable.

20 56. Section 215 bulk telephony metadata complements other counterterrorist-related
21 collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the
22 NSA in applying limited linguistic resources available to the counterterrorism mission against
23 links that have the highest probability of connection to terrorist targets. Put another way, while

1 Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA
2 prioritize for content analysis communications of non-U.S. persons which it acquires under other
3 authorities. Such persons are of heightened interest if they are in a communication network with
4 persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and
5 applying content analysis so that the U.S. Government gains the best possible understanding of
6 terrorist target actions and intentions.

7 57. Reliance solely on traditional, case-by-case intelligence gathering methods, restricted
8 to known terrorist identifiers, would significantly impair the NSA's ability to accomplish many
9 of the aforementioned objectives.

10 58. Without the ability to obtain and analyze bulk metadata, the NSA would lose a tool
11 for detecting communication chains that link to identifiers associated with known and suspected
12 terrorist operatives, which can lead to the identification of previously unknown persons of
13 interest in support of anti-terrorism efforts both within the U.S. and abroad. Having the bulk
14 telephony metadata available to query is part of this effort, as there is no way to know in advance
15 which numbers will be responsive to the authorized queries.

16 59. The bulk metadata allows retrospective analyses of prior communications of newly
17 discovered terrorists in an efficient and comprehensive manner. Any other means that might be
18 used to attempt to conduct similar analyses would require multiple, time-consuming steps that
19 would frustrate needed rapid analysis in emergent situations, and could fail to capture some data
20 available through bulk metadata analysis.

21 60. If the telephony metadata are not aggregated and retained for a sufficient period of
22 time, it will not be possible for the NSA to detect chains of communications that cross different
23 providers and telecommunications networks. But for the NSA's metadata collection, the NSA

1 would need to seek telephonic records from multiple providers whenever a need to inquire arose,
2 and each such provider may not maintain records in a format that is subject to a standardized
3 query.

4 61. Thus, the Government could not achieve the aforementioned benefits of Section 215
5 metadata collection through alternative means.

6 62. The use of more targeted means of collection—whether through subpoenas, national
7 security letters (“NSLs”), or pen-register and trap-and-trace (“PR/TT”) devices authorized under
8 the FISA—solely of records directly pertaining to a terrorism subject would fail to permit the
9 comprehensive and retrospective analyses detailed above of communication chains that might,
10 and sometimes do, reveal previously unknown persons of interest in terrorism investigations.

11 Targeted inquiries also would fail to capture communications chains and overlaps that can be of
12 investigatory significance, because targeted inquiries would eliminate the NSA’s ability to
13 collect and analyze metadata of communications occurring at the second and third “hop” from a
14 terrorist suspect’s initial “seed”; rather, they would only reveal communications directly
15 involving the specific targets in question. In other words, targeted inquiries would capture only
16 one “hop.” As a result, the Government’s ability to discover and analyze communications
17 metadata revealing the fact that as-yet unknown identifiers are linked in a chain of
18 communications with identified terrorist networks would be impaired.

19 63. In sum, any order barring the Government from employing the Section 215 metadata
20 collection program would deprive the Government of unique capabilities that could not be
21 completely replicated by other means, and as a result would cause an increased risk to national
22 security and the safety of the American public.

1 I declare under penalty of perjury that the foregoing is true and correct to the best of my
2 knowledge.

3
4 DATE: 12-5-13

Teresa H. Shea
5 Teresa H. Shea
6 Signals Intelligence Director
7 National Security Agency
8

EXHIBIT A

~~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 [REDACTED]

[REDACTED]

Docket Number: BR

13 - 8 0

PRIMARY ORDER

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]
[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]

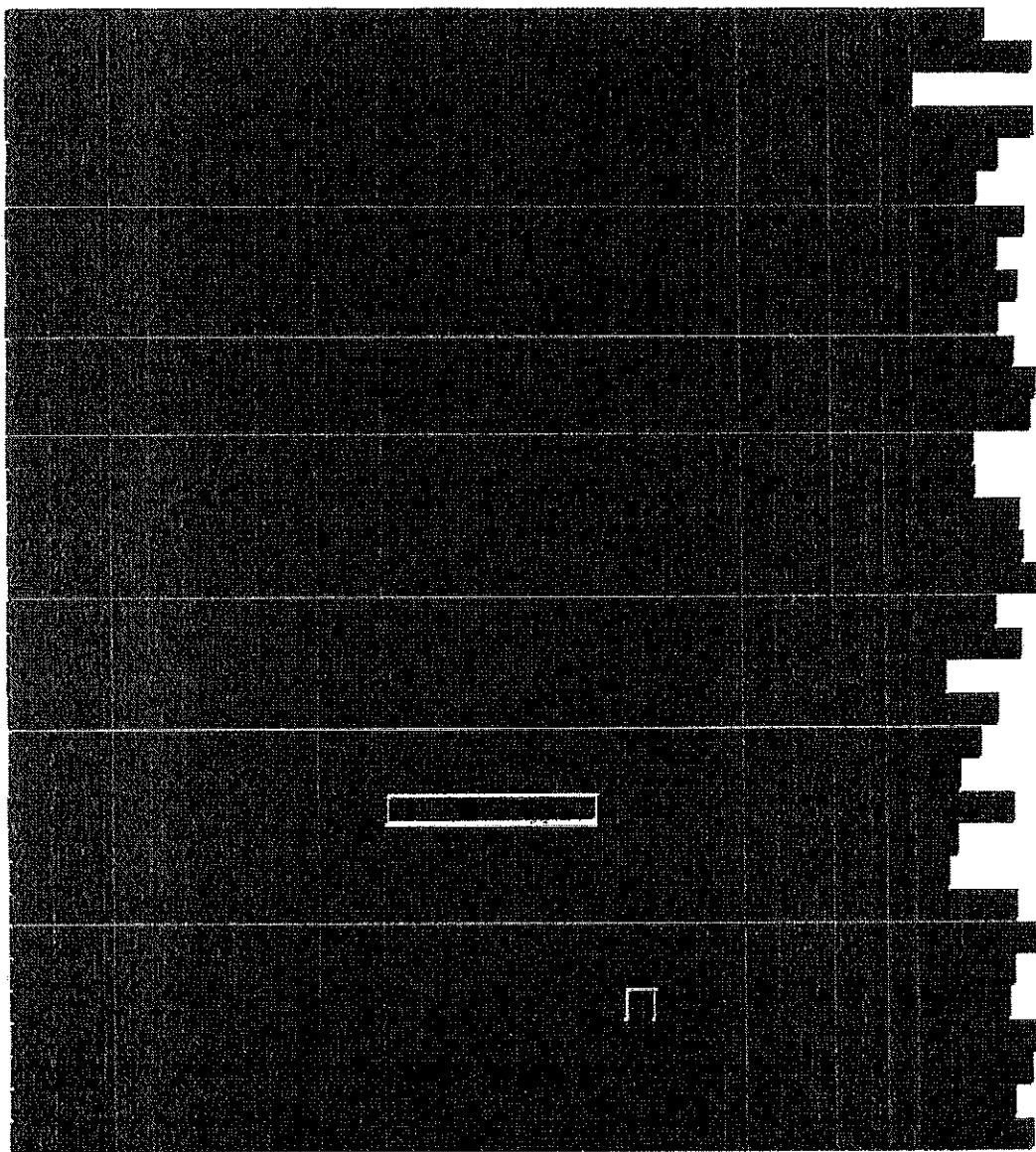
⁶ This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[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]

~~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]

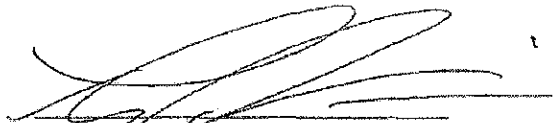
[REDACTED]

[REDACTED]

[REDACTED] expires on the 19th day

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

Signed 04-25-2013 02:26 Eastern Time
Date Time



ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

[REDACTED]

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

EXHIBIT B

~~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.

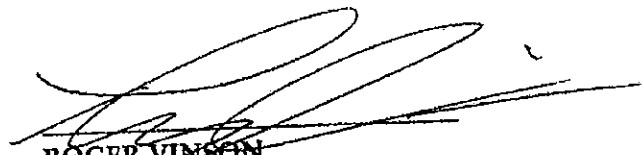
-- Remainder of page intentionally left blank. --

~~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 _____ Eastern Time
Date Time
 04-25-2013 10:26


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 B

1 STUART F. DELERY
 Assistant Attorney General
 2 JOSEPH H. HUNT
 Director, Federal Programs Branch
 3 ANTHONY J. COPPOLINO
 Deputy Branch Director
 4 tony.coppolino@usdoj.gov
 JAMES J. GILLIGAN
 5 Special Litigation Counsel
james.gilligan@usdoj.gov
 6 MARCIA BERMAN
 Senior Trial Counsel
 7 marcia.berman@usdoj.gov
 BRYAN W. DEARINGER
 8 Trial Attorney
bryan.dearinger@usdoj.gov
 9 RODNEY PATTON
 Trial Attorney
 10 rodney.patton@usdoj.gov
 U.S. Department of Justice, Civil Division
 11 20 Massachusetts Avenue, NW, Rm. 7132
 Washington, D.C. 20001
 12 Phone: (202) 514-2205; Fax: (202) 616-8470

13 *Attorneys for the Government Defs. in their Official Capacity*

14 **UNITED STATES DISTRICT COURT**
 15 **NORTHERN DISTRICT OF CALIFORNIA**
SAN FRANCISCO DIVISION

16 FIRST UNITARIAN CHURCH OF LOS
 17 ANGELES, *et al.*,

18 Plaintiffs,

19 v.

20 NATIONAL SECURITY AGENCY, *et al.*,

21 Defendants.

Case No. 3:13-cv-03287-JSW

**DECLARATION OF ACTING
 ASSISTANT DIRECTOR JOSHUA
 SKULE, FEDERAL BUREAU
 OF INVESTIGATION**

22
 23 I, Joshua Skule, hereby state and declare as follows:

24 1. I am the Acting Assistant Director of the Counterterrorism Division, Federal
 25 Bureau of Investigation (FBI), United States Department of Justice, a component of an Executive
 26 Department of the United States Government. I am responsible for, among other things,
 27 directing and overseeing the conduct of investigations originating from the FBI's
 28

1 Counterterrorism Division. As Acting Assistant Director, I have official supervision and control
2 over files and records of the Counterterrorism Division, FBI, Washington, D.C.

3 2. The FBI submits this declaration in the above-captioned case in support of the
4 Government's opposition to the plaintiffs' motion for partial summary judgment. The statements
5 made herein are based on my personal knowledge, and information I have obtained in the course
6 of carrying out my duties and responsibilities as Acting Assistant Director.

7 3. I discuss herein the National Security Agency's (NSA's) telephony metadata
8 program, authorized by the Foreign Intelligence Surveillance Court (FISC) pursuant to Section
9 215 of the USA-PATRIOT Act, under which the NSA obtains and queries bulk telephony
10 metadata for counterterrorism purposes. I address in unclassified terms the value of this program
11 as a tool, including as a complement to other classified and unclassified FBI investigatory
12 capabilities not discussed herein, for protecting the United States and its people from terrorist
13 attack.

14 Overview of the NSA Telephony Metadata Program

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

21 5. One method that the NSA has developed to accomplish this objective is the
22 FISC-authorized bulk collection and analysis of telephony metadata that principally pertains to
23 telephone calls to, from, or within the United States. Under the NSA's telephony metadata
24 program authorized by the FISC, the term "metadata" refers to information that is about
25 telephone calls but does not include cell site location information or the content of any
26 communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial
27 information of a subscriber or customer. Specifically, such telephony metadata include
28 comprehensive communications routing information, including but not limited to session

1 identifying information (*e.g.*, originating and terminating telephone number, International
2 Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity
3 (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of
4 call. By analyzing telephony metadata based on telephone numbers (or other identifiers)
5 associated with terrorist operatives or activity, NSA analysts can work to determine whether
6 known or suspected terrorists have been in contact with individuals in the United States. The
7 NSA telephony metadata program was specifically developed to assist the Government in
8 detecting communications between known or suspected terrorists who are operating outside of
9 the United States and who are in contact with others inside the United States, as well as
10 communications between operatives within the United States.

11 6. Under the NSA telephony metadata program at issue in this case, the FBI obtains
12 orders from the FISC directing certain telecommunications service providers to produce
13 telephony metadata, also referred to as call detail records, to the NSA. The NSA then stores,
14 queries, and analyzes the metadata for counterterrorism purposes. The FISC issues these orders
15 under the “business records” provision of the Foreign Intelligence Surveillance Act (FISA), 50
16 U.S.C. § 1861, enacted by section 215 of the USA PATRIOT Act (Section 215). Under the
17 terms of the FISC’s orders, the authority to continue the program must be renewed every 90
18 days. The FISC first authorized the program in May 2006, and since then it has periodically
19 renewed the program thirty-four (34) times under orders issued by fifteen (15) different FISC
20 judges.

21 7. Under the FISC’s orders, the information produced to the NSA is strictly limited
22 to telephony metadata, including the telephone numbers used to make and receive the call, when
23 the call took place, and how long the call lasted. The metadata obtained under this FISC-
24 authorized program do not include any information about the content of those calls. The
25 Government cannot, through this program, listen to or record any telephone conversations. The
26 metadata principally pertain to telephone calls made from foreign countries to the United States,
27 calls made from the United States to foreign countries, and calls within the United States.

1 8. Telephony metadata can be an important tool in a counter-terrorism investigation
2 because analysis of the data permits the Government to determine quickly whether known or
3 suspected terrorist operatives have been in contact with other persons who may be engaged in
4 terrorist activities, including persons and activities within the United States. The NSA Section
5 215 telephony metadata program is carefully limited to this purpose: it is not lawful for anyone
6 to query the bulk telephony metadata for any purpose other than counterterrorism, and FISC -
7 imposed rules strictly limit all such queries. The program includes a variety of oversight
8 mechanisms to prevent misuse, as well as external reporting requirements to the FISC and the
9 United States Congress.

10 9. The utility of analyzing telephony metadata as an intelligence tool is not a matter
11 of conjecture. Pen-register and trap-and-trace (PR/TT) devices provide no historical contact
12 information, only a record of contacts with the target occurring after the devices have been
13 installed. For decades reaching back to the Cold-War era, the FBI has relied on contact chaining
14 as a method of detecting foreign espionage networks and operatives, both in the United States
15 and abroad, and disrupting their plans. As discussed below, experience has shown that NSA
16 metadata analysis, in complement with other FBI investigatory and analytical capabilities,
17 produces information pertinent to FBI counter-terrorism investigations, and can contribute to the
18 prevention of terrorist attacks. Indeed, in March 2009, the FISC ordered that the continued
19 collection and retention of such metadata be justified by the submission of an affidavit from the
20 Director of the FBI articulating the value of the program. The FBI provided the declaration as
21 ordered and the Court reauthorized the program.

22 Court Approval

23 10. Under the Section 215 program at issue, the FBI submits an application to the
24 FISC seeking orders directing named telecommunications service providers to produce to NSA
25 call detail records created in the ordinary course of business. As required by Section 215, the
26 Government's application contains a statement of facts showing that there are reasonable
27 grounds to believe the records sought are relevant to the FBI's authorized investigations of the
28 specified foreign terrorist organizations. In addition, the application explains that the records are

1 sought for investigations to protect against international terrorism, conducted under guidelines
2 approved by the Attorney General pursuant to Executive Order 12333 (as amended) that concern
3 specified foreign terrorist organizations. The application is supported by a declaration from a
4 senior official of NSA's Signals Intelligence Directorate (SID).

5 11. Starting in May 2006 fifteen (15) separate judges of the FISC have granted the
6 Government's applications for bulk production of telephony metadata under this program on
7 thirty-five (35) separate occasions. From time to time, prior to granting the Government's
8 application the Court convenes a hearing to receive additional evidence and testimony regarding
9 the program and its implementation (as occurred in connection with the most recent renewal of
10 the program on July 19, 2013). On granting an application, the FISC issues a "Primary Order"
11 that recites the court's findings, including that there are reasonable grounds to believe the call
12 detail records sought are relevant to authorized FBI investigations to protect against international
13 terrorism. The Primary Order then provides that certain telecommunications service providers,
14 upon receipt of appropriate Secondary Orders (discussed below), shall produce to NSA on an
15 ongoing daily basis for the duration of the Primary Order electronic copies of the call detail
16 records created by them containing the "telephony metadata" discussed above, explicitly
17 excluding the substantive content of any communication, the name, address, or financial
18 information of a subscriber or customer, and cell site location information.

19 12. The Primary Order also sets a specific date and time on which the NSA's
20 authority to collect bulk telephony metadata from the providers expires, usually within 90 days
21 of the date on which the FISC issues the order, necessitating the submission of an application for
22 additional orders to renew the NSA's authority if the program is to continue.

23 13. In conjunction with the Primary Order, the FISC also issues a so-called
24 "Secondary Order" to each of the telecommunications service providers identified in the Primary
25 Order. These orders direct the providers, consistent with the Primary Order, to produce
26 "telephony metadata" to NSA on an ongoing daily basis thereafter for the duration of the Order.
27 Telephony metadata is defined under the Secondary Orders to include (and exclude) the same
28 information as under the Primary Order.

1 14. These prospective orders for the production of metadata make for efficient
2 administration of the process for all parties involved—the FISC, the Government, and the
3 providers. In theory the FBI could seek a new set of orders on a daily basis for the records
4 created within the preceding 24 hours. But the creation and processing of such requests would
5 impose entirely unnecessary burdens on both the FISC and the FBI – no new information would
6 be anticipated in such a short period of time to alter the basis of the FBI’s request or the facts
7 upon which the FISC has based its orders. Providers would also be forced to review daily
8 requests, rather than merely continuing to comply with one ongoing request, a situation that
9 would be more onerous on the providers and raise potential and unnecessary compliance issues.
10 The prospective orders sought and obtained by the FBI merely ensure that the records can be
11 sought in a reasonable manner for a reasonable period of time (90 days) while avoiding
12 unreasonable and burdensome paperwork.

13 NSA’s Query and Analysis of the Metadata and Dissemination of the Results

14 15. Under the FISC Orders at issue, before NSA may query the metadata acquired
15 under the FISC’s orders for intelligence purposes, authorized NSA officials must determine that
16 the identifiers on which the queries will be based are reasonably suspected of being associated
17 with one (or more) of the foreign terrorist organizations specified in the Primary Order.

18 16. The information on which such determinations of “reasonable, articulable
19 suspicion” are based comes from several sources, including the FBI. The FBI, based on
20 information acquired in the course of one or more counter-terrorism investigations, may develop
21 reasons for concluding that a particular identifier, such as a foreign telephone number, is
22 associated with a person (located in the United States or abroad) who is affiliated with one of the
23 specified terrorist organizations. On that basis, the FBI may submit a request to NSA for further
24 information about that identifier available from the collected telephony metadata.

25 Investigative Value of Telephony Metadata to the FBI’s Counter-Terrorism Mission

26 17. Counter-terrorism investigations serve important purposes beyond the ambit of
27 routine criminal inquiries and prosecution, which ordinarily focus retrospectively on specific
28 crimes that have already occurred and the persons known or suspected to have committed them.

1 The key purpose of terrorism investigations, in contrast, is to prevent terrorist attacks before they
2 occur. Terrorism investigations also provide the basis for, and inform decisions concerning,
3 other measures needed to protect the national security, including: excluding or removing persons
4 involved in terrorism from the United States; freezing assets of organizations that engage in or
5 support terrorism; securing targets of terrorism; providing threat information and warnings to
6 other federal, state, local, and private agencies and entities; diplomatic or military actions; and
7 actions by other intelligence agencies to counter international terrorism threats.

8 18. As a result, national security investigations often have remarkable breadth,
9 spanning long periods of time and multiple geographic regions to identify terrorist groups, their
10 members, and their intended targets, plans, and means of attack, many of which are often
11 unknown to the intelligence community at the outset. National security investigations thus
12 require correspondingly far-reaching means of information-gathering to shed light on suspected
13 terrorist organizations, their size and composition, geographic reach, relation to foreign powers,
14 financial resources, past acts, goals, plans, and capacity for carrying them out, so that their plans
15 may be thwarted before terrorist attacks are launched. Contact chaining information derived from
16 queries and analysis of the Section 215 bulk telephony metadata has contributed to achieving this
17 critical objective.

18 19. The FBI derives significant value from the advantages of telephony metadata
19 analysis. The FBI is charged with collecting intelligence and conducting investigations to detect,
20 disrupt, and prevent terrorist threats to national security. The more pertinent information the FBI
21 has regarding such threats, the more likely it will be able to protect against them. The oft-used
22 metaphor is that the FBI is responsible for "connecting the dots" to form a picture of the threats
23 to national security. Information gleaned from analysis of bulk telephony metadata provides
24 additional "dots" that the FBI uses to ascertain the nature and extent of domestic threats to the
25 national security.

26 20. The NSA provides "tips" to the FBI regarding certain telephone numbers
27 resulting from a query of the Section 215 telephony metadata. In certain instances, the FBI has
28 received metadata-based tips containing information not previously known to the FBI about

1 domestic telephone numbers utilized by targets of pending preliminary investigations. The
2 information from the metadata tips has provided articulable factual bases to believe that the
3 subjects posed a threat to the national security such that the preliminary investigations could be
4 converted to full investigations, which, in turn, led the FBI to focus resources on those targets
5 and their activities. The FBI has also re-opened previously closed investigations based on
6 information contained in metadata tips. In those instances, the FBI had previously exhausted all
7 leads and concluded that no further investigation was warranted. The new information from the
8 metadata tips was significant enough to warrant the re-opening of the investigations.

9 21. In other situations, the FBI may already have an investigative interest in a
10 particular domestic telephone number prior to receiving a metadata tip from NSA. Nevertheless,
11 the tip may be valuable if it provides new information regarding the domestic telephone number
12 that re-vitalizes the investigation, or otherwise allows the FBI to focus its resources more
13 efficiently and effectively on individuals who present genuine threats (by helping either to
14 confirm or to rule out particular individuals as subjects for further investigation).

15 22. Accordingly, the NSA telephony metadata program authorized under Section 215
16 is a valuable source of intelligence for the FBI that is relevant to FBI-authorized international
17 terrorism investigations.

18 23. The tips or leads the FBI receives from bulk metadata analysis under this program
19 can also act as an early warning of a possible threat to the national security. The sooner the FBI
20 obtains information about particular threats to national security, the more likely it will be able to
21 prevent and protect against them. Bulk metadata analysis sometimes provides information
22 earlier than the FBI's other investigative methods and techniques. In those instances, the Section
23 215 NSA telephony metadata program acts as an "early warning system" of potential threats
24 against national security. Earlier receipt of this information may advance an investigation and
25 contribute to the FBI preventing a terrorist attack that, absent the metadata tip, the FBI could not.

26 24. A number of recent episodes illustrate the role that telephony metadata analysis
27 can play in preventing and protecting against terrorist attack. In January 2009, using authorized
28 collection under Section 702 of the Foreign Intelligence Surveillance Act to monitor the

1 communications of an extremist overseas with ties to al-Qa'ida, NSA discovered a connection
2 with an individual based in Kansas City. NSA tipped the information to the FBI, which during
3 the course of its investigation discovered that there had been a plot in its early stages to attack the
4 New York Stock Exchange. After further investigation, NSA queried the telephony metadata to
5 ensure that all potential connections were identified, which assisted the FBI in running down
6 leads. As a result of the investigation, three defendants pled guilty and were convicted of
7 terrorism offenses relating to their efforts to support al-Qa'ida.

8 25. In October 2009, David Coleman Headley, a Chicago businessman and dual U.S.
9 and Pakistani citizen, was arrested by the FBI as he tried to depart from Chicago O'Hare airport
10 on a trip to Pakistan. At the time of his arrest, Headley and his colleagues, at the behest of al-
11 Qa'ida, were plotting to attack the Danish newspaper that published cartoons depicting the
12 Prophet Mohammed. Headley was later charged with support to terrorism based on his
13 involvement in the planning and reconnaissance for the 2008 hotel attack in Mumbai. Collection
14 against foreign terrorists and telephony metadata analysis were utilized in tandem with FBI law
15 enforcement authorities to establish Headley's foreign ties and put them in context with his U.S.
16 based planning efforts.

17 26. In September 2009, using authorized collection under Section 702 to monitor al-
18 Qa'ida terrorists overseas, NSA discovered that one of the al-Qa'ida associated terrorists was in
19 contact with an unknown person located in the U.S. about efforts to procure explosive material.
20 NSA immediately tipped this information to the FBI, which investigated further, and identified
21 the al-Qa'ida contact as Colorado-based extremist Najibullah Zazi. NSA and FBI worked
22 together to determine the extent of Zazi's relationship with al-Qa'ida and to identify any other
23 foreign or domestic terrorist links. NSA received Zazi's telephone number from the FBI and ran
24 it against the Section 215 telephony metadata, identifying and passing additional leads back to
25 the FBI for investigation. One of these leads revealed a previously unknown number for co-
26 conspirator Adis Medunjanin and corroborated his connection to Zazi as well as to other U.S.-
27 based extremists. Zazi and his co-conspirators were subsequently arrested. Upon indictment,
28

1 Zazi pled guilty to conspiring to bomb the New York City subway system. In November 2012,
2 Medunjanin was sentenced to life in prison.

3 Alternatives to the NSA's Bulk Collection of Telephony Metadata

4 27. The NSA bulk collection program at issue here presents distinct advantages.
5 The contact chaining capabilities offered by the program exceed the chaining that is performed
6 on data collected pursuant to other means, including traditional means of case-by-case
7 intelligence gathering targeted at individual telephone numbers such as subpoena, warrant,
8 national security letter, pen-register and trap-and-trace (PR/TT) devices, or more narrowly
9 defined orders under Section 215. This is so in at least two important respects, namely, the
10 NSA's querying and analysis of the aggregated bulk telephony metadata under this program.

11 28. First, the agility of querying the metadata collected by NSA under this program
12 allows for more immediate contact chaining, which is significant in time-sensitive situations of
13 suspects' communications with known or as-yet unknown co-conspirators. For example, if
14 investigators find a new telephone number when an agent of one of the identified international
15 terrorist organizations is captured, and the Government issues a national security letter for the
16 call detail records for that particular number, it would only be able to obtain the first tier of
17 telephone number contacts and, in rare instances, the second tier of contacts if the FBI separately
18 demonstrates the relevance of the second-generation information to the national security
19 investigation. At least with respect to the vast majority of national security letters issued, new
20 national security letters would have to be issued for telephone numbers identified in the first tier,
21 in order to find an additional tier of contacts. The delay inherent in issuing new national security
22 letters would necessarily mean losing valuable time.

23 29. Second, aggregating the NSA telephony metadata from different
24 telecommunications providers enhances and expedites the ability to identify chains of
25 communications across multiple providers. Furthermore, NSA disseminations provided to the
26 FBI from this program may include NSA's analysis informed by its unique collection
27 capabilities.

28

EXHIBIT C

~~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 [REDACTED]

[REDACTED]

Docket Number: BR 13-109

AMENDED MEMORANDUM OPINION

I. Background.

On July 18, 2013, a verified Final "Application for Certain Tangible Things for Investigations to Protect Against International Terrorism" (Application) was submitted to the Court by the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States

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

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

Code (U.S.C.), § 1861, as amended (also known as Section 215 of the USA PATRIOT Act),¹ requiring the ongoing daily production to the National Security Agency (NSA) of certain call detail records or “telephony metadata” in bulk.² The Court, after having fully considered the United States Government’s (government) earlier-filed Proposed Application pursuant to Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 9(a),³ and having held an extensive hearing to receive testimony and

¹ “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,” Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) (“PATRIOT Act”), amended by, “USA PATRIOT Improvement Reauthorization Act of 2005,” Pub. L. No. 109-177, 120 Stat. 192 (Mar. 9, 2006); “USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006,” Pub. L. No. 109-178, 120 Stat. 278 (Mar. 9, 2006); and Section 215 expiration extended by “Department of Defense Appropriations Act, 2010,” Pub. L. No. 111-118 (Dec. 19, 2009); “USA PATRIOT—Extension of Sunsets,” Pub. L. No. 111-141 (Feb. 27, 2010); “FISA Sunsets Extension Act of 2011,” Pub. L. No. 112-3 (Feb. 25, 2011); and, “PATRIOT Sunsets Extension Act of 2011,” Pub. L. No. 112-14, 125 Stat. 216 (May 26, 2011).

² For purposes of this matter, “‘telephony metadata’ includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile station Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) 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.” App. at 4. In addition, the Court has explicitly directed that its authorization does not include “the production of cell site location information (CSLI).” Primary Ord. at 3.

³ Prior to scheduling a hearing in this matter, the Court reviewed the Proposed Application and its filed Exhibits pursuant to its standard procedure. Exhibit A consists of a Declaration from the NSA in support of the government’s Application. As Ordered by this Court in Docket No. BR 13-80, Exhibit B is a Renewal Report to describe any significant changes proposed in the way in which records would be received, and any significant changes to controls NSA has in place to receive, store, process, and disseminate the information. [REDACTED] It also provides the final segment of information normally contained in the 30-day reports discussed below. As Ordered by this Court in Docket No. BR 13-80, Exhibit C is a summary of a meeting held by Executive Branch representatives to assess compliance with this Court’s Orders. Furthermore, the Court reviewed the previously filed 30-day reports that were Ordered by this Court in Docket No. 13-80, discussing NSA’s application of the reasonable, articulable suspicion (RAS) standard for approving selection terms and implementation of the automated query process. In addition, the 30-day reports describe disseminations of U.S.-person information obtained under this program.

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

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

evidence on this matter on July 18, 2013,⁴ GRANTED the application for the reasons stated in this Memorandum Opinion and in a Primary Order issued on July 19, 2013, which is appended hereto.

In conducting its review of the government's application, the Court considered whether the Fourth Amendment to the U.S. Constitution imposed any impediment to the government's proposed collection. Having found none in accord with U.S. Supreme Court precedent, the Court turned to Section 215 to determine if the proposed collection was lawful and that Orders requested from this Court should issue. The Court found that under the terms of Section 215 and under operation of the canons of statutory construction such Orders were lawful and required, and the requested Orders were therefore issued.

⁴ The proceedings were conducted *ex parte* under security procedures as mandated by 50 U.S.C. §§ 1803(c), 1861(c)(1), and FISC Rules 3, 17(a)-(b). See Letter from Presiding Judge Walton, U.S. FISC to Chairman Leahy, Senate Judiciary Committee (Jul. 29, 2013), at 7 (noting that initial proceedings before the FISC are handled *ex parte* as is the universal practice in courts that handle government requests for orders for the production of business records, pen register/trap and trace implementation, wiretaps, and search warrants), <http://www.uscourts.gov/uscourts/fisc/honorable-patrick-leahy.pdf>. Pursuant to FISC Rules 17(b)-(d), this Court heard oral argument by attorneys from the U.S. Department of Justice, and received sworn testimony from personnel from the FBI and NSA. The Court also entered into evidence Exhibits 1-7 during the hearing. Except as cited in this Memorandum Opinion, at the request of the government, the transcript of the hearing has been placed under seal by Order of this Court for security reasons. Draft Tr. at 3-4. At the hearing, the government notified the Court that it was developing an updated legal analysis expounding on its legal position with regard to the application of Section 215 to bulk telephony metadata collection. Draft Tr. at 25. The government was not prepared to present such a document to the Court. The Court is aware that on August 9, 2013, the government released to the public an "Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act" (Aug. 9, 2013). The Court, however, has not reviewed the government's "White Paper" and the "White Paper" has played no part in the Court's consideration of the government's Application or this Memorandum Opinion.

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

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

Specifically, the government requested Orders from this Court to obtain certain business records of specified telephone service providers. Those telephone company business records consist of a very large volume of each company's call detail records or telephony metadata, but expressly exclude the contents of any communication; the name, address, or financial information of any subscriber or customer; or any cell site location information (CSLI). Primary Ord. at 3 n.1.⁵ The government requested production of this data on a daily basis for a period of 90 days. The sole purpose of this production is to obtain foreign intelligence information in support of [REDACTED] individual authorized investigations to protect against international terrorism and concerning various international terrorist organizations. See Primary Ord. at 2, 6; App. at 8; and, Ex. A. at 2-3. In granting the government's request, the Court has prohibited the government from accessing the data for any other intelligence or investigative purpose.⁶ Primary Ord. at 4.

⁵ In the event that the government seeks the production of CSLI as part of the bulk production of call detail records in the future, the government would be required to provide notice and briefing to this Court pursuant to FISC Rule 11. The production of all call detail records of all persons in the United States has never occurred under this program. For example, the government [REDACTED] App. at 13 n.4.

⁶ The government may, however, permit access to "trained and authorized technical personnel ... to perform those processes needed to make [the data] usable for intelligence analysis," Primary Ord. at 5, and may share query results "[1] to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate lawful oversight functions." Id. at 14.

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

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

By the terms of this Court's Primary Order, access to the data is restricted through technical means, through limits on trained personnel with authorized access, and through a query process that requires a reasonable, articulable suspicion (RAS), as determined by a limited set of personnel, that the selection term (e.g., a telephone number) that will be used to search the data is associated with one of the identified international terrorist organizations.⁷ Primary Ord. at 4-9. Moreover, the government may not make the RAS determination for selection terms reasonably believed to be used by U.S. persons solely based on activities protected by the First Amendment. *Id.* at 9; and see 50 U.S.C. § 1861(a)(1). To ensure adherence to its Orders, this Court has the authority to oversee compliance, see 50 U.S.C. § 1803(h), and requires the government to notify the Court in writing immediately concerning any instance of non-compliance, see FISC Rule 13(b). According to the government, in the prior authorization period there have been no compliance incidents.⁸

Finally, although not required by statute, the government has demonstrated through its written submissions and oral testimony that this production has been and remains valuable for obtaining foreign intelligence information regarding international

⁷ A selection term that meets specific legal standards has always been required. This Court has not authorized government personnel to access the data for the purpose of wholesale "data mining" or browsing.

⁸ The Court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information. Through oversight by this Court over a period of months, those issues were resolved.

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

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

terrorist organizations, see App. Ex. B at 3-4; Thirty-Day Report for Filing in Docket Number BR 13-80 (Jun. 25, 2013) at 3-4; Thirty-Day Report for Filing in Docket Number BR 13-80 (May 24, 2013) a 3-4.

II. Fourth Amendment.⁹

The production of telephone service provider metadata is squarely controlled by the U.S. Supreme Court decision in Smith v. Maryland, 442 U.S. 735 (1979). The Smith decision and its progeny have governed Fourth Amendment jurisprudence with regard to telephony and communications metadata for more than 30 years. Specifically, the Smith case involved a Fourth Amendment challenge to the use of a pen register on telephone company equipment to capture information concerning telephone calls,¹⁰ but not the content or the identities of the parties to a conversation. Id. at 737, 741 (citing Katz v. United States, 389 U.S. 347 (1967), and United States v. New York Tel. Co., 434 U.S. 159 (1977)). The same type of information is at issue here.¹¹

⁹ "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

¹⁰ Because the metadata was obtained from telephone company equipment, the Court found that "petitioner obviously cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'" Id. at 741.

¹¹ The Court is aware that additional call detail data is obtained via this production than was acquired through the pen register acquisition at issue in Smith. Other courts have had the opportunity to review whether there is a Fourth Amendment expectation of privacy in call detail records similar to the data sought in this matter and have found that there is none. See United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009) (finding that because "data about the 'call origination, length, and time of call' ... is nothing more than pen register and trap and trace data, there is no Fourth Amendment 'expectation of privacy.'"

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

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

The Supreme Court in Smith recognized that telephone companies maintain call detail records in the normal course of business for a variety of purposes. Id. at 742 (“All subscribers realize ... that the phone company has facilities for making permanent records of the number they dial....”). This appreciation is directly applicable to a business records request. “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.” Id. at 743. Furthermore, the Supreme Court found that once a person has transmitted this information to a third party (in this case, a telephone company), the person “has no legitimate expectation of privacy in [the] information....”¹² Id. The telephone user, having conveyed this information to a telephone company that retains the information in the ordinary course of business, assumes the risk that the company will provide that information to the

(citing Smith, 442 U.S. at 743-44)) cert. denied 559 U.S. 987, 988 (2010); United States Telecom Ass’n, 227 F.3d 450, 454 (D.C. Cir. 2000) (noting pen registers record telephone numbers of outgoing calls and trap and trace devices are like caller ID systems, and that such information is not protected by the Fourth Amendment); United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990) (recognizing that “[t]he installation and use of a pen register and trap and trace device is not a ‘search’ requiring a warrant pursuant to the Fourth Amendment,” and noting that there is no “‘legitimate expectation of privacy’ at stake.” (citing Smith, 442 U.S. at 739-46)).

¹² The Supreme Court has applied this principle – that there is no Fourth Amendment search when the government obtains information that has been conveyed to third parties – in cases involving other types of business records. See United States v. Miller, 425 U.S. 435 (1976) (bank records); see also S.E.C. v. Jerry T. O’Brien, Inc., 467 U.S. 735, 743 (1984) (“It is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities.”) (citing Miller, 425 U.S. at 443).

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

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

government. See id. at 744. Thus, the Supreme Court concluded that a person does not have a legitimate expectation of privacy in telephone numbers dialed and, therefore, when the government obtained that dialing information, it “was not a ‘search,’ and no warrant was required” under the Fourth Amendment. Id. at 746.¹³

In Smith, the government was obtaining the telephone company’s metadata of one person suspected of a crime. See id. at 737. Here, the government is requesting daily production of certain telephony metadata in bulk belonging to companies without specifying the particular number of an individual. This Court had reason to analyze this distinction in a similar context in [REDACTED]

[REDACTED] In that case, this Court found that “regarding the breadth of the proposed surveillance, it is noteworthy that the application of the Fourth Amendment depends on the government’s intruding into some individual’s reasonable expectation of privacy.” Id. at 62. The Court noted that Fourth Amendment rights are personal and individual, see id. (citing Steagald v. United States, 451 U.S. 204, 219 (1981); accord, e.g., Rakas v. Illinois, 439 U.S. 128, 133 (1978) (“Fourth Amendment rights are personal rights which ... may not be vicariously asserted.”) (quoting Alderman v. United States, 394 U.S. 165, 174 (1969))), and that “[s]o long as no individual has a reasonable expectation of privacy

¹³ If a service provider believed that a business records order infringed on its own Fourth Amendment rights, it could raise such a challenge pursuant to 50 U.S.C. § 1861(f).

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

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

in meta data, the large number of persons whose communications will be subjected to the ... surveillance is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur." *Id.* at 63. Put another way, where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*.

In sum, because the Application at issue here concerns only the production of call detail records or "telephony metadata" belonging to a telephone company, and not the contents of communications, Smith v. Maryland compels the conclusion that there is no Fourth Amendment impediment to the collection. Furthermore, for the reasons stated in [REDACTED] and discussed above, this Court finds that the volume of records being acquired does not alter this conclusion. Indeed, there is no legal basis for this Court to find otherwise.

III. Section 215.

Section 215 of the USA PATRIOT Act created a statutory framework, the various parts of which are designed to ensure not only that the government has access to the information it needs for authorized investigations, but also that there are protections and prohibitions in place to safeguard U.S. person information. It requires the government to demonstrate, among other things, that there is "an investigation to

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

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

obtain foreign intelligence information ... to [in this case] protect against international terrorism," 50 U.S.C. § 1861(a)(1); that investigations of U.S. persons are "not conducted solely upon the basis of activities protected by the first amendment to the Constitution," *id.*; that the investigation is "conducted under guidelines approved by the Attorney General under Executive Order 12333," *id.* § 1861(a)(2); that there is "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to the investigation, *id.* § 1861(b)(2)(A);¹⁴ that there are adequate minimization procedures "applicable to the retention and dissemination" of the information requested, *id.* § 1861(b)(2)(B); and, that only the production of such things that could be "obtained with a subpoena *duces tecum*" or "any other order issued by a court of the United States directing the production of records" may be ordered, *id.* § 1861(c)(2)(D), *see infra* Part III.a. (discussing Section 2703(d) of the Stored Communications Act). If the Court determines that the government has met the requirements of Section 215, it shall enter an *ex parte* order compelling production.¹⁵

¹⁴ This section also provides that the records sought are "presumptively relevant to an authorized investigation if the applicant shows in the statement of facts that they pertain to—(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known, to, a suspected agent of a foreign power who is the subject of such authorized investigation." 50 U.S.C. § 1861(b)(2)(A)(i)-(iii). The government has not invoked this presumption and, therefore, the Court need not address it.

¹⁵ "Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of [Section 215], the judge *shall* enter an *ex parte* order as requested, or as modified, approving the release of tangible things." *Id.* § 1861(c)(1) (emphasis added). As indicated, the Court may modify the Orders as necessary, and compliance issues could present situations requiring modification.

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

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

This Court must verify that each statutory provision is satisfied before issuing the requested Orders. For example, even if the Court finds that the records requested are relevant to an investigation, it may not authorize the production if the minimization procedures are insufficient. Under Section 215, minimization procedures are “specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” *Id.* § 1861(g)(2)(A). Congress recognized in this provision that information concerning U.S. persons that is not directly responsive to foreign intelligence needs will be produced under these orders and established post-production protections for such information. As the Primary Order issued in this matter demonstrates, this Court’s authorization includes detailed restrictions on the government through minimization procedures. *See* Primary Ord. at 4-17. Without those restrictions, this Court could not, nor would it, have approved the proposed production. This Court’s Primary Order also sets forth the requisite findings under Section 215 for issuing the Orders requested by the government in its Application. *Id.* at 2, 4-17.

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

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

The Court now turns to its interpretation of Section 215 with regard to how it compares to 18 U.S.C. § 2703 (Stored Communications Act); its determination that “there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation,” 50 U.S.C. § 1861(b)(2)(A); and, the doctrine of legislative re-enactment as it pertains to the business records provision.

- a. Section 215 of FISA and Section 2703(d) of the Stored Communications Act.

It is instructive to compare Section 215, which is used for foreign intelligence purposes and is codified as part of FISA, with 18 U.S.C. § 2703 (“Required disclosure of customer communications or records”), which is used in criminal investigations and is part of the Stored Communications Act (SCA). See In Re Production of Tangible Things From [REDACTED]

[REDACTED], Docket No. BR 08-13, Supp. Op. (Dec. 12, 2008) (discussing Section 215 and Section 2703). Section 2703 establishes a process by which the government can obtain information from electronic communications service providers, such as telephone companies. As with FISA, this section of the SCA provides the mechanism for obtaining either the contents of communications, or non-content records of communications. See 18 U.S.C. §§ 2703(a)-(c).

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

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

For non-content records production requests, such as the type sought here, Section 2703(c) provides a variety of mechanisms, including acquisition through a court order under Section 2703(d). Under this section, which is comparable to Section 215, the government must offer to the court “*specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation.*” *Id.* § 2703(d) (emphasis added). Section 215, the comparable provision for foreign intelligence purposes, requires neither “specific and articulable facts” nor does it require that the information be “material.” Rather, it merely requires a statement of facts showing that there are reasonable grounds to believe that the records sought are relevant to the investigation. See 50 U.S.C. §1861(b)(2)(A). That these two provisions apply to the production of the same type of records from the same type of providers is an indication that Congress intended this Court to apply a different, and in specific respects lower, standard to the government’s Application under Section 215 than a court reviewing a request under Section 2703(d). Indeed, the pre-PATRIOT Act version of FISA’s business records provision required “specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.” 50 U.S.C. §1862(b)(2)(B) as it read on October 25, 2001.¹⁶ In enacting Section 215,

¹⁶ Prior to enactment of the PATRIOT Act, the business records provision was in Section 1862 vice 1861.

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

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

Congress removed the requirements for “specific and articulable facts” and that the records pertain to “a foreign power or an agent of a foreign power.” Accordingly, now the government need not provide specific and articulable facts, demonstrate any connection to a particular suspect, nor show materiality when requesting business records under Section 215. To find otherwise would be to impose a higher burden – one that Congress knew how to include in Section 215, but chose to dispense with.

Furthermore, Congress provided different measures to ensure that the government obtains and uses information properly, depending on the purpose for which it sought the information. First, Section 2703 has no provision for minimization procedures. However, such procedures are mandated under Section 215 and must be designed to restrict the retention and dissemination of information, as imposed by this Court’s Primary Order. Primary Ord. at 4-17; see 50 U.S.C. §§ 1861(c)(1), (g).

Second, Section 2703(d) permits the service provider to file a motion with a court to “quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause undue burden on such provider.” Id. Congress recognized that, even with the higher statutory standard for a production order under Section 2703(d), some requests authorized by a court would be “voluminous” and provided a means by which the provider could seek relief using a motion. Id. Under Section 215, however, Congress

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

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

provided a specific and complex statutory scheme for judicial review of an Order from this Court to ensure that providers could challenge both the legality of the required production and the nondisclosure provisions of that Order. 50 U.S.C. § 1861(f). This adversarial process includes the selection of a judge from a pool of FISC judges to review the challenge to determine if it is frivolous and to rule on the merits, *id.* § 1861(f)(2)(A)(ii), provides standards that the judge is to apply during such review, *id.* §§ 1861(f)(2)(B)-(C), and provides for appeal to the Foreign Intelligence Surveillance Court of Review and, ultimately, the U.S. Supreme Court, *id.* § 1861(f)(3).¹⁷ This procedure, as opposed to the motion process available under Section 2703(d) to challenge a production as unduly voluminous or burdensome, contemplates a substantial and engaging adversarial process to test the legality of this Court's Orders under Section 215.¹⁸ This enhanced process appears designed to ensure that there are additional safeguards in light of the lower threshold that the government is required to meet for production under Section 215 as opposed to Section 2703(d). To date, no holder of

¹⁷ For further discussion on the various means by which adversarial proceedings before the FISC may occur, *see* Letter from Presiding Judge Walton, U.S. FISC to Chairman Leahy, Senate Judiciary Committee (Jul. 29, 2013), at 7-10, <http://www.uscourts.gov/uscourts/fisc/honorable-patrick-leahy.pdf>.

¹⁸ In *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F.Supp.2d 114, 128-29 (E.D. Va. 2011), the court found that only the service provider, as opposed to a customer or subscriber, could challenge the execution of a § 2703(d) non-content records order. The court reasoned that "[b]ecause Congress clearly provided ... protections for one type of § 2703 order [content] but not for others, the Court must infer that Congress deliberately declined to permit challenges for the omitted orders." *Id.* The court also noted that the distinction between content and non-content demonstrates an incorporation of *Smith v. Maryland* into the SCA. *Id.* at 128 n.11. As discussed above, the operation of Section 215 within FISA represents that same distinction.

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

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

records who has received an Order to produce bulk telephony metadata has challenged the legality of such an Order. Indeed, no recipient of any Section 215 Order has challenged the legality of such an Order, despite the explicit statutory mechanism for doing so.

When analyzing a statute or a provision thereof, a court considers the statutory schemes as a whole. See Kokoszka v. Belford, 417 U.S. 642, 650 (1974) (noting that when a court interprets a statute, it looks not merely to a particular clause but will examine it within the whole statute or statutes on the same subject) (internal quotation and citation omitted); Jones v. St. Louis-San Francisco Ry. Co., 728 F.2d 257, 262 (6th Cir. 1984) (“[W]here two or more statutes deal with the same subject, they are to be read *in pari materia* and harmonized, if possible. This rule of statutory construction is based upon the premise that when Congress enacts a new statute, it is aware of all previously enacted statutes on the same subject.”) (citations omitted). Here, the Court finds that Section 215 and Section 2703(d) operate in a complementary manner and are designed for their specific purposes. In the criminal investigation context, Section 2703(d) includes front-end protections by imposing a higher burden on the government to obtain the information in the first instance. On the other hand, when the government seeks to obtain the same type of information, but for a foreign intelligence purpose, Congress provided the government with more latitude at the production stage under

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

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

Section 215 by not requiring specific and articulable facts or meeting a materiality standard. Instead, it imposed post-production checks in the form of mandated minimization procedures and a structured adversarial process. This is a logical framework and it comports well with the Fourth Amendment concept that the required factual predicate for obtaining information in a case of special needs, such as national security, can be lower than for use of the same investigative measures for an ordinary criminal investigation. See United States v. United States District Court (Keith), 407 U.S. 297, 308-09, 322-23 (1972); and, In re Sealed Case, 310 F.3d 717, 745-46 (FISA Ct. Rev. 2002) (differentiating requirements for the government to obtain information obtained for national security reasons as opposed to a criminal investigation).¹⁹ Moreover, the government's interest is significantly greater when it is attempting to thwart attacks and disrupt activities that could harm national security, as opposed to gathering evidence on domestic crimes. See In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (“[T]he relevant government interest—the interest in national security—is of the highest order of magnitude.”) (citing Haig v. Agee, 453 U.S. 280, 307 (1981)); and, In re Sealed Case, 310 F.3d at 745-46.

¹⁹ As discussed above, there is no Fourth Amendment interest here, as per Smith v. Maryland.

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

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

b. Relevance.

Because known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, the production of the information sought meets the standard for relevance under Section 215.

As an initial matter and as a point of clarification, the government's burden under Section 215 is not to prove that the records sought are, in fact, relevant to an authorized investigation. The explicit terms of the statute require "a statement of facts showing that there are *reasonable grounds to believe* that the tangible things sought are relevant...." 50 U.S.C. § 1861(b)(2)(A) (emphasis added). In establishing this standard, Congress chose to leave the term "relevant" undefined. It is axiomatic that when Congress declines to define a term a court must give the term its ordinary meaning. See, e.g., Taniguchi v. Kan Pacific Saipan, Ltd., ___ U.S. ___, 132 S.Ct. 1997, 2002 (2012). Accompanying the government's first application for the bulk production of telephone company metadata was a Memorandum of Law which argued that "[i]nformation is 'relevant' to an authorized international terrorism investigation if it bears upon, or is pertinent to, that investigation." Mem. of Law in Support of App. for Certain Tangible

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

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

Things for Investigations to Protect Against International Terrorism, Docket No. BR 06-05 (filed May 23, 2006), at 13-14 (quoting dictionary definitions, Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351 (1978), and Fed. R. Evid. 401²⁰). This Court recognizes that the concept of relevance here is in fact broad and amounts to a relatively low standard.²¹ Where there is no requirement for specific and articulable facts or materiality, the government may meet the standard under Section 215 if it can demonstrate reasonable grounds to believe that the information sought to be produced has some bearing on its investigations of the identified international terrorist organizations.

This Court has previously examined the issue of relevance for bulk collections.

See [REDACTED]

[REDACTED]

[REDACTED]

²⁰ At the time of the government's submission in Docket No. BR 06-05, a different version of Fed. R. Evid. 401 was in place. While not directly applicable in this context, the current version reads: "Evidence is relevant if: (a) it has *any tendency* to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." (Emphasis added.)

²¹ Even under the higher "relevant and material" standard for 18 U.S.C. § 2703(d), discussed above, "[t]he government need not show actual relevance, such as would be required at trial." In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F.Supp.2d 114, 130 (E.D. Va. 2011). The petitioners had argued in that case that most of their activity for which records were sought was "unrelated" and that "the government cannot be permitted to blindly request everything that 'might' be useful..." Id. (internal quotation omitted). The court rejected this argument, noting that "[t]he probability that some gathered information will not be material is not a substantial objection," and that where no constitutional right is implicated, as is the case here, "there is no need for ... narrow tailoring." Id.

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

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] While those matters involved different collections from the one at issue here, the relevance standard was similar. See 50 U.S.C. § 1842(c)(2) (“[R]elevant to an ongoing investigation to protect against international terrorism....”). In both cases, there were facts demonstrating that information concerning known and unknown affiliates of international terrorist organizations was contained within the non-content metadata the government sought to obtain. As this Court noted in 2010, the “finding of relevance most crucially depended on the conclusion that bulk collection is *necessary* for NSA to employ tools that are likely to generate useful investigative leads to help identify and track terrorist operatives.” [REDACTED]

[REDACTED]

[REDACTED] Indeed, in [REDACTED] this Court noted that bulk collections such as these are “necessary to identify the much smaller number of [international terrorist] communications.” [REDACTED]

As a result, it is this showing of necessity that led the Court to find that “the entire mass of collected metadata is relevant to investigating [international terrorist groups] and affiliated persons.” [REDACTED]

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

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

This case is no different. The government stated, and this Court is well aware, that individuals associated with international terrorist organizations use telephonic systems to communicate with one another around the world, including within the United States. Ex. A. at 4. The government argues that the broad collection of telephone company metadata “is necessary to create a historical repository of metadata that enables NSA to find or identify known *and unknown* operatives ..., some of whom may be in the United States or in communication with U.S. persons.” App. at 6 (emphasis added). The government would use such information, in part, “to detect and prevent terrorist acts against the United States and U.S. interests.” Ex. A. at 3. The government posits that bulk telephonic metadata is necessary to its investigations because it is impossible to know where in the data the connections to international terrorist organizations will be found. *Id.* at 8-9. The government notes also that “[a]nalysts know that the terrorists’ communications are located somewhere” in the metadata produced under this authority, but cannot know where until the data is aggregated and then accessed by their analytic tools under limited and controlled queries. *Id.* As the government stated in its 2006 Memorandum of Law, “[a]ll of the metadata collected is thus relevant, because the success of this investigative tool depends on bulk collection.” Mem. of Law at 15, Docket No. BR 06-05.

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

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

The government depends on this bulk collection because if production of the information were to wait until the specific identifier connected to an international terrorist group were determined, most of the historical connections (the entire purpose of this authorization) would be lost. See Ex. A. at 7-12. The analysis of past connections is only possible "if the Government has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related." Mem. of Law at 2, Docket No. BR 06-05. Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity.

The government must demonstrate "facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." 50 U.S.C. 1861(b)(2)(A). The fact that international terrorist operatives are using telephone communications, and that it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, is sufficient to meet the low statutory hurdle set out in Section 215 to

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

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

obtain a production of records. Furthermore, it is important to remember that the relevance finding is only one part of a whole protective statutory scheme. Within the whole of this particular statutory scheme, the low relevance standard is counter-balanced by significant post-production minimization procedures that must accompany such an authorization and an available mechanism for an adversarial challenge in this Court by the record holder. See supra Part III.a. Without the minimization procedures set out in detail in this Court's Primary Order, for example, no Orders for production would issue from this Court. See Primary Ord. at 4-17. Taken together, the Section 215 provisions are designed to permit the government wide latitude to seek the information it needs to meet its national security responsibilities, but only in combination with specific procedures for the protection of U.S. person information that are tailored to the production and with an opportunity for the authorization to be challenged. The Application before this Court fits comfortably within this statutory framework.

c. Legislative Re-enactment or Ratification.

As the U.S. Supreme Court has stated, "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." Lorillard v. Pons, 434 U.S. 575, 580 (1978) (citing cases and authorities); see also Forest Grove Sch. Dist. v. T.A., 557 U.S. 230, 239-40 (2009) (quoting Lorillard, 434 U.S. at 580). This doctrine of legislative re-enactment,

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

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

also known as the doctrine of ratification, is applicable here because Congress re-authorized Section 215 of the PATRIOT Act without change in 2011. "PATRIOT Sunsets Extension Act of 2011," Pub. L. No. 112-14, 125 Stat. 216 (May 26, 2011).²² This doctrine applies as a presumption that guides a court in interpreting a re-enacted statute. See Lorillard, 434 U.S. at 580-81 (citing cases); NLRB v. Gullett Gin Co., 340 U.S. 361, 365-66 (1951) ("[I]t is a fair assumption that by reenacting without pertinent modification ... Congress accepted the construction ... approved by the courts."); 2B Sutherland on Statutory Construction § 49:8 and cases cited (7th ed. 2009). Admittedly, in the national security context where legal decisions are classified by the Executive Branch and, therefore, normally not widely available to Members of Congress for scrutiny, one could imagine that such a presumption would be easily overcome. However, despite the highly-classified nature of the program and this Court's orders, that is not the case here.

Prior to the May 2011 congressional votes on Section 215 re-authorization, the Executive Branch provided the Intelligence Committees of both houses of Congress with letters which contained a "Report on the National Security Agency's Bulk

²² The Senate and House of Representatives voted to re-authorize Section 215 for another four years by overwhelming majorities. See http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=112&session=1&vote=00084 (indicating a 72-23 vote in the Senate); and, <http://clerk.house.gov/evs/2011/roll376.xml> (indicating a 250-153 vote in the House). President Obama signed the re-authorization into law on May 26, 2011.

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

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

Collection Programs for USA PATRIOT Act Reauthorization" (Report). Ex. 3 (Letter to Hon. Mike Rogers, Chairman, and Hon. C.A. Dutch Ruppersberger, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives (HPSCI), from Ronald Weich, Asst. Attorney General (Feb. 2, 2011) (HPSCI Letter); and, Letter to Hon. Dianne Feinstein, Chairman, and Hon. Saxby Chambliss, Vice Chairman, Select Committee on Intelligence, U.S. Senate (SSCI), from Ronald Weich, Asst. Attorney General (Feb. 2, 2011) (SSCI Letter)). The Report provided extensive and detailed information to the Committees regarding the nature and scope of this Court's approval of the implementation of Section 215 concerning bulk telephone metadata.²³ The Report noted that "[a]lthough these programs have been briefed to the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about th[is] ... program[] when considering reauthorization of the

²³ Specifically, the Report provided the following information: 1) the Section 215 production is a program "authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls ... but not the content of the calls" Ex. 3, Report at 1 (emphasis in original); 2) this Court's "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," *id.* at 3 (emphasis added); 3) "Although the program[] collect[s] 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," *id.* at 1; 4) "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," *id.*; 5) "Although there have been compliance problems in recent years, the Executive Branch has worked to resolve them, subject to oversight by the FISA Court," *id.*; 6) "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" regarding a terrorist plot, *id.* at 2; 7) "NSA collects and analyzes large amounts of transactional data obtained from certain telecommunications service providers in the United States," *id.*; and, 8) that the program operates "on a very large scale." *Id.*

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

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

expiring PATRIOT Act provisions.” *Id.* Report at 3. Furthermore, the government stated the following in the HPSCI and SSCI Letters: “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....” *Id.* HPSCI Letter at 1; SSCI Letter at 1. It is clear from the letters that the Report would be made available to *all* Members of Congress and that HPSCI, SSCI, and Executive Branch staff would also be made available to answer any questions from Members of Congress.²⁴ *Id.* HPSCI Letter at 2; SSCI Letter at 2.

In light of the importance of the national security programs that were set to expire, the Executive Branch and relevant congressional committees worked together to ensure that *each* Member of Congress knew or had the opportunity to know how

²⁴ It is unnecessary for the Court to inquire how many of the 535 individual Members of Congress took advantage of the opportunity to learn the facts about how the Executive Branch was implementing Section 215 under this Court’s Orders. Rather, the Court looks to congressional action on the whole, not the preparatory work of individual Members in anticipation of legislation. In fact, the Court is bound to presume regularity on the part of Congress. *See City of Richmond v. J.A. Croson Co.*, 488 U.S. 469, 500 (1989) (“The factfinding process of legislative bodies is generally entitled to a presumption of regularity and deferential review by the judiciary.” (citing cases)). The ratification presumption applies here where each Member was presented with an opportunity to learn about a highly-sensitive classified program important to national security in preparation for upcoming legislative action. Furthermore, Congress as a whole may debate such legislation in secret session. *See* U.S. Const. art. I, Sec. 5. (“Each House may determine the Rules of its Proceedings, Each House shall keep a Journal of its Proceedings, and from time to time publish the same *excepting such Parts as may in their Judgment require Secrecy; ...*”) (emphasis added.). In fact, according to a Congressional Research Service Report, both Houses have implemented rules for such sessions pursuant to the Constitution. *See* “Secret Sessions of the House and Senate: Authority, Confidentiality, and Frequency” Congressional Research Service (Mar. 15, 2013), at 1-2 (citing House Rules XVII, cl. 9; X, cl. 11; and, Senate Rules XXI; XXIX; and, XXXI). Indeed, both Houses have entered into secret session in the past decade to discuss intelligence matters. *See id.* at 5 (Table 1. Senate “Iraq war intelligence” (Nov. 1, 2005); Table 2. House of Representatives “Foreign Intelligence Surveillance Act and electronic surveillance” (Mar. 13, 2008)).

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

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

Section 215 was being implemented under this Court's Orders.²⁵ Documentation and personnel were also made available to afford each Member full knowledge of the scope of the implementation of Section 215 and of the underlying legal interpretation.

The record before this Court thus demonstrates that the factual basis for applying the re-enactment doctrine and presuming that in 2011 Congress intended to ratify Section 215 as applied by this Court is well supported. Members were informed that this Court's "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." Ex. 3, Report at 3 (emphasis added). When Congress subsequently re-authorized Section 215 without change, except as to expiration date, that re-authorization carried with it this Court's interpretation of the statute, which permits the bulk collection of telephony metadata under the restrictions that are in place. Therefore, the passage of the PATRIOT Sunsets Extension Act

²⁵ Indeed, one year earlier when Section 215 was previously set to expire, SSCI Chairman Feinstein and Vice Chairman Bond sent a letter to every Senator inviting "each Member of the Senate" to read a very similar Report to the one provided in the 2011 Letters, and pointing out that this would "permit each Member of Congress access to information on the nature and significance of intelligence authority on which they are asked to vote." Ex. 7 ("Dear Colleague" Letter from SSCI Chairman Dianne Feinstein and Vice Chairman Christopher Bond (Feb. 23, 2010)). The next day, HPSCI Chairman Reyes sent a similar notice to each Member of the House that this information would be made available "on important intelligence collection programs made possible by these expiring authorities." Ex. 2 ("Dear Colleague" Notice from HPSCI Chairman Silvestre Reyes (Feb. 24, 2010)). This notice also indicated that the HPSCI Chairman and Chairman Conyers of the House Judiciary Committee would "make staff available to meet with any member who has questions" along with Executive Branch personnel. *Id.*

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

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

provides a persuasive reason for this Court to adhere to its prior interpretations of Section 215.

IV. Conclusion.

This Court is mindful that this matter comes before it at a time when unprecedented disclosures have been made about this and other highly-sensitive programs designed to obtain foreign intelligence information and carry out counter-terrorism investigations. According to NSA Director Gen. Keith Alexander, the disclosures have caused "significant and irreversible damage to our nation." Remarks at "Clear and Present Danger: Cyber-Crime; Cyber-Espionage; Cyber-Terror; and Cyber-War," Aspen, Colo. (Jul. 18, 2013). In the wake of these disclosures, whether and to what extent the government seeks to continue the program discussed in this Memorandum Opinion is a matter for the political branches of government to decide.

As discussed above, because there is no cognizable Fourth Amendment interest in a telephone company's metadata that it holds in the course of its business, the Court finds that there is no Constitutional impediment to the requested production. Finding no Constitutional issue, the Court directs its attention to the statute. The Court concludes that there are facts showing reasonable grounds to believe that the records sought are relevant to authorized investigations. This conclusion is supported not only by the plain text and structure of Section 215, but also by the statutory modifications

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

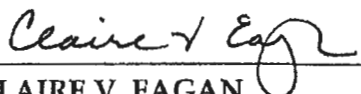
~~TOP SECRET//SI//NOFORN~~

and framework instituted by Congress. Furthermore, the Court finds that this result is strongly supported, if not required, by the doctrine of legislative re-enactment or ratification.

For these reasons, for the reasons stated in the Primary Order appended hereto, and pursuant to 50 U.S.C. § 1861(c)(1), the Court has GRANTED the Orders requested by the government.

Because of the public interest in this matter, pursuant to FISC Rule 62(a), the undersigned FISC Judge requests that this Memorandum Opinion and the Primary Order of July 19, 2013, appended herein, be published, and directs such request to the Presiding Judge as required by the Rule.

ENTERED this 29th day of August, 2013.



CLAIRE V. EAGAN
Judge, United States Foreign
Intelligence Surveillance Court

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

~~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 BR 13-80 and its predecessors. [50 U.S.C. § 1861(c)(1)]

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

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

Accordingly, and as further explained in a Memorandum Opinion to follow, 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]
[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. Furthermore, this Order does not authorize the production of cell site location information (CSLI).

~~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.

⁴ [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 queries of the BR metadata to obtain contact chaining information 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

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~~

adequate and 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~~

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

[REDACTED]

~~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] solely 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

~~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 [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}

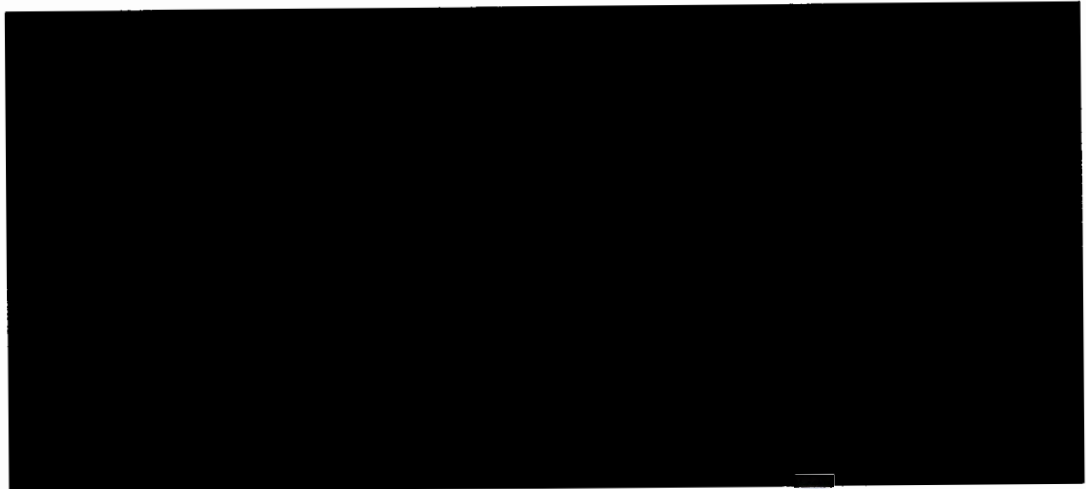
⁹ The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, 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.

¹⁰ The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to this Order. [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:

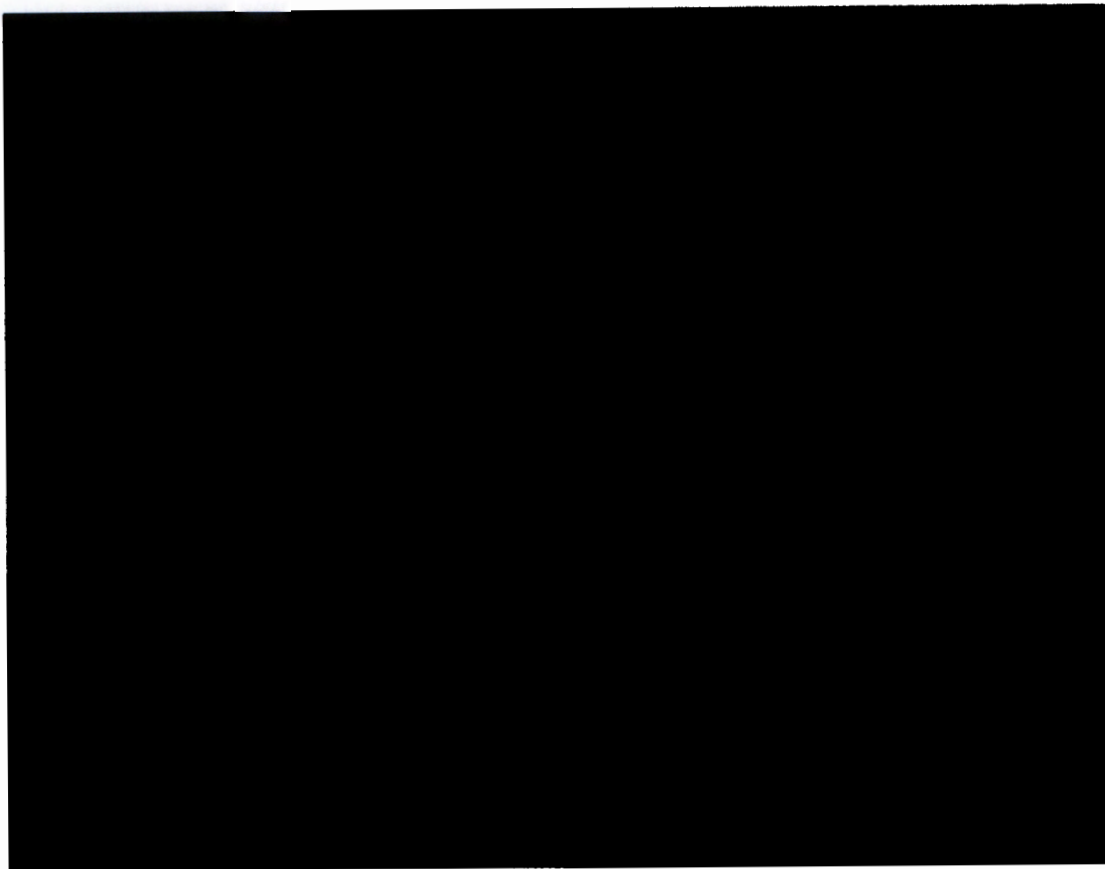


¹¹ This automated query process was initially approved by this Court in its November 8, 2012 Order amending docket number BR 12-178.

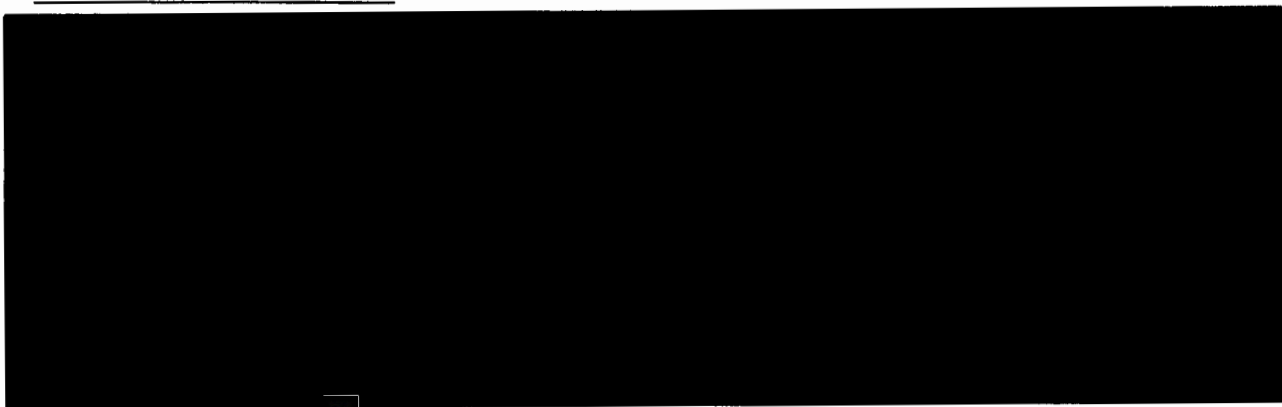
¹² As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms 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~~



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



~~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) Other than the automated query process described in the [REDACTED] Declaration and this Order, prior to implementation of any new or modified automated query processes, such new or modified 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 and operation 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

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

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

authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

This authorization regarding

[REDACTED]

expires on the 11th day

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

Signed _____ Eastern Time

10-9-13 10:45

Date Time

Claire V. Eagan

CLAIRE V. EAGAN
Judge, United States Foreign
Intelligence Surveillance Court

[REDACTED]

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

EXHIBIT D

~~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 [REDACTED]

[REDACTED]

Docket Number: BR 13-158

MEMORANDUM

The Court has today issued the Primary Order appended hereto granting the "Application for Certain Tangible Things for Investigations to Protect Against International Terrorism" ("Application"), which was submitted to the Court on October

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

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

10, 2013, by the Federal Bureau of Investigation ("FBI"). The Application requested the issuance of orders pursuant to 50 U.S.C. § 1861, as amended (also known as Section 215 of the USA PATRIOT Act), requiring the ongoing daily production to the National Security Agency ("NSA") of certain telephone call detail records in bulk.

The Primary Order appended hereto renews the production of records made pursuant to the similar Primary Order issued by the Honorable Claire V. Eagan of this Court on July 19, 2013 in Docket Number BR 13-109 ("July 19 Primary Order"). On August 29, 2013, Judge Eagan issued an Amended Memorandum Opinion setting forth her reasons for issuing the July 19 Primary Order ("August 29 Opinion"). Following a declassification review by the Executive Branch, the Court published the July 19 Primary Order and August 29 Opinion in redacted form on September 17, 2013.

The call detail records to be produced pursuant to the orders issued today in the above-captioned docket are identical in scope and nature to the records produced in response to the orders issued by Judge Eagan in Docket Number BR 13-109. The records will be produced on terms identical to those set out in Judge Eagan's July 19 Primary Order and for the same purpose, and the information acquired by NSA through the production will be subject to the same provisions for oversight and identical restrictions on access, retention, and dissemination.

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

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

This is the first time that the undersigned has entertained an application requesting the bulk production of call detail records. The Court has conducted an independent review of the issues presented by the application and agrees with and adopts Judge Eagan's analysis as the basis for granting the Application. The Court writes separately to discuss briefly the issues of "relevance" and the inapplicability of the Fourth Amendment to the production.

Although the definition of relevance set forth in Judge Eagan's decision is broad, the Court is persuaded that that definition is supported by the statutory analysis set out in the August 29 Opinion. That analysis is reinforced by Congress's re-enactment of Section 215 after receiving information about the government's and the FISA Court's interpretation of the statute. Although the existence of this program was classified until several months ago, the record is clear that before the 2011 re-enactment of Section 215, many Members of Congress were aware of, and each Member had the opportunity to learn about, the scope of the metadata collection and this Court's interpretation of Section 215. Accordingly, the re-enactment of Section 215 without change in 2011 triggered the doctrine of ratification through re-enactment, which provides a strong reason for this Court to continue to adhere to its prior interpretation of Section 215. See Lorillard v. Pons, 434 U.S. 575, 580 (1978); see also EEOC v. Shell Oil Co., 466 U.S. 54, 69 (1984); Haig v. Agee, 453 U.S. 280, 297-98 (1981).

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

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

The undersigned also agrees with Judge Eagan that, under Smith v. Maryland, 442 U.S. 735 (1979), the production of call detail records in this matter does not constitute a search under the Fourth Amendment. In Smith, the Supreme Court held that the use of a pen register to record the numbers dialed from the defendant's home telephone did not constitute a search for purposes of the Fourth Amendment. In so holding, the Court stressed that the information acquired did not include the contents of any communication and that the information was acquired by the government from the telephone company, to which the defendant had voluntarily disclosed it for the purpose of completing his calls.

The Supreme Court's more recent decision in United States v. Jones, — U.S. —, 132 S. Ct. 945 (2012), does not point to a different result here. Jones involved the acquisition of a different type of information through different means. There, law enforcement officers surreptitiously attached a Global Positioning System (GPS) device to the defendant's vehicle and used it to track his location for 28 days. The Court held in Justice Scalia's majority opinion that the officers' conduct constituted a search under the Fourth Amendment because the information at issue was obtained by means of a physical intrusion on the defendant's vehicle, a constitutionally-protected area. The majority declined to decide whether use of the GPS device, without the physical intrusion, impinged upon a reasonable expectation of privacy.

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

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

Five Justices in Jones signed or joined concurring opinions suggesting that the precise, pervasive monitoring by the government of a person's location could trigger Fourth Amendment protection even without any physical intrusion. This matter, however, involves no such monitoring. Like Smith, this case concerns the acquisition of non-content metadata other than location information. See Aug. 29 Op. at 29 at 4 n.5; id. at 6 & n.10.

Justice Sotomayor stated in her concurring opinion in Jones that it "may be necessary" for the Supreme Court to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," which she described as "ill suited to the digital age." See Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing Smith and United States v. Miller, 425 U.S. 435, 443 (1976), as examples of decisions relying upon that premise). But Justice Sotomayor also made clear that the Court undertook no such reconsideration in Jones. See id. ("Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision."). The Supreme Court may some day revisit the third-party disclosure principle in the context of twenty-first century communications technology, but that day has not arrived. Accordingly, Smith remains controlling with respect to the acquisition by the government from service providers of non-content telephony


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

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

metadata such as the information to be produced in this matter.

In light of the public interest in this matter and the government's declassification of related materials, including substantial portions of Judge Eagan's August 29 Opinion and July 19 Primary Order, the undersigned requests pursuant to FISC Rule 62 that this Memorandum and the accompanying Primary Order also be published and directs such request to the Presiding Judge as required by the Rule.

ENTERED this 11th day of October, 2013.


MARY A. McLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

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

Page 6

~~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 BR 13-109 and its predecessors. [50 U.S.C. § 1861(c)(1)]

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

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

Accordingly, and as further explained in the accompanying Memorandum, 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]

[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. Furthermore, this Order does not authorize the production of cell site location information (CSLI).

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

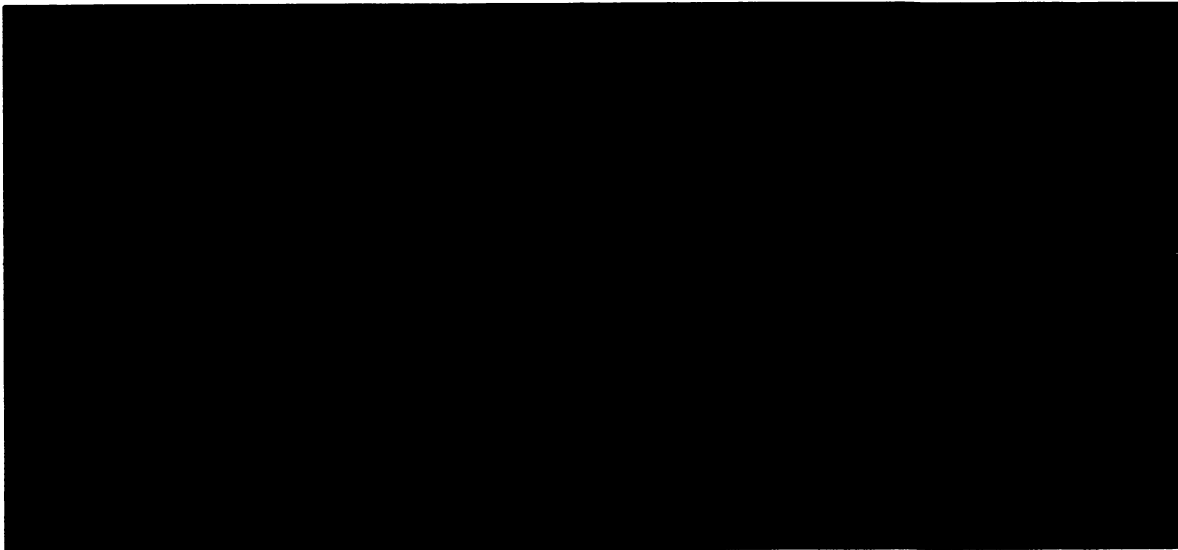
~~TOP SECRET//SI//NOFORN~~

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.



~~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 queries of the BR metadata to obtain contact chaining information as described in paragraph 17 of the Declaration of [REDACTED] [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,

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~~

through adequate and 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]

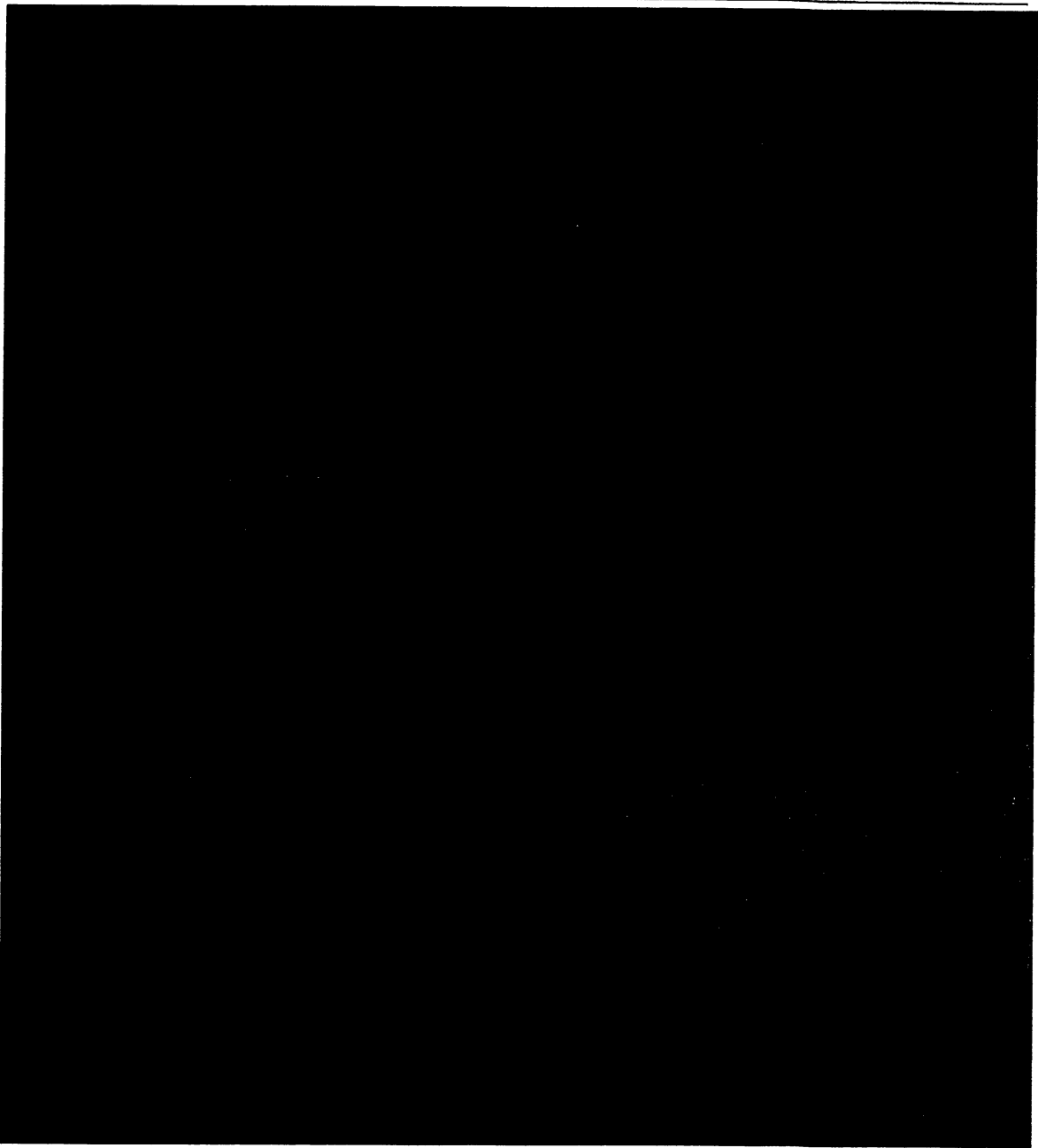
[REDACTED]

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

~~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] solely 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] 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

~~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}

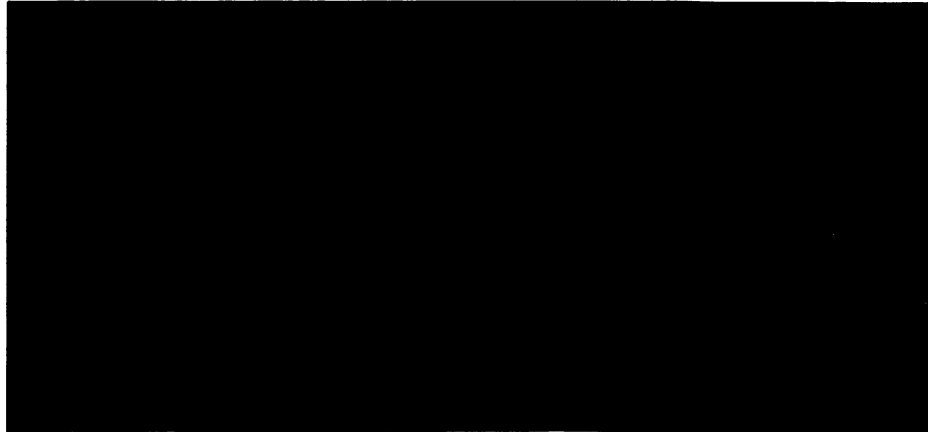
⁹ The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, 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.

¹⁰ The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to this Order [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:

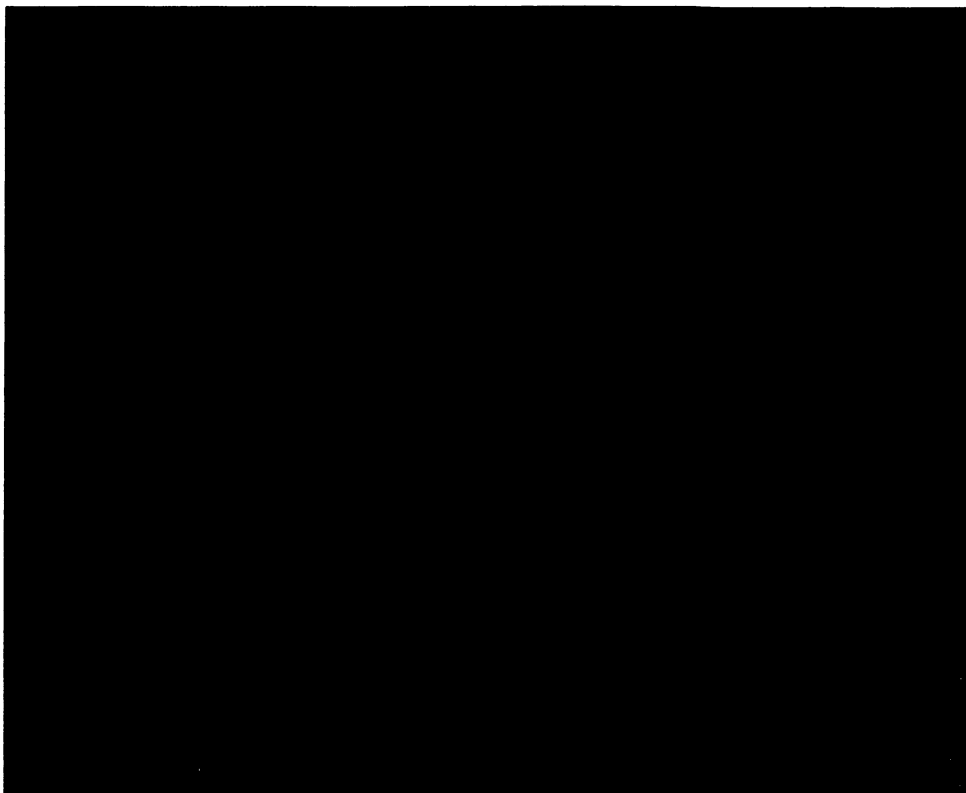


¹¹ This automated query process was initially approved by this Court in its November 8, 2012 Order amending docket number BR 12-178.

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~~



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



~~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) Other than the automated query process described in the [REDACTED] Declaration and this Order, prior to implementation of any new or modified automated query processes, such new or modified 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 and operation 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.

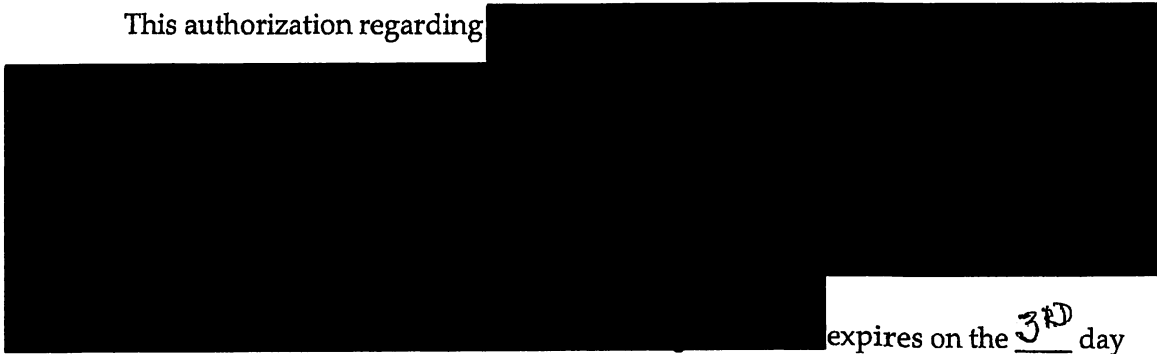
Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials

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

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

authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

This authorization regarding



expires on the 3rd day

of January, 2014, at 5:00 p.m., Eastern Time.

Signed _____ Eastern Time
10-11-2013 P12:05
Date Time

Mary A. McLaughlin
MARY A. MCLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

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

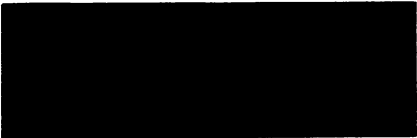


EXHIBIT E

~~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 [REDACTED]

[REDACTED]

Docket Number: BR

13 - 8 0

PRIMARY ORDER

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]
[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]

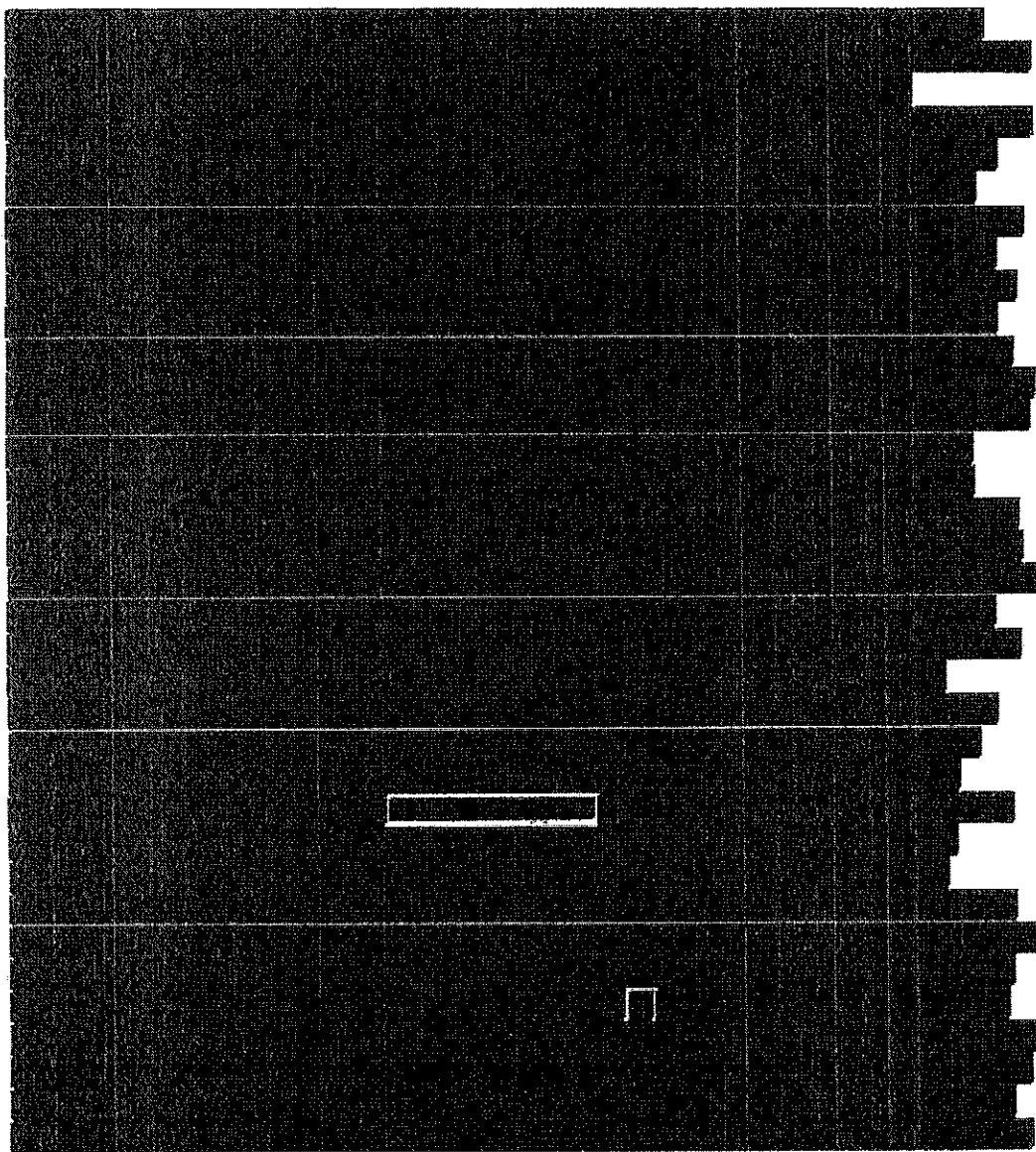
⁶ This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[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]

~~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]

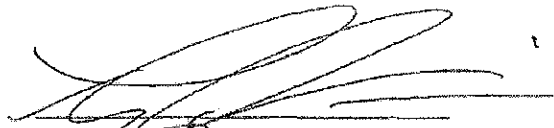
[REDACTED]

[REDACTED]

[REDACTED] expires on the 19th day

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

Signed 04-25-2013 02:26 Eastern Time
Date Time



ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

[REDACTED]

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

EXHIBIT F

~~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.

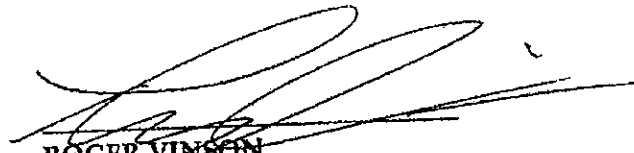
-- Remainder of page intentionally left blank. --

~~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 _____ Eastern Time
Date Time
 04-25-2013 10:26


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 G

~~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 H

~~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.  and
- ~~(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 Qaeda 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]

Although these programs have been briefed to [REDACTED]

~~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]. 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 I

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

JOHN D. ROCKEFELLER IV, WEST VIRGINIA
RON WYDEN, OREGON
EVAN BAYNE, 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

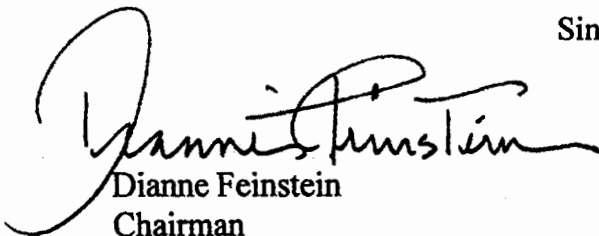
Dear Colleague:

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 J

USA Patriot Act

From: The Permanent Select Committee on Intelligence
Sent By: Khizer.Sved@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 K

~~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~~

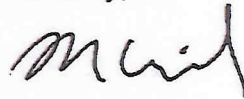
~~TOP SECRET//COMINT//NOFORN~~

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 L

~~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 Ruppertsberger
Ranking Minority Member
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman and Congressman Ruppertsberger:

~~(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 M

~~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 Qaeda 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]

[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]

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] 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]

[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 N

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

SCI#

2011 - 0823

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

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

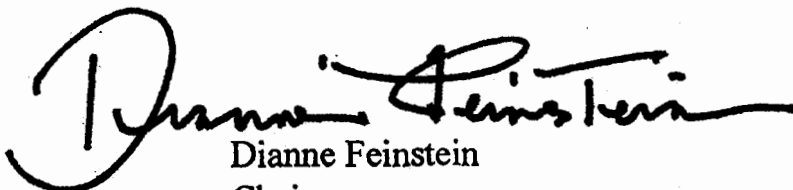
Dear Colleague:

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


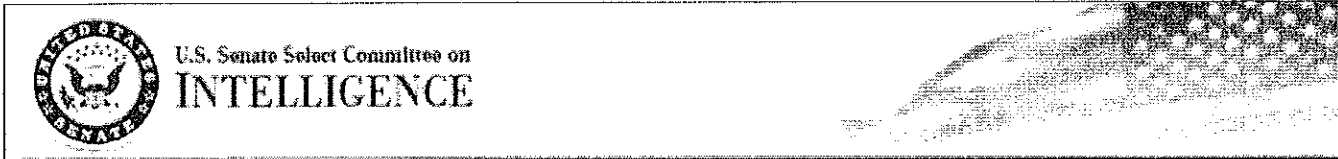

Saxby Chambliss
Vice Chairman

EXHIBIT O



Home Members Legislation Hearings Publications Laws/Executive Orders Press About Links

Press Releases



- [113th Congress](#)
(2013-2014)
- [112th Congress](#)
(2011-2012)
- [111th Congress](#)
(2009-2010)
- [110th Congress](#)
(2007-2008)
- [109th Congress](#)
(2005-2006)
- [108th Congress](#)
(2003-2004)
- [107th Congress](#)
(2001-2002)

Press Release of Intelligence Committee

Feinstein, Chambliss Statement on NSA Phone Records Program

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

Thursday, June 6, 2013

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

“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.

“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 P

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 suspicious 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...

RUPPERTSBERGER: 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 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

EXHIBIT Q

FILED

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

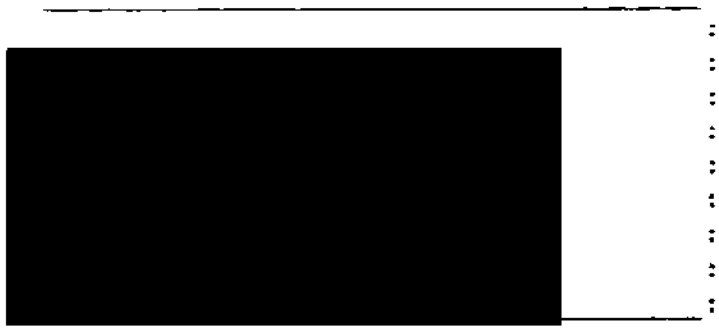


U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.



:
:
:
:
:
:
:
:
:
:
:

Docket Number: PR/TT

OPINION AND ORDER

This matter comes before the Court on an application of the Government for authority for the National Security Agency (NSA) to collect information regarding e-mail and certain other forms of Internet communications under the pen register and trap and trace provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States Code (U.S.C.), §§ 1801-1811, 1841-1846. This application seeks authority for a

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

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

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

much broader type of collection than other pen register/trap and trace applications and therefore presents issues of first impression.¹ For that reason, it is appropriate to explain why the Court concludes that the application should be granted as modified herein.

Accordingly, this Opinion and Order sets out the bases for the Court's findings that: (1) the collection activities proposed in the application involve the installation and use of "pen registers" and/or "trap and trace devices" as those terms are used in FISA, 50 U.S.C. §§ 1841-1846; (2) the application, which specifies restrictions on the retention, accessing, use, and dissemination of information obtained from these collection activities, "satisfies the requirements" of 50 U.S.C. § 1842 for the issuance of an order "approving the installation and use of a pen register or trap and trace device," *id.* § 1842(d)(1), subject to modifications stated herein;² and (3) the installation and use of these pen registers and/or trap and trace devices pursuant to

¹ The application was filed in two steps: an application filed on [REDACTED] followed by an addendum filed on [REDACTED]. For ease of reference, the following discussion refers to both submissions collectively as the application.

² The Court has authority in this case to "enter an ex parte order as requested, or as modified." 50 U.S.C. § 1842(d)(1).

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

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

this Opinion and Order will comply with the First and Fourth Amendments.

In making these findings, the Court relies on factual representations made in the application, which was submitted by the Attorney General as applicant and verified by the Director of the NSA (DIRNSA); in the separate declaration of the DIRNSA (Attachment A to the application); and in the declaration of the [REDACTED] (Attachment B to the application). The Court has given careful consideration to the arguments presented in the Government's memorandum of law and fact (Attachment C to the application).

By letter dated [REDACTED] the Court directed the Government to respond to two questions necessary to its ruling on this application. The Court relies on the Government's responses to these questions, which were provided in a letter submitted on [REDACTED]

The Court also relies on information and arguments presented in a briefing to the Court on [REDACTED] which addressed the current and near-term threats posed by [REDACTED]

³ One of these questions concerned First Amendment issues presented by the application. The other concerned the length of time that the Government expected the collected information to retain operational significance. These questions and the Government's responses are discussed more fully below.

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

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

[REDACTED] investigations conducted by the Federal Bureau of Investigation (FBI) to counter those threats, the proposed collection activities of the NSA (now described in the instant application), the expected analytical value of information so collected in efforts to identify and track operatives [REDACTED] [REDACTED] and the legal bases for conducting these collection activities under FISA's pen register/trap and trace provisions.⁴

The principal statutory issues in this matter are whether the proposed collection constitutes the installation and use of "pen registers" and/or "trap and trace devices" and, if so, whether the certification pursuant to 50 U.S.C. § 1842(c)(2) is adequate. These issues are addressed below.

I. THE PROPOSED COLLECTION IS A FORM OF PEN REGISTER AND TRAP AND TRACE SURVEILLANCE.

For purposes of 50 U.S.C. §§ 1841-1846, FISA adopts the definitions of "pen register" and "trap and trace device" set out

⁴ This briefing was attended by (among others) the Attorney General; [REDACTED] the DIRNSA; the Director of the FBI; the Counsel to the President; the Assistant Attorney General for the Office of Legal Counsel; the Director of the Terrorist Threat Integration Center (TTIC); and the Counsel for Intelligence Policy.

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

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

in 18 U.S.C. § 3127. See 50 U.S.C. § 1841(2). Section 3127 gives the following definitions:

(3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of business;

(4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

These definitions employ three other terms - "electronic communication," "wire communication," and "contents" - that are themselves governed by statutory definitions "set forth for such terms in section 2510" of title 18. 18 U.S.C. § 3127(1).

Section 2510 defines these terms as follows:

(1) "Electronic communication" is defined at 18 U.S.C. § 2510(12) as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole

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

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

or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include - (A) any wire or oral communication."⁵

(2) "Wire communication" is defined at 18 U.S.C. § 2510(1)

as

any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

(3) "Contents" is defined at 18 U.S.C. § 2510(8) to

"include[] any information concerning the substance, purport, or meaning" of a "wire, oral, or electronic communication."⁶

While the definitions of "pen register" and "trap and trace device" each contain several elements, the application of these

⁵ The other exclusions to this definition at § 2510(12)(B)-(D) are not relevant to this case.

⁶ Different definitions of "wire communication" and "contents" are provided at 50 U.S.C. § 1801(1), (n). However, the definitions set forth in § 1801 apply to terms "[a]s used in this subchapter," *i.e.*, in 50 U.S.C. §§ 1801-1811 (FISA subchapter on electronic surveillance), and thus have no bearing on the meaning of "wire communication" and "contents" as used in the definitions of "pen register" and "trap and trace device" applicable to §§ 1841-1846 (separate FISA subchapter on pen registers and trap and trace devices).

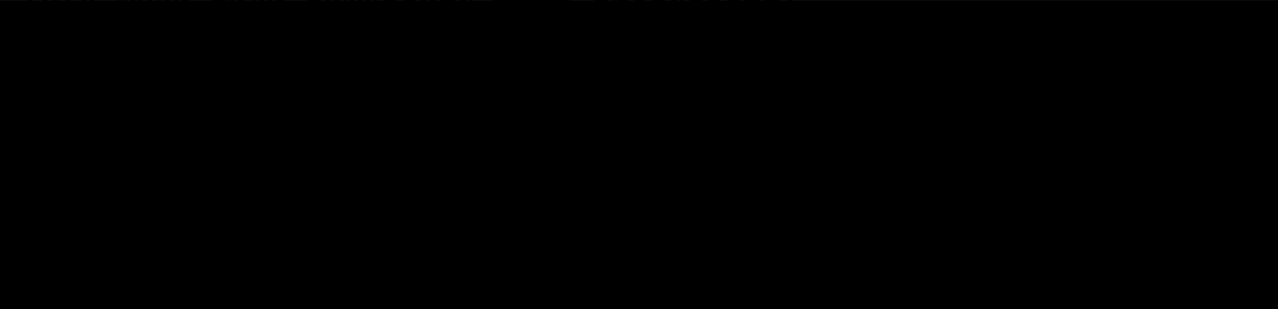
~~TOP SECRET//HCS//COMINT//NOFORN~~

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

definitions to the devices described in the application presents two primary questions: (1) Does the information to be obtained constitute "dialing, routing, addressing, or signaling information" that does not include the "contents" of any communication? (2) Does the means by which such information would be obtained come within the definition of "pen register" or "trap and trace device?" In addressing these questions, the Court is mindful that "when the statute's language is plain, the sole function of the courts - at least where the disposition required by the text is not absurd - is to enforce it according to its terms." Lamie v. United States Trustee, 124 S. Ct. 1023, 1030 (2004) (internal quotations and citations omitted).

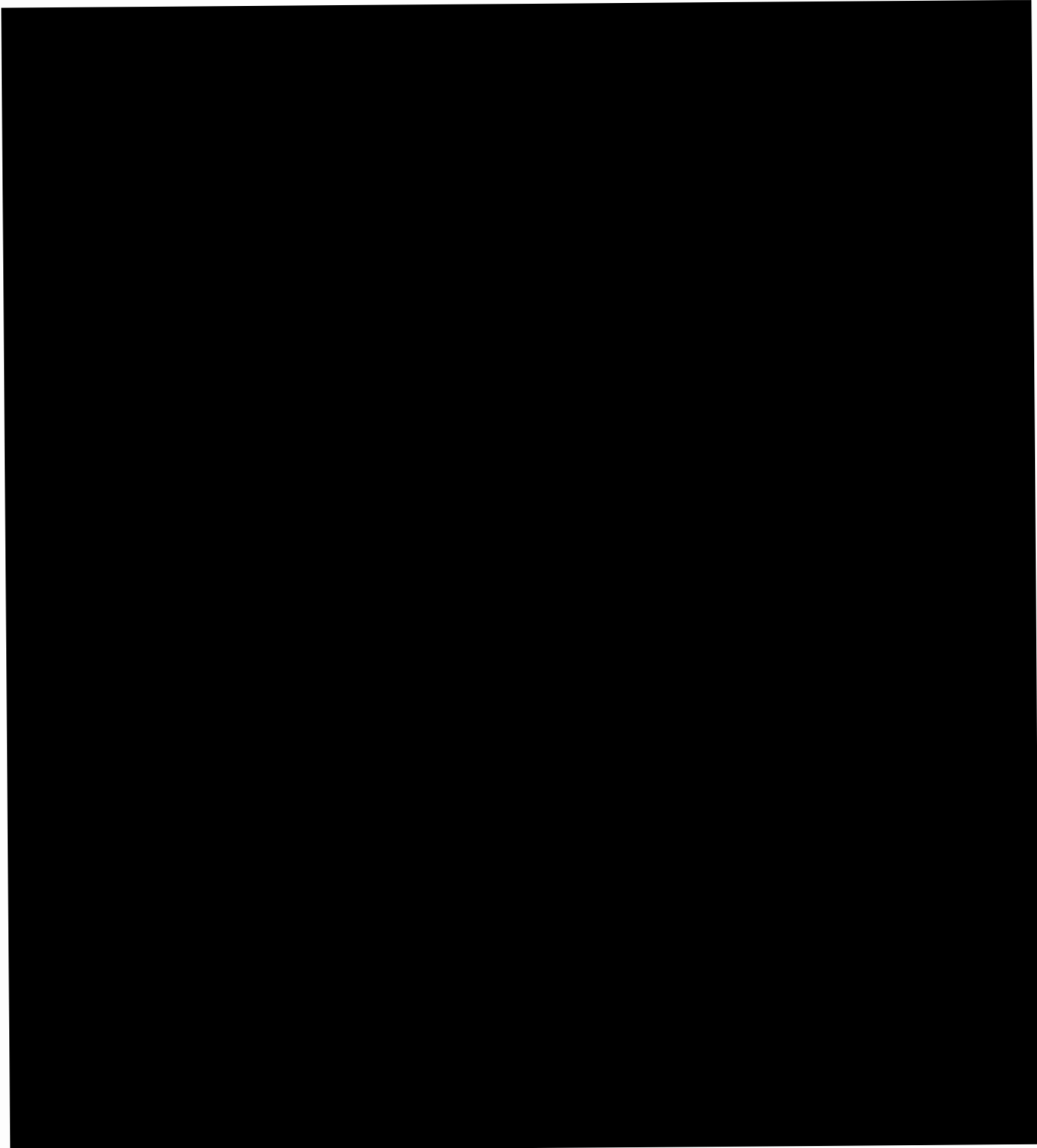
A. The Information to Be Obtained Is "Dialing, Routing, Addressing, or Signaling Information" and Not "Contents."

The Government uses the umbrella term "meta data" to designate the categories of information it proposes to collect. This meta data comprises [REDACTED] categories:



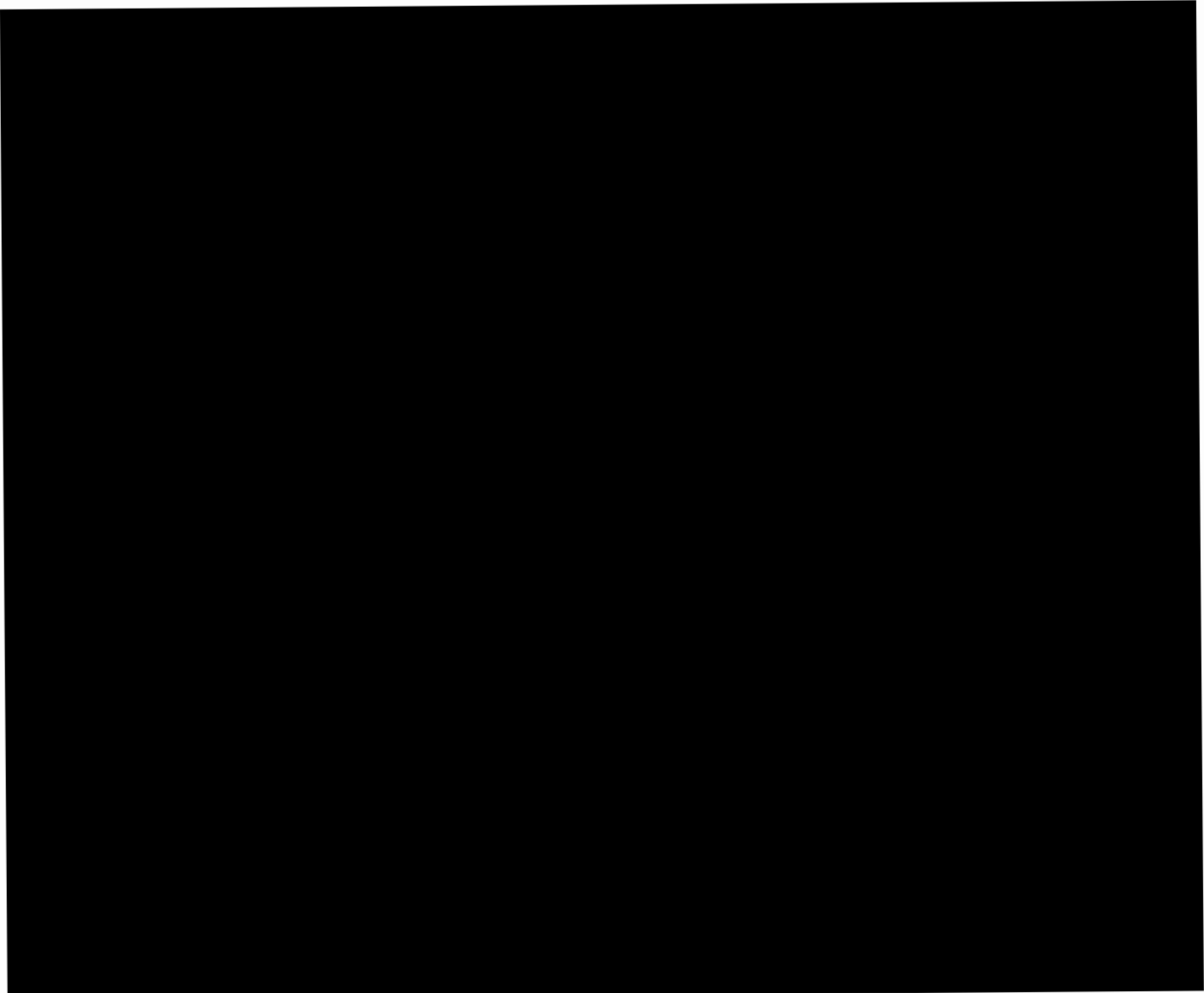
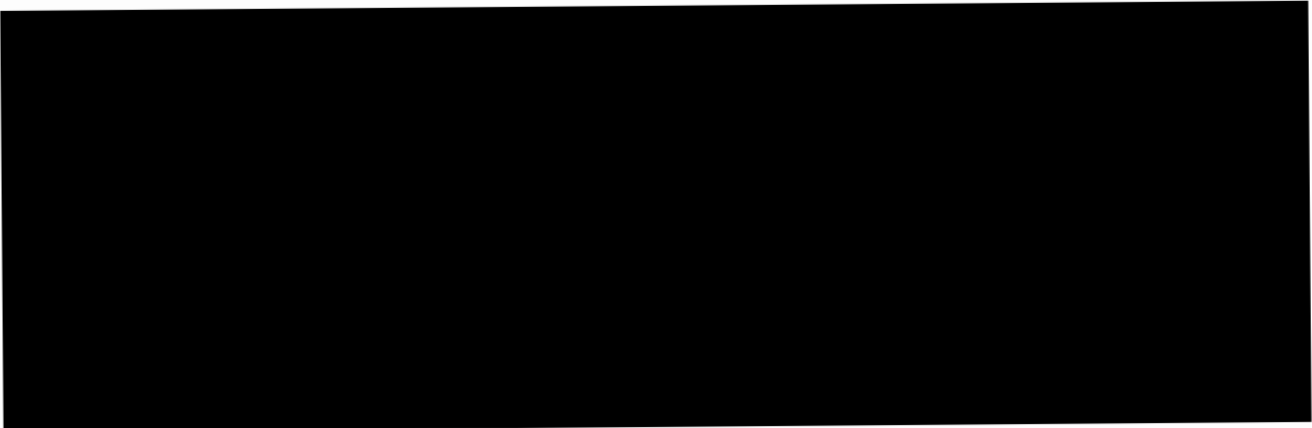
~~TOP SECRET//HCS//COMINT//NOFORN~~

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



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

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



TOP SECRET//HCS//COMINT//NOFORN

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

[REDACTED]

[REDACTED]

Also, the address from which an e-mail was sent and [REDACTED]

[REDACTED] are not part of the e-mail's "contents."

⁸ This is the first application presented to this Court for authority to [REDACTED] under pen register/trap and trace authority. The Court understands that FBI devices implementing prior pen register/trap and trace surveillance authorized by this Court have not obtained [REDACTED]. See Memorandum of Law and Fact at 23-24 n.14. The fact that prior applications did not seek authority for this specific form of collection sheds no light on the merits of the instant application.

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

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

B. The Methods By Which NSA Proposes to Obtain This Information Involve the Use of "Pen Registers" and "Trap and Trace Devices."

NSA proposes to obtain meta data in the above-described Categories [REDACTED]

[REDACTED]

[REDACTED]

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

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

[REDACTED]

Because the application of the definitions of "pen register" and "trap and trace device" to this means of collection involves a similar analysis for meta data in Categories [REDACTED] [REDACTED] [REDACTED]

[REDACTED], these groups of information are discussed separately below.

1. The Methods of Collecting Categories [REDACTED] [REDACTED] Fall Within the Plain Meaning of the Statutory Definitions.

The above-described means of collecting information in Categories [REDACTED] [REDACTED] [REDACTED] satisfies each of the elements of the applicable statutory definition of a "pen register." It consists of "a device or process which records or decodes" non-content routing or addressing information "transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). [REDACTED]

[REDACTED]

¹¹ "Transmit" means "1. To convey or dispatch from one person, thing, or place to another. . . . 4. Electron. To send (a signal), as by wire or radio." Webster's II New College Dictionary 1171 (2001).

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

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

Finally, the proposed collection does not involve "any device or process used . . . for billing, or recording as an incident to billing, for communications services . . . or . . . for cost accounting or other like purposes," which is excluded from the definition of "pen register" under section 3127(3).

Accordingly, based on "the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose," Engine Mfrs. Ass'n v. South Coast Air Quality Mgmt. Dist., 124 S. Ct. 1756, 1761 (2004) (internal quotations and citation omitted), the Court concludes that the means by which the NSA proposes to collect

¹² For ease of reference, this Opinion and Order generally speaks of "electronic communications." The communication involved will usually be an "electronic communication" under the above-quoted definition at 18 U.S.C. § 2510(12). In the event that the communication consists of an "aural transfer," *i.e.*, "a transfer containing the human voice at any point between and including the point of origin and the point of reception," *id.* § 2510(18), then it could fall instead under the above-quoted definition of "wire communication" at § 2510(1). In either case, the communication would be "a wire or electronic communication," as required to fall within the definitions at §§ 3127(3) and 3127(4).

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

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

meta data in Categories [REDACTED] [REDACTED] [REDACTED] above falls under the definition of "pen register" at section 3127(3).

The application also seeks authority to collect at least some of the same meta data by the same means under the rubric of a "trap and trace device" as defined at section 3127(4).

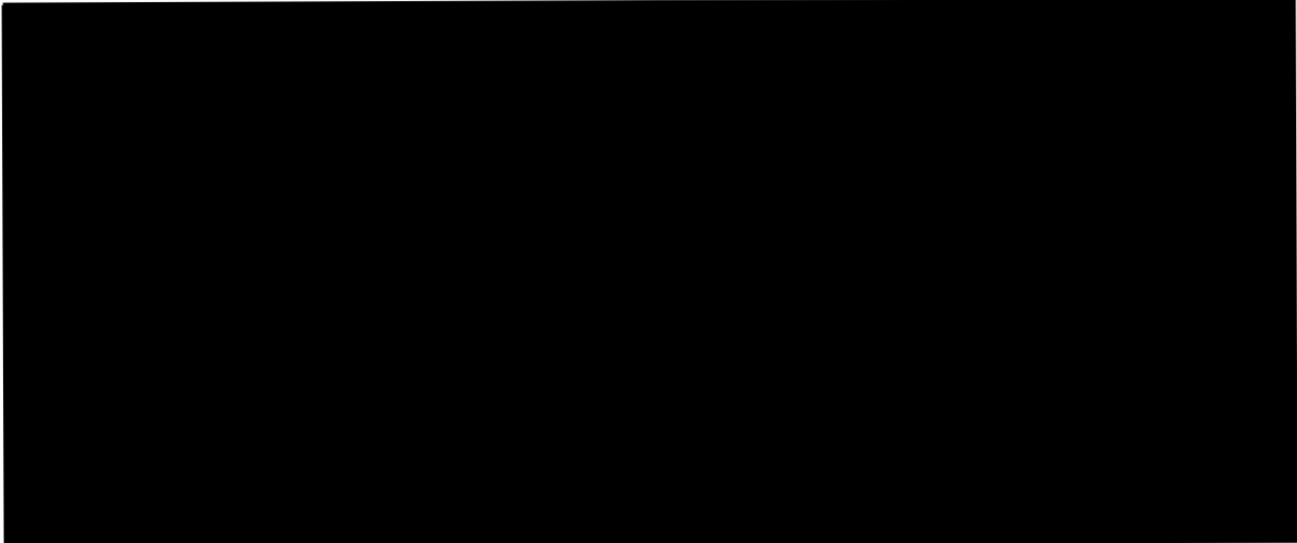
Although it appears to the Court that all of the collection authorized herein comes within the definition of "pen register," the Court additionally finds that such collection, as it pertains to meta data in Categories [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED] (for example, information from the "from" line of an e-mail), also satisfies the definition of "trap and trace device" under section 3127(4).

Under section 3127(4), a "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other [non-content] dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." As discussed above, the proposed collection would use a device or process to obtain non-content meta data [REDACTED]

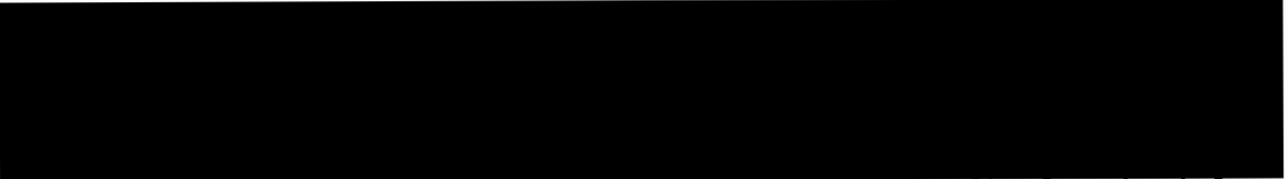
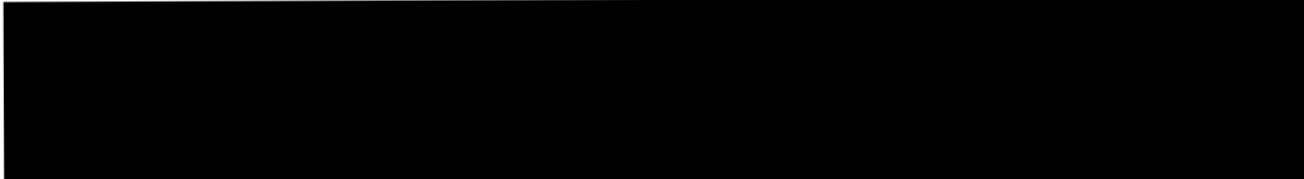
~~TOP SECRET//HCS//COMINT//NOFORN~~

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

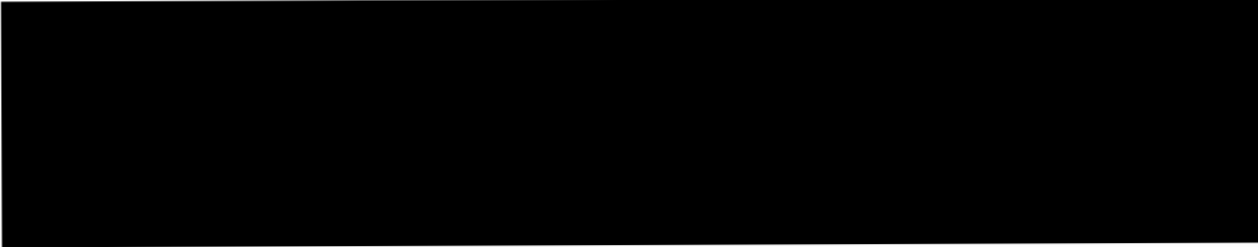


Thus, based on the plain meaning of

¹³ "Capture" is defined as, inter alia, " . . . 3. To succeed in preserving in a permanent form." Webster's II New College Dictionary 166 (2001).



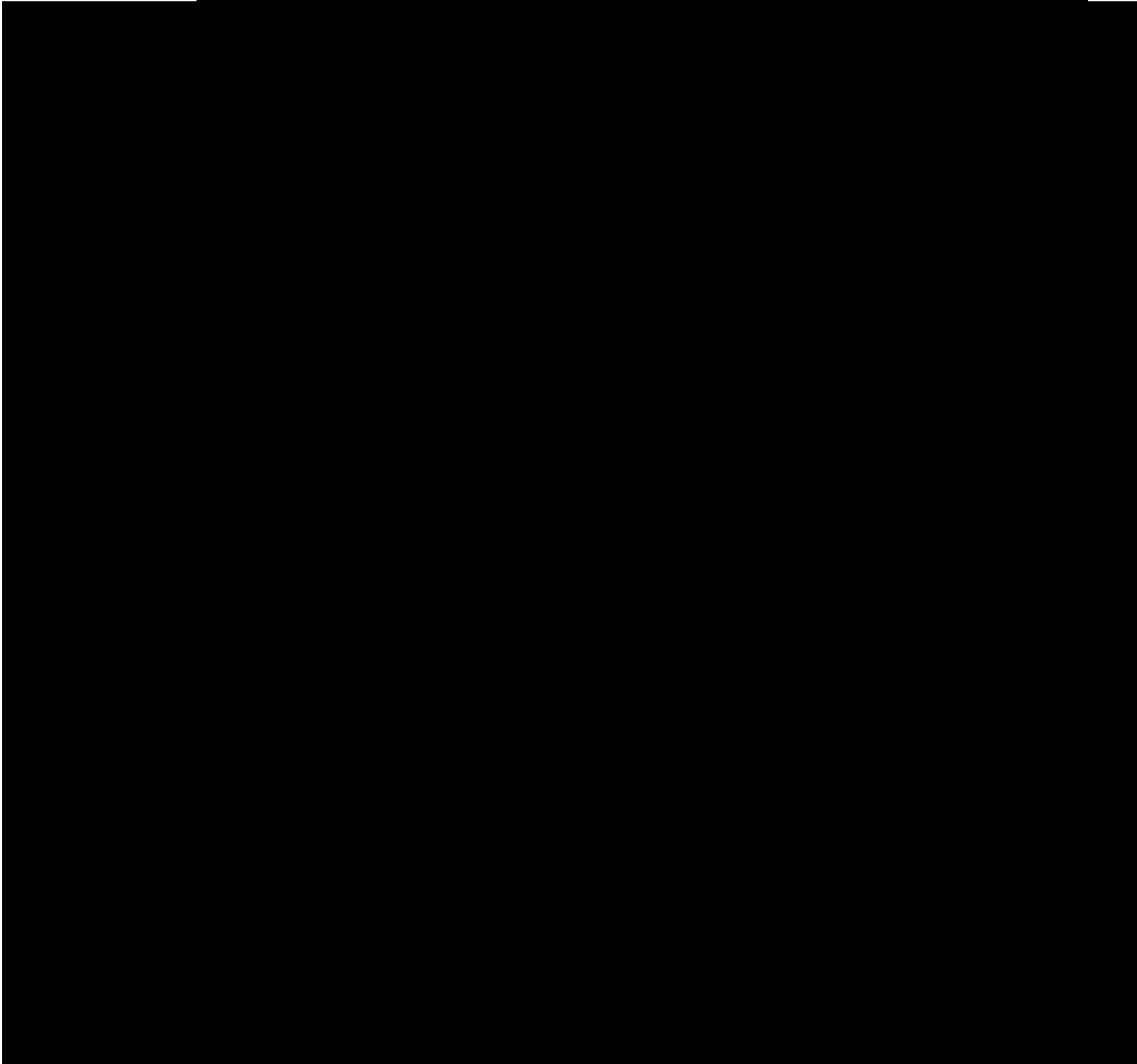
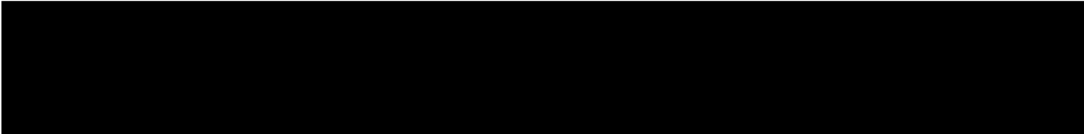
Such a result could be argued to violate the "cardinal principle of statutory construction that we must give effect, if possible, to every clause and word of a statute." Williams v. Taylor, 529 U.S. 362, 404 (2000) (internal quotations and citation omitted).



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

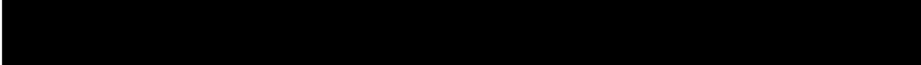
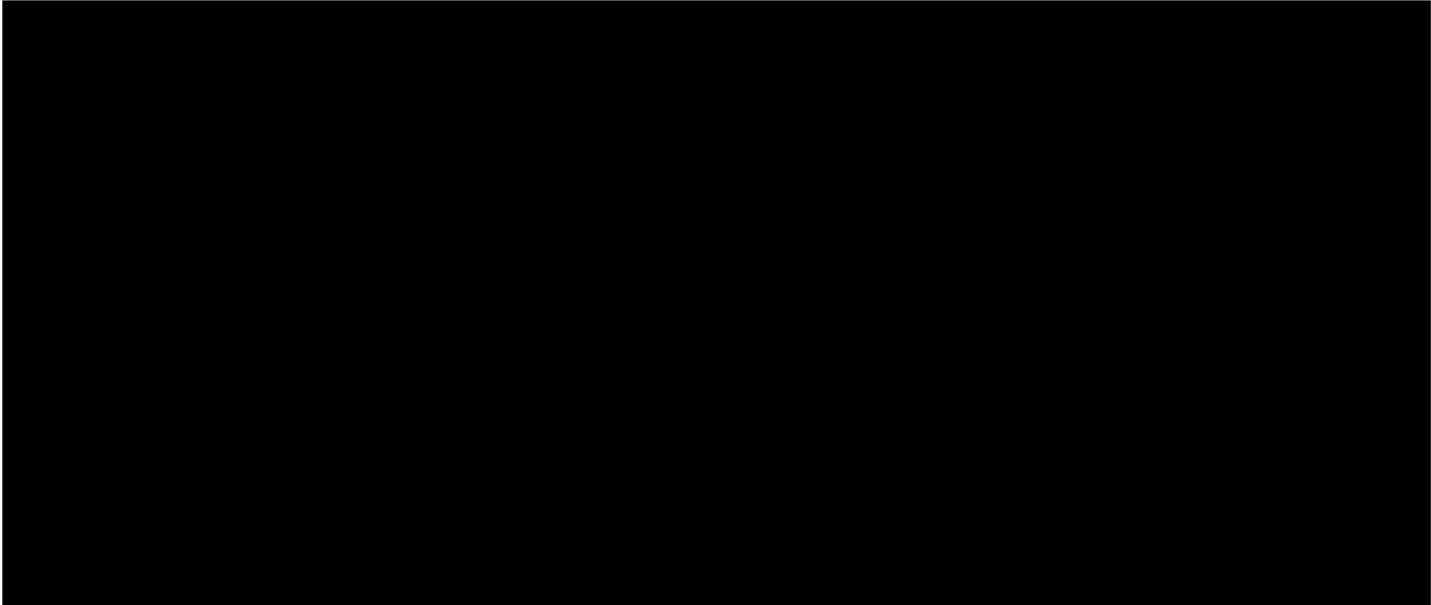
~~TOP SECRET//HCS//COMINT//NOFORN~~

the applicable definitions, the proposed collection involves a form of both pen register and trap and trace surveillance.



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

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



The Court


accordingly finds that the plain meaning of sections 3127(3) and 3127(4) encompasses the proposed collection of meta data.


Alternatively, the Court finds that any ambiguity on this point should be resolved in favor of including this proposed collection within these definitions, since such an interpretation would promote the purpose of Congress in enacting and amending FISA regarding the acquisition of non-content addressing information. Congress amended FISA in 1998, and again in 2001,

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

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

to relax the requirements for Court-authorized surveillance to obtain non-content addressing information through pen register and trap-and-trace devices, recognizing that such information is not protected by the Fourth Amendment. See page 29 below. As part of the USA PATRIOT Act in 2001, Congress also amended FISA to provide for Court orders for the production of "any tangible things," such as business records, under the same relevance standard as was adopted for pen register/trap and trace authorizations. See Pub. L. No. 107-56, Title II, § 215, 115 Stat. 290, codified at 50 U.S.C. § 1861.

 like other forms of meta data, is not protected by the Fourth Amendment because users of e-mail do not have a reasonable expectation of privacy in such information. See pages 59-62 below. It is a form of non-content addressing information, which Congress has determined should receive a limited form of statutory protection under a relevance standard if obtained through pen register/trap and trace devices pursuant to 50 U.S.C. § 1842, and/or through compelled production of business records (e.g., toll records for long-distance phone calls) under 50 U.S.C. § 1861.

A narrow reading of the definitions of "pen register" and "trap-and-trace device" to exclude  would

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

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

remove this particular type of non-content addressing information from the statutory framework that Congress specifically created for it. Based on such a narrow interpretation, this information could not be collected through pen register/trap and trace surveillance, even where it unquestionably satisfies the relevance standard. Nor could this information be obtained under the business records provision, because it is not generally retained by communications service providers. See page 41 below.

There is no indication that Congress believed that the availability of non-content addressing information under the relevance standard should hinge on the technical means of collection. If anything, the legislative history, see 147 Cong. Rec. S11000 (daily ed. Oct. 25, 2001) (statement of Sen. Patrick Leahy) (supporting clarification of "the statute's proper application to tracing communications in an electronic environment . . . in a manner that is technology neutral"), and the adoption of an identical relevance standard for the production of business records and other tangible things under section 1861, suggest otherwise.

Accordingly, the Court alternatively finds that, if the application of sections 3127(3) and 3127(4) to the [REDACTED] [REDACTED] were thought to be ambiguous, such

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

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

ambiguity should be resolved in favor of an interpretation of the definitions of "pen register" and "trap and trace device" that encompasses the proposed collection.

3. The Proposed Collection is Consistent With Other Provisions of FISA

Nothing that is fairly implied by other provisions of FISA governing pen register and trap and trace surveillance would prevent authorization of the proposed collection as a form of pen register/trap and trace surveillance. One provision requires that an order authorizing a pen register or trap and trace surveillance specify "the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." 50 U.S.C. § 1842(d)(2)(A)(ii). Plainly, there is no requirement to state the identity of such a person if it is not "known." However, this provision might still be read to imply that Congress expected that such facilities would be leased or listed to some particular person, even if the identity of that person were unknown in some cases. However, even if Congress had such a general expectation, the language of the statute does not require that there be such a person for every facility to which a pen register or trap and trace device is to be attached or applied. Drawing the contrary conclusion

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

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

from the wording of § 1842(d)(2)(A)(ii) would make the applicability of the statute depend on the commercial or administrative practices of particular communications service providers - a result that here would serve no apparent purpose of Congress. Cf. Smith v. Maryland, 442 U.S. 735, 745 (1979) (finding that the "fortuity of whether or not the phone company elects to make [for its own commercial purposes] a quasi-permanent record of a particular number dialed" is irrelevant to whether the Fourth Amendment applies to use of a pen register).¹⁶

In this case [REDACTED]

[REDACTED]

¹⁶ Similarly, for purposes of the subchapter on pen register/trap and trace surveillance, FISA defines an "aggrieved person," in relevant part, as any person "whose communication instrument or device was subject to the use of a pen register or trap and trace device . . . to capture incoming electronic or other communications impulses." 50 U.S.C. § 1841(3)(B). The term "whose" suggests a relationship between some person and "a communication instrument or device" that was "subject to the use of a pen register or trap and trace device." [REDACTED]

[REDACTED] Indeed, the use of different language implies that these phrases can refer to different objects, so that the definition of "aggrieved person" sheds no light on whether a "facility" under § 1842(d)(2)(A)(ii)-(iii) is necessarily associated with an individual user.

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

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

The

Court is satisfied that this Opinion and Order complies with the specification requirements of § 1842(d)(2)(A).

The Court recognizes that, by concluding that these definitions do not restrict the use of pen registers and trap and trace devices to communication facilities associated with individual users, it is finding that these definitions encompass an exceptionally broad form of collection. Perhaps the opposite result would have been appropriate under prior statutory language.¹⁷ However, our "starting point" must be "the existing

¹⁷ Prior to amendments in 2001 by the USA PATRIOT Act, Public Law 107-56, Title II, § 216(c), 18 U.S.C. § 3127(3) defined "pen register" as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached," and § 3127(4) defined "trap and trace device" as a "device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 18 U.S.C.A. § 3127(3), (4) (2000). Despite this textual focus on telephone communications, especially in § 3127(3), many (though not all) courts expansively construed both definitions to apply as well to e-mail communications. Memorandum of Law and Brief at 20 & n.16; Orin S. Kerr, Internet Surveillance Law (continued...)

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

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

statutory text," not "predecessor statutes," Lamie, 124 S. Ct. at 1030, and analysis of that text shows that collecting information in Categories ■■■ above by the means described in the application involves use of "pen registers" and "trap and trace devices."¹⁸

Of course, merely finding that the proposed collection falls within these definitions does not mean that the requirements for an order authorizing such collection have been met. We turn now to those requirements.

¹⁷(...continued)

After the USA PATRIOT Act: The Big Brother That Isn't, 97 Nw. U. L. Rev. 607, 633-36 (2003). Extending these prior definitions to bulk collection regarding e-mail communications would have required further departure from the pre-USA PATRIOT Act statutory language.

¹⁸ The legislative history of the USA PATRIOT Act indicates that Congress sought to make the definitions of "pen register" and "trap and trace device" "technology neutral" by confirming that they apply to Internet communications. See footnote 45 below. It does not suggest that Congress specifically gave thought to whether the new definitions would encompass collection in bulk from communications facilities that are not associated with individual users. The silence of the legislative history on this point provides no basis for departing from the plain meaning of the current definitions. See Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479, 495 n.13 (1985).

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

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

- II. THE STATUTORY REQUIREMENTS FOR ISSUING AN ORDER AUTHORIZING THE PROPOSED PEN REGISTER AND TRAP AND TRACE SURVEILLANCE HAVE BEEN MET.

Under FISA's pen register/trap and trace provisions:

Notwithstanding any other provision of law, the Attorney General . . . may make an application for an order . . . authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism . . ., provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the [FBI] under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

50 U.S.C. § 1842(a)(1). This authority "is in addition to the authority . . . to conduct . . . electronic surveillance" under §§ 1801-1811. Id. § 1842(a)(2).

Such applications shall include, inter alia, a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism . . ., provided that such investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution.

Id. § 1842(c)(2). "Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register

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

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

or trap and trace device if the judge finds that the application satisfies the requirements of [§ 1842]." Id. § 1842(d)(1).

Obviously, the application has been made by the Attorney General, § 1842(a)(1), has been approved by the Attorney General, § 1842(c), and has been submitted in writing and under oath to a judge of this Court. § 1842(b)(1). The application, at 5, identifies the DIRNSA as "the Federal officer seeking to use the pen register or trap and trace device." § 1842(c)(1).

The application also contains a certification by the Attorney General, at 26, containing the language specified in § 1842(c)(2). The Government argues that FISA prohibits the Court from engaging in any substantive review of this certification. In the Government's view, the Court's exclusive function regarding this certification would be to verify that it contains the words required by § 1842(c)(2); the basis for a properly worded certification would be of no judicial concern. See Memorandum of Law and Fact at 28-34.

The Court has reviewed the Government's arguments and authorities and does not find them persuasive.¹⁹ However, in

¹⁹ For example, the Government cites legislative history that "Congress intended to 'authorize[] FISA judges to issue a pen register or trap and trace order upon a certification that the information sought is relevant to'" an FBI investigation.

(continued...)

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

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

this case the Court need not, and does not, decide whether it would be obliged to accept the applicant's certification without any explanation of its basis. Arguing in the alternative, the Government has provided a detailed explanation of 1) the threat currently posed by [REDACTED] 2) the reason the bulk collection described in the application is believed necessary as a means for NSA [REDACTED] [REDACTED] 3) how that information will contribute to FBI investigations to protect against [REDACTED] and 4) what safeguards will be observed to ensure that the information collected will not be used for unrelated purposes or

¹⁹(...continued)

Memorandum of Law and Fact at 30 (quoting S. Rep. No. 105-185, at 27 (1998)). However, authorizing the Court to issue an order when a certification is made, and requiring it to do so without resolving doubts about the correctness of the certification, are quite different.

The Government also cites United States v. Hallmark, 911 F.2d 399 (10th Cir. 1990), in arguing that the Court should not review the basis of the certification. However, the Hallmark court reserved the analogous issue under Title 18 - "the precise nature of the court's review under 18 U.S.C. § 3123" of the relevancy certification in an application for a law enforcement pen register or trap and trace device - and expressed "no opinion as to whether the court may, for instance, inquire into the government's factual basis for believing the pen register or trap and trace information to be relevant to a criminal investigation." Id. at 402 n.3.

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

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

otherwise misused. The Government also provides legal arguments that, under these specific circumstances, the proposed collection satisfies the relevancy requirement of § 1842(c)(2), despite its resulting in the collection of meta data from an enormous volume of communications, the large majority of which will be unrelated to international terrorism. In view of this record, the Court will assume for purposes of this case that it may and should consider the basis of the certification under § 1842(c)(2).

Nonetheless, the Court is mindful that FISA does not require any finding of probable cause in order for pen register and trap and trace surveillance to be authorized. In this regard, the statutory provisions that govern this case contrast sharply with those that apply to other forms of electronic surveillance and physical search.²⁰ Before Congress amended FISA in 1998 to add §§ 1841-1846, this Court could authorize pen register and trap and trace surveillance only upon the same findings as would be required to authorize interception of the full contents of

²⁰ To issue an electronic surveillance order, the Court must find "probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power" and "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3). Similar probable cause findings are required for warrants authorizing physical search under *id.* § 1824(a)(3).

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

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

communications. See S. Rep. 105-185, at 27 (1998). When it originally enacted §§ 1841-1846 in 1998, Congress recognized that pen register and trap and trace information is not protected by the Fourth Amendment and concluded that a lower standard for authorization "was necessary in order to permit, as is the case in criminal investigations, the use of this very valuable investigative tool at the critical early stages of foreign intelligence and international terrorism investigations." Id. These 1998 provisions included a form of a "reasonable suspicion" standard for pen register/trap and trace authorizations.²¹ As part of the USA PATRIOT Act in 2001, Congress lowered the standard again, to the current requirement of relevance.²² Given this history, it is obvious that Congress intended pen register

²¹ Under the provisions enacted in 1998, a pen register or trap and trace application had to include "information which demonstrates that there is reason to believe" that a communication facility "has been or is about to be used in communication with," inter alia, "an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities." Public Law 105-272 § 601(2).

²² The legislative history of the USA PATRIOT Act reflects that, "in practice," the standard passed in 1998 was "almost as burdensome as the requirement to show probable cause required . . . for more intrusive techniques" and that the FBI "made a clear case that a relevance standard is appropriate for counterintelligence and counterterrorism investigations." 147 Cong. Rec. S11003 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

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

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

and trap and trace authorizations to be more readily available than authorizations for electronic surveillance to acquire the full contents of communications.

The Court also recognizes that, for reasons of both constitutional authority and practical competence, deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats²³ and in determining the potential significance of intelligence-related information.²⁴ Such deference is particularly

²³ See, e.g., Reno v. American-Arab Anti-Discrimination Comm., 525 U.S. 471, 491 (1999) ("a court would be ill equipped to determine [the] authenticity and utterly unable to assess [the] adequacy" of the executive's security or foreign policy reasons for treating certain foreign nationals as "a special threat"); Regan v. Wald, 468 U.S. 222, 243 (1984) (giving "the traditional deference to executive judgment" in foreign affairs in sustaining President's decision to restrict travel to Cuba against a Due Process Clause challenge); cf. Department of Navy v. Egan, 484 U.S. 518, 529 (1988) (outside body reviewing executive branch decisions on eligibility for security clearances could not "determine what constitutes an acceptable margin of error in assessing the potential risk").

²⁴ The Supreme Court has observed that, in deciding whether disclosing particular information might compromise an intelligence source, what "may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context." CIA v. Sims, 471 U.S. 159, 178 (1985) (internal quotation and citation omitted). Accordingly, the decisions of [REDACTED] "who must of course be familiar with 'the whole picture,' as judges are not, are worthy of great deference given the magnitude of the national security interests and potential (continued...)

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

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

appropriate in this context, where the Court is not charged with making independent probable cause findings.

A. The Government Has Provided Information In Support of the Certification of Relevance.

In support of the certification of relevance, the Government relies on the following facts and circumstances:

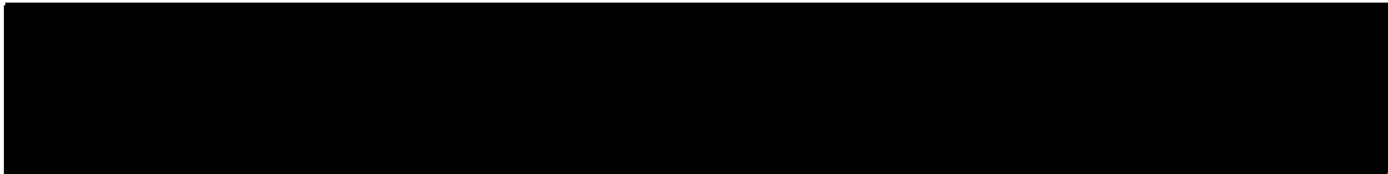
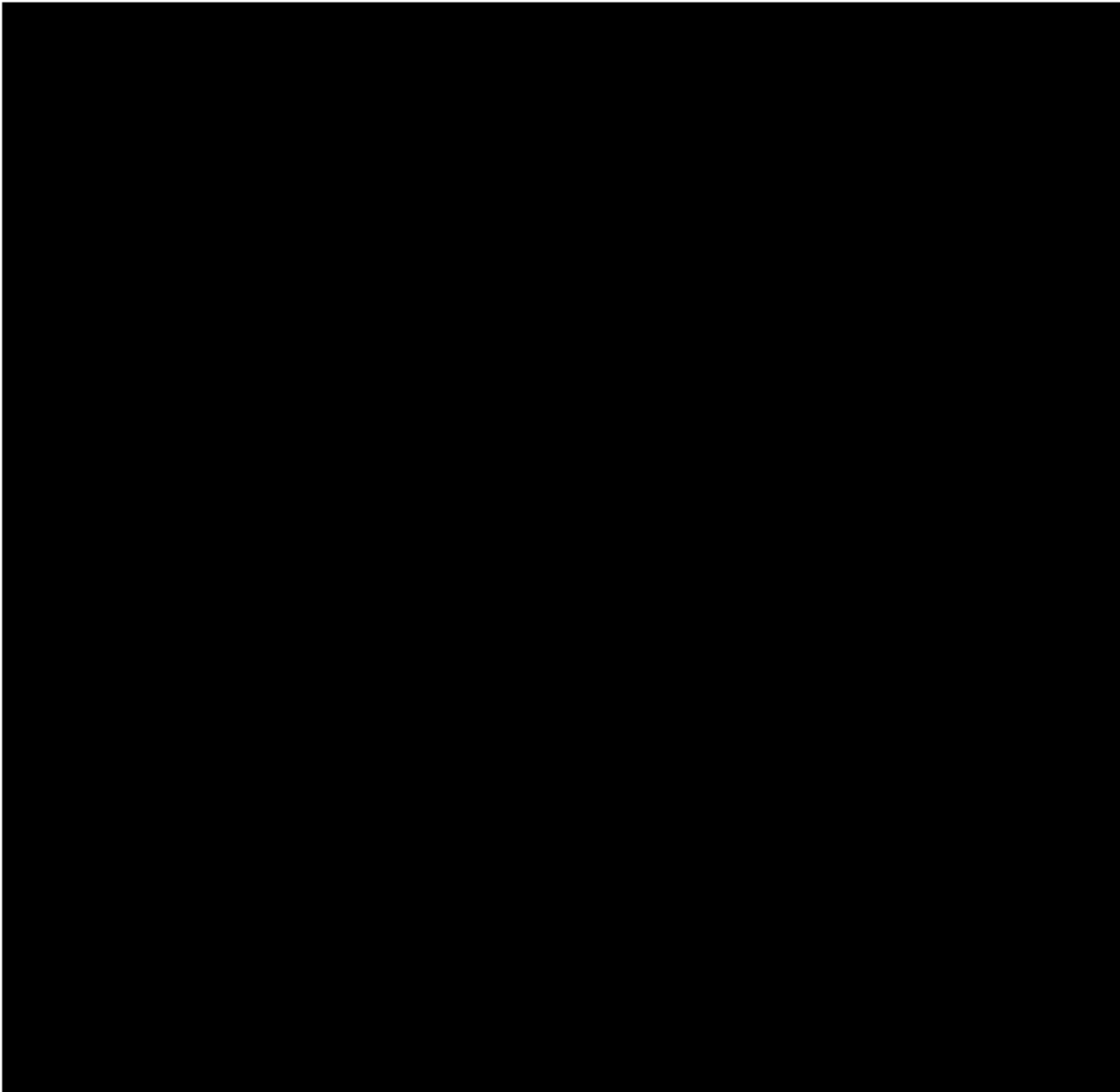
1. The Threat Currently Posed

²⁴(...continued)
risks at stake." Id. at 179.

²⁵ For simplicity, this opinion standardizes the variant spellings of foreign names appearing in different documents submitted in support of the application.

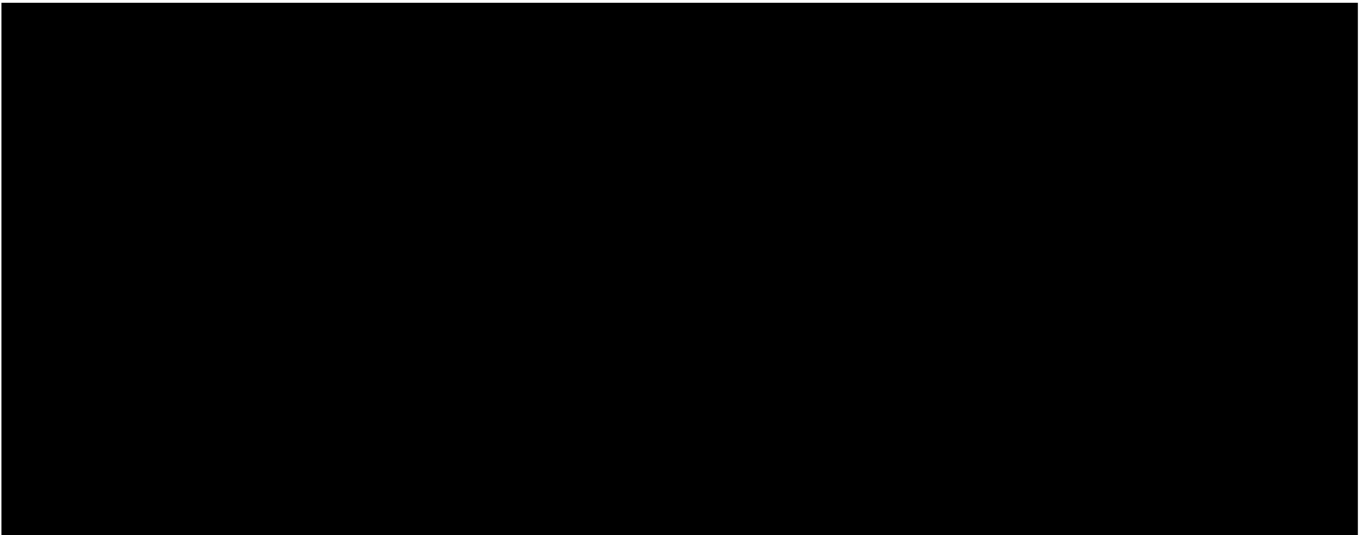
~~TOP SECRET//HCS//COMINT//NOFORN~~

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

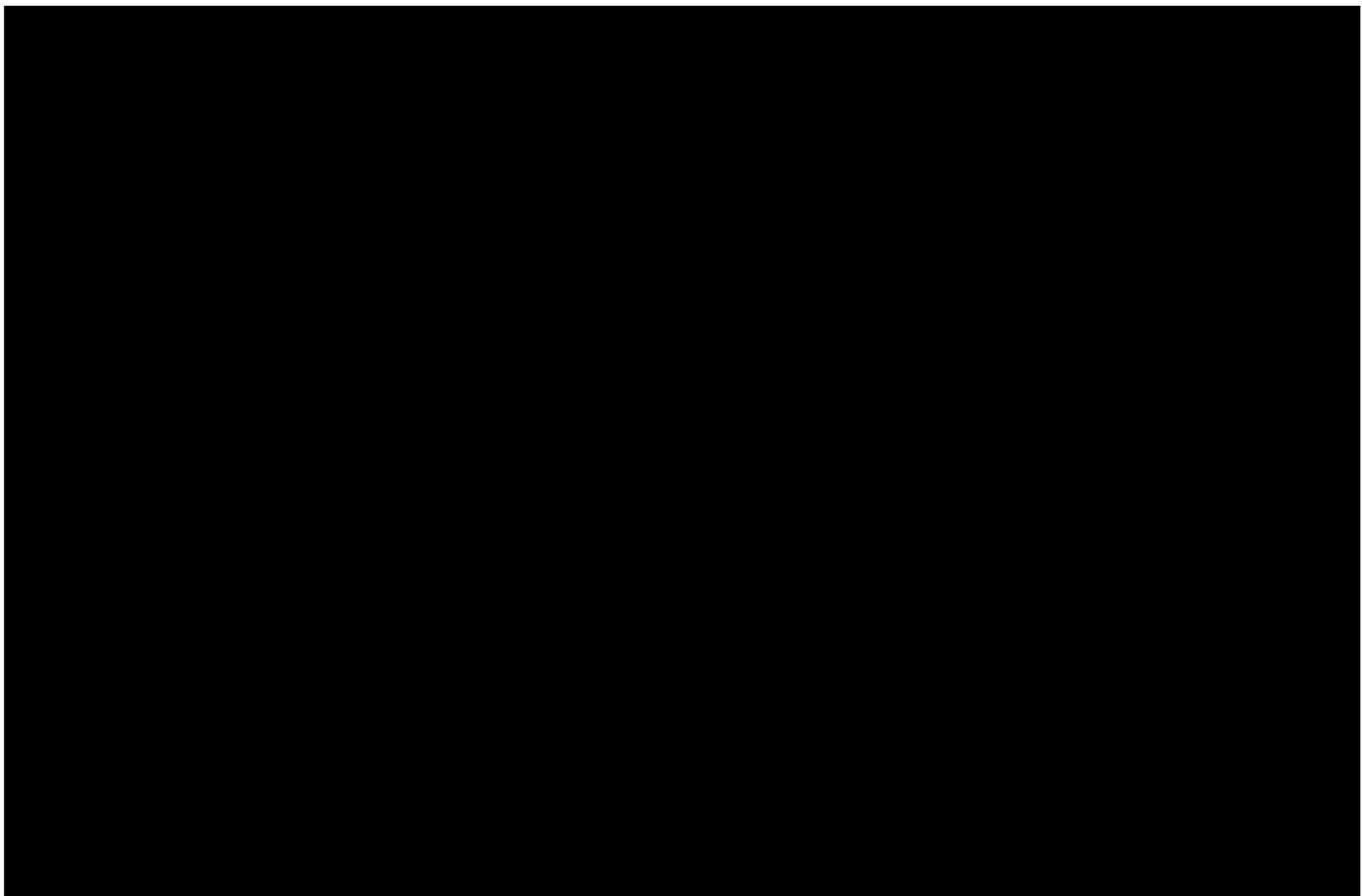


TOP SECRET//HCS//COMINT//NOFORN

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

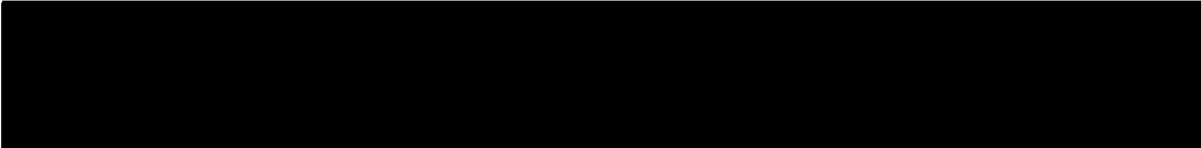



2. FBI Investigations to Track and Identify [REDACTED]
[REDACTED] in the United States

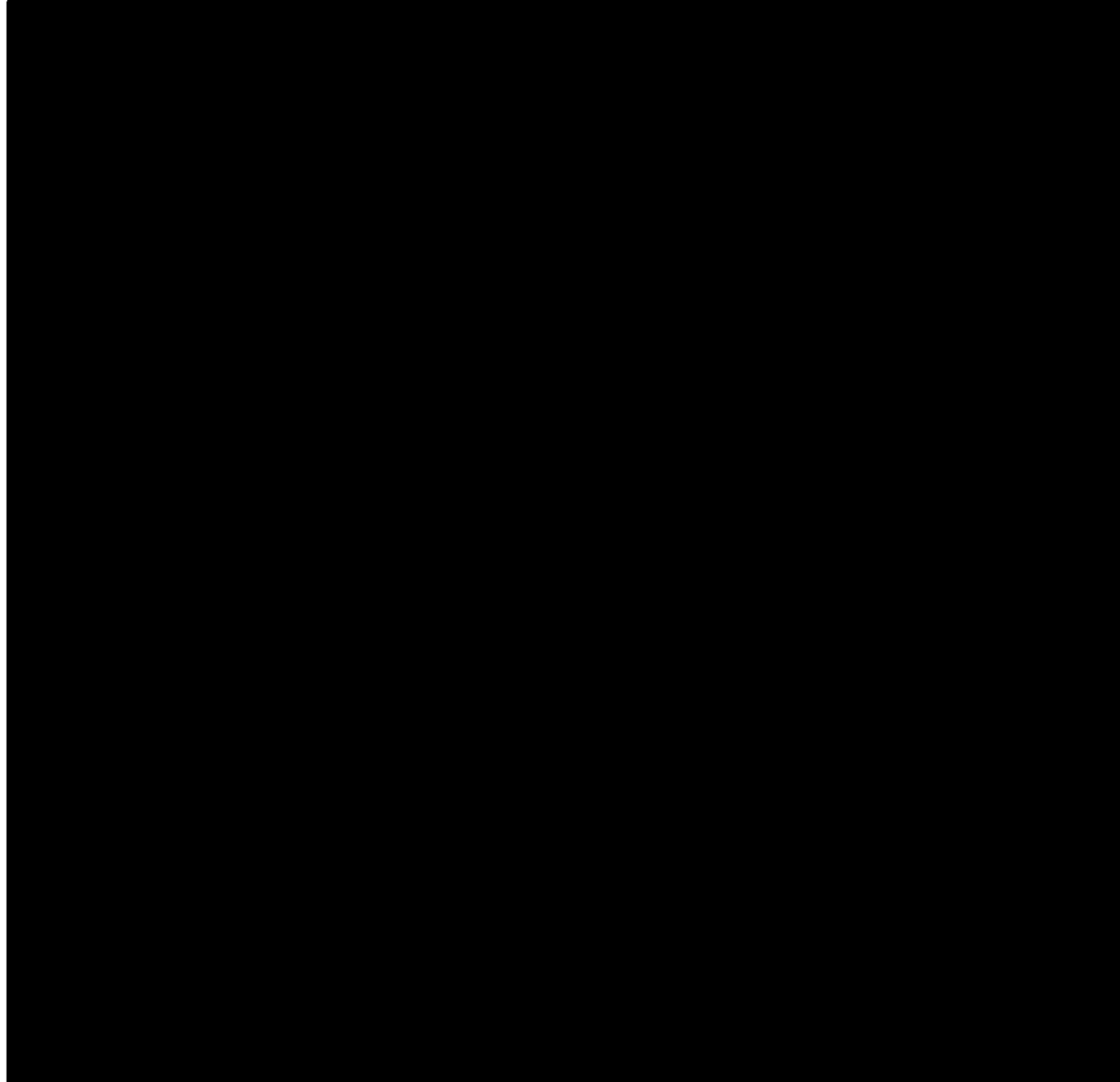


~~TOP SECRET//HCS//COMINT//NOFORN~~

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



3. The Use of the Internet by 



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

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

4. The Scope of the Proposed Collection of Meta Data

In an effort both to identify unknown and to track known operatives [REDACTED] through their Internet communications, NSA seeks to acquire meta data, as described above, from all e-mail [REDACTED]

[REDACTED] are described in detail in the application and the DIRNSA Declaration. In brief, they are:

²⁷ For ease of reference, the term [REDACTED] is used to mean [REDACTED]

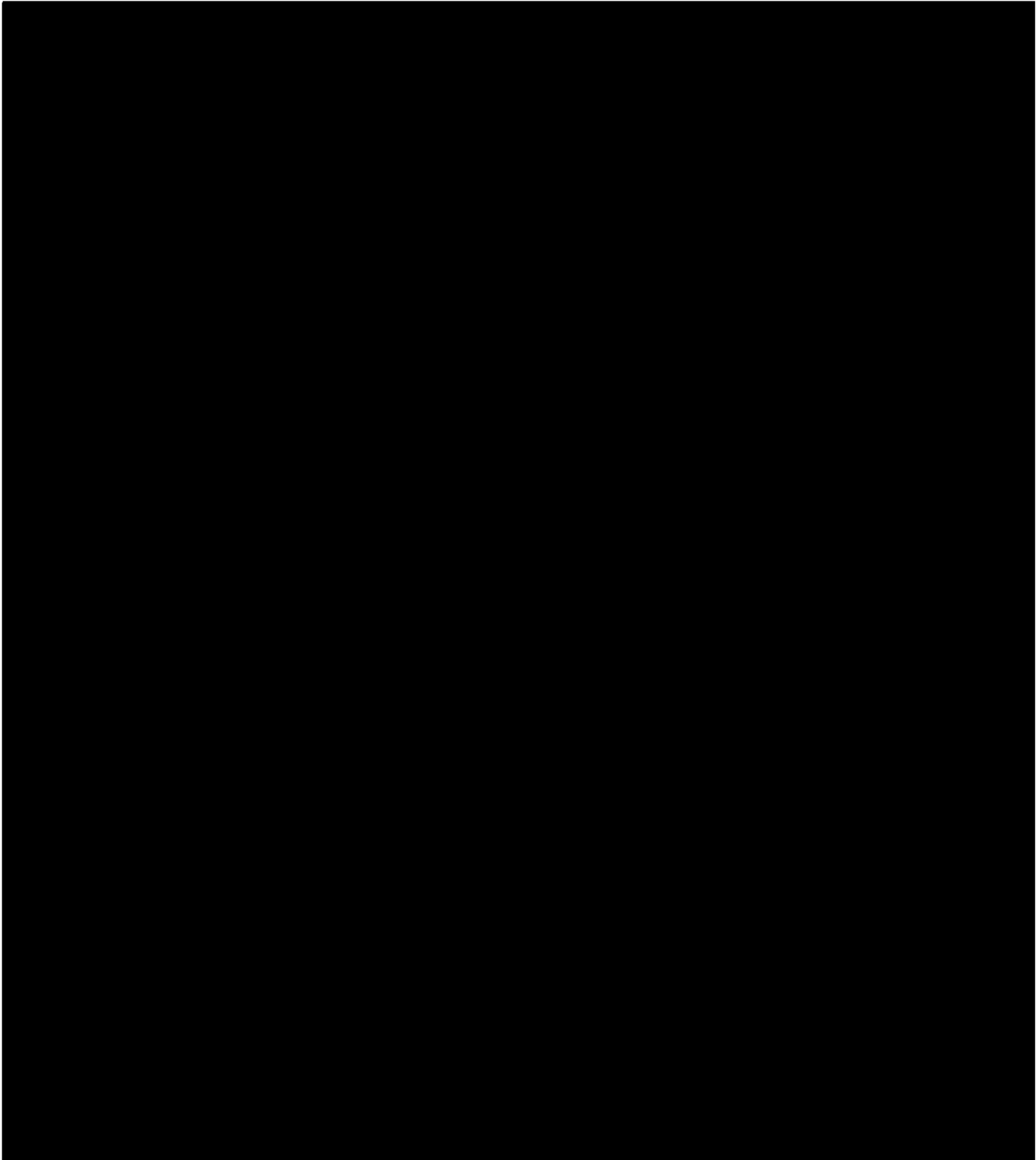
~~TOP SECRET//HCS//COMINT//NOFORN~~

TOP SECRET//HCS//COMINT//NOFORN



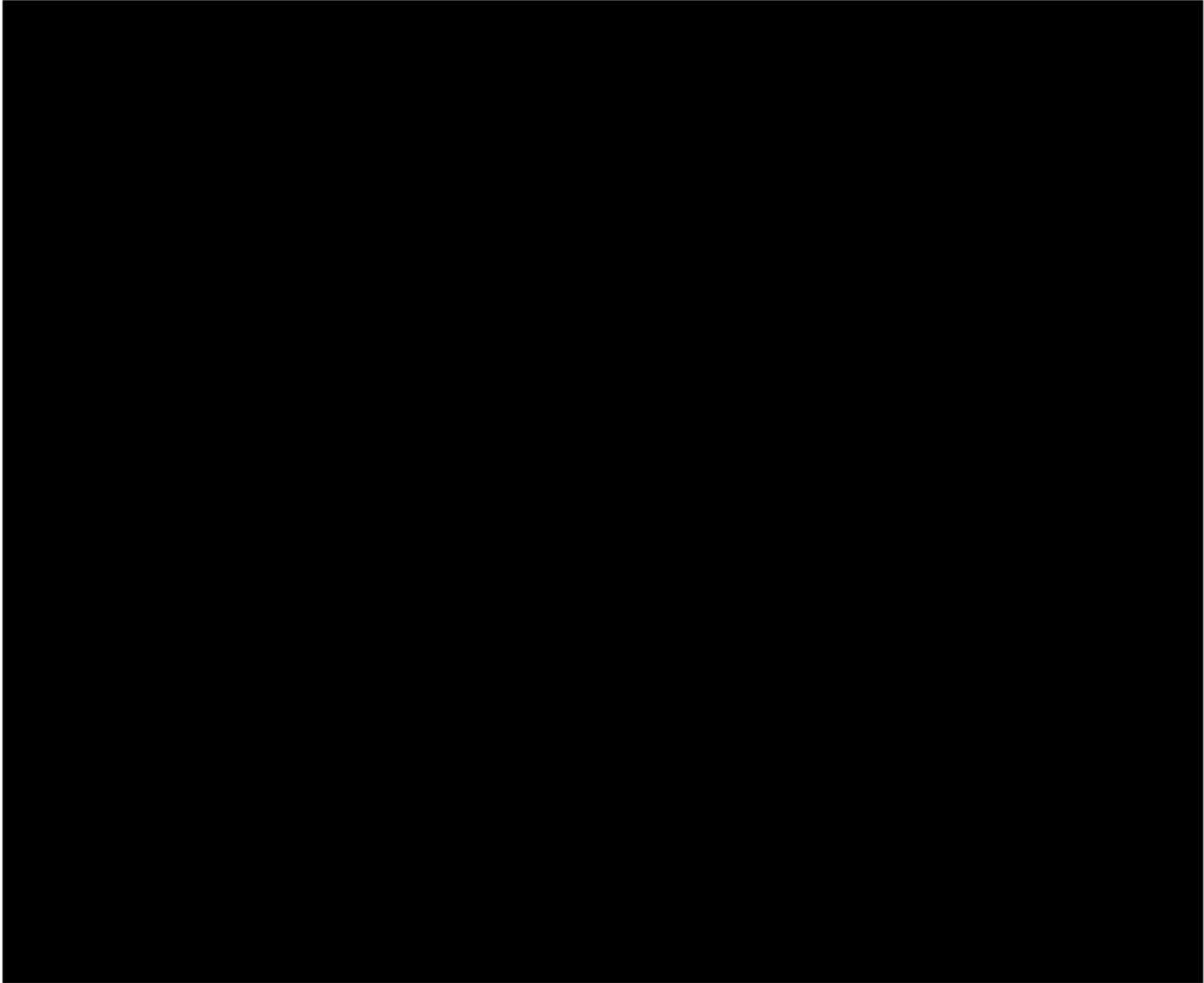
~~TOP SECRET//HCS//COMINT//NOFORN~~

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



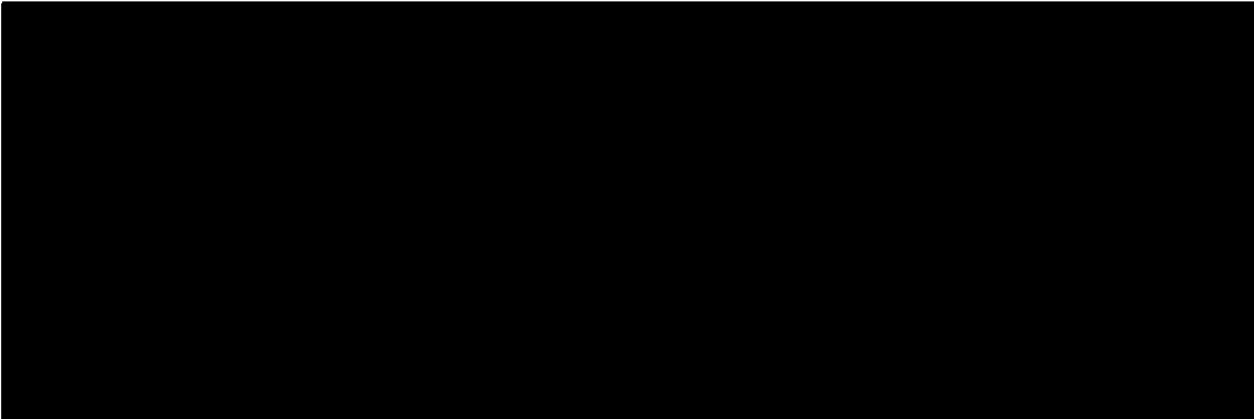
~~TOP SECRET//HCS//COMINT//NOFORN~~

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

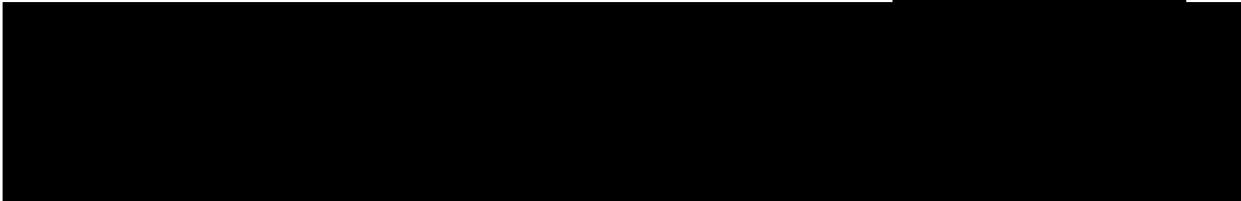


~~TOP SECRET//HCS//COMINT//NOFORN~~

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



The raw volume of the proposed collection is enormous. NSA estimates that this collection will encompass [REDACTED]



[REDACTED] In absolute terms, the proposed surveillance "will result in the collection of meta data pertaining to [REDACTED] [REDACTED] electronic communications, including meta data pertaining to communications of United States persons located within the United States who are not the subject of any FBI investigation." Application at 4. Some proportion of these communications - less than half, but still a huge number in absolute terms - can be expected to be communications [REDACTED]

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

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

[REDACTED] who bear no relation to [REDACTED]

[REDACTED]

5. How NSA Proposes to Use this Data to Track Known [REDACTED]

[REDACTED]


As noted above, the purpose of this collection is to track known operatives and to identify unknown operatives of [REDACTED] through their Internet communications. NSA

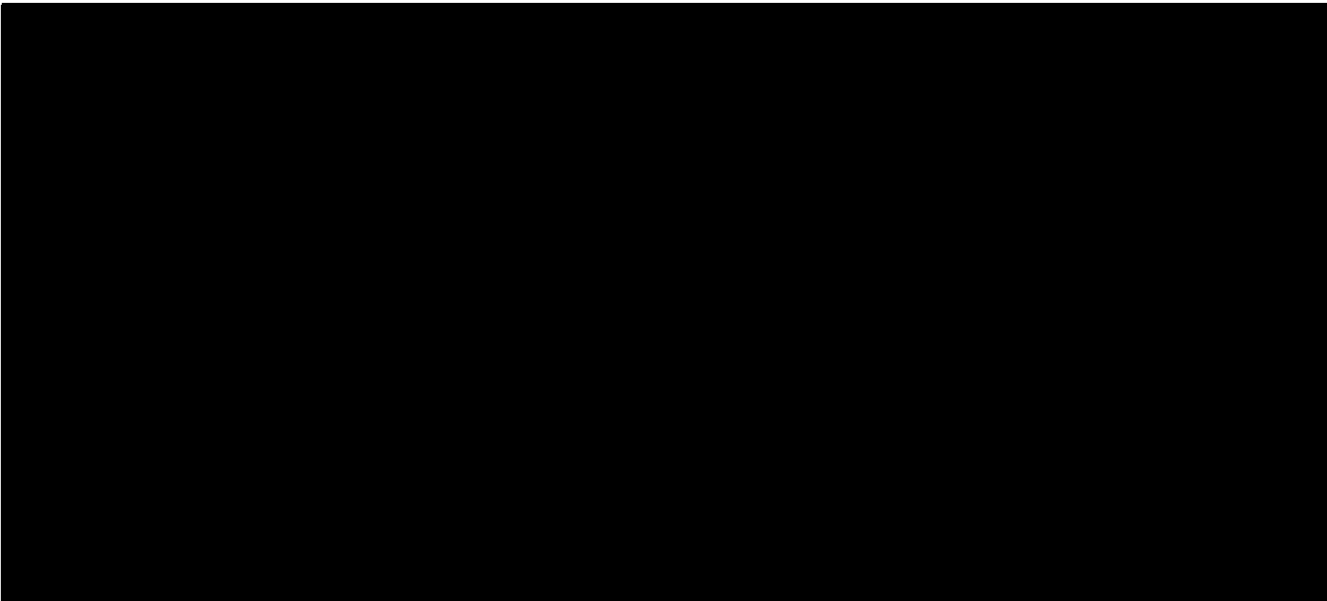

²⁹ As noted above, collection of meta data from [REDACTED]


[REDACTED]

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

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

states that even identified operatives 



Through the proposed bulk collection, NSA would acquire an archive of meta data for large volumes of communications that, in NSA's estimation, represent a relatively rich environment for finding  communications through later analysis.³¹

³¹ See DIRNSA Declaration at 5 



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

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

NSA asserts that more precisely targeted forms of collection against known accounts would tend to screen out the "unknowns" that NSA wants to discover, so that NSA needs bulk collection in order to identify unknown [REDACTED] communications. See id. at 14 ("It is not possible . . . to target collection solely to known terrorist E-mail accounts and at the same time use the advantages of meta data analysis to discover the enemy."), 15 ("To be able to fully exploit meta data, the data must be collected in bulk. Analysts know that terrorists' E-mails are located somewhere in the billions of data bits; what they cannot know ahead of time is exactly where.")

NSA proposes to employ two analytic methods on the body of archived meta data it seeks to collect. Both these methods involve querying the archived meta data regarding a particular "seed" account. In the Government's proposal, an account would qualify as a seed account only if NSA concludes, "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 that a particular known e-mail address is associated with [REDACTED]"

[REDACTED]

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

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

[REDACTED] Application at 19-20; accord DIRNSA

Declaration at 19. The two methods are:

(1) Contact chaining. NSA will use computer algorithms to identify within the archived meta data all e-mail [REDACTED]

[REDACTED] accounts that have been in contact with the seed account, as well as all accounts that have been in contact with an account within the first tier of accounts that had direct contact with the seed account, and [REDACTED]

[REDACTED] DIRNSA Declaration at 15-16.

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

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

An example may illustrate the claimed benefits of bulk collection and subsequent analysis of meta data. [REDACTED]

[REDACTED] Without an archive of meta data, the Government could target prospective collection on that account, but information about past use would be unavailable. [REDACTED]

[REDACTED].³²

However, if an archive of meta data were available, NSA could use the newly discovered account as a "seed" account. Accounts previously in contact with the "seed" account could be identified and further investigation could be pursued to determine if the users of those accounts are [REDACTED]

³² Assuming that applicable legal requirements could be met, the Government also could collect the full contents of future messages by electronic surveillance of the account and of stored prior messages by physical search of the account. However, [REDACTED] could thwart these forms of collection also.

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

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

[REDACTED]

These avenues of discovery made possible by archived meta data provide the basis for NSA's assertion that bulk collection to accumulate a meta data archive "will substantially increase NSA's ability to detect and identify members of [REDACTED] [REDACTED] DIRNSA Declaration at 15.

6. How FBI Investigations Would Benefit from the NSA's Collection and Analysis

The Government asserts that NSA's collection and analysis of this meta data will be relevant to [REDACTED] FBI investigations in two ways. First, ongoing FBI investigations may develop grounds for reasonable suspicion that particular accounts are used in furtherance of [REDACTED]

[REDACTED] The FBI may identify such accounts to NSA for use as "seed" accounts. Using the methods described above, NSA may obtain from the archived data other accounts that are in contact with, or appear to have the same user as, the "seed" account. This information may then be passed to the FBI as investigative leads in furtherance of its investigation. Memorandum of Law and Fact at 27-28. Alternatively, NSA querying of the archived meta data based on information from sources other than the FBI may identify accounts that appear to be used by someone involved in

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

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

[REDACTED] activities. If such accounts are relevant to FBI investigative responsibilities - for example, if it appears that their users are in the United States - then NSA will provide information to the FBI, which may prove relevant to ongoing FBI investigations or provide the predicate for new investigations of persons involved in [REDACTED]. Under the proposed program, NSA estimates that roughly 400 accounts would be "tipped" to the FBI and CIA³³ annually, with an estimated twenty-five percent of that number associated with U.S. persons. DIRNSA Declaration at 20.

7. The Government's Proposed Procedures for Accessing, Retaining, and Disseminating Collected Information

The application specifies proposed procedures and restrictions for accessing, retaining, and disseminating information from this bulk collection of meta data. Application at 18-24. These procedures and restrictions, with certain modifications, are set out at pages 82-87 below.

³³ As long as the proposed collection satisfies the standard of relevance to an FBI investigation described in section 1842(a)(1), (c)(2), dissemination of information to other agencies when it is relevant to their responsibilities is appropriate.

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

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

B. The Information To Be Obtained is Likely to be Relevant to Ongoing FBI Investigations to Protect Against International Terrorism

As shown above, the application and supporting materials demonstrate that the FBI has numerous pending investigations on [REDACTED] subjects and that a major challenge faced by the FBI is the identification of [REDACTED] within the United States. [REDACTED]

[REDACTED] The application and DIRNSA declaration provide detailed explanations of why NSA regards bulk collection of meta data as necessary for contact chaining [REDACTED] and how those analytical methods can be expected to uncover and monitor unknown [REDACTED] [REDACTED] who could otherwise elude detection. The DIRNSA also explains why NSA has chosen the proposed [REDACTED] and selection criteria in order to build a meta data archive that will be, in relative terms, richly populated with [REDACTED] related communications. On each of these points, the Court has received sufficient information to conclude that the Government's

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

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

assessments are fully considered and plausibly grounded in facts submitted to the Court.

Accordingly, the Court accepts for purposes of this application that the proposed bulk collection of meta data is necessary for NSA to employ contact chaining [REDACTED]

[REDACTED] The Court similarly accepts that those analytic tools are likely to generate useful investigative leads for ongoing efforts by the FBI (and other agencies) to identify and track [REDACTED] [REDACTED] potentially including unidentified operatives in place to facilitate or execute imminent large scale attacks within the United States.

The question remains whether these circumstances adequately support the certification that "the information likely to be obtained . . . is relevant to an ongoing investigation to protect against international terrorism," § 1842(c)(2), even though only a very small percentage of the information obtained will be from [REDACTED] communications and therefore directly relevant to such an investigation. As the Government points out, the meaning of "relevant" is broad enough, at least in some contexts, to encompass information that may reasonably lead to the discovery of directly relevant information. Memorandum of Law and Fact at 34. Here, the bulk collection of meta data - i.e.,

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

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

the collection of both a huge volume and high percentage of unrelated communications - is necessary to identify the much smaller number of [REDACTED] communications.

The Court is persuaded that, in the circumstances of this case, the scope of the proposed collection is consistent with the certification of relevance.³⁴ In so finding, the Court concludes that, under the circumstances of this case, the applicable relevance standard does not require a statistical "tight fit" between the volume of proposed collection and the much smaller proportion of information that will be directly relevant to [REDACTED]

³⁴ The Government analogizes this case to ones in which the Court has authorized overbroad electronic surveillance under 50 U.S.C. §§ 1801-1811. Memorandum of Fact and Law at 42-43. The Court has authorized the latter form of collection where it is not technologically possible to acquire [REDACTED]

[REDACTED] The two situations are similar in that they both involve collection of an unusually large volume of non-foreign intelligence information as a necessary means of obtaining the desired foreign intelligence information. Yet there are also important differences between these cases. An overbroad electronic surveillance under 50 U.S.C. §§ 1801-1811 requires probable cause to believe that the target is an agent of a foreign power and uses the particular facility at which surveillance will be directed. § 1805(a)(3). In this case under 50 U.S.C. §§ 1841-1846, no probable cause findings are required, and the bulk collection is justified as necessary to discover unknown [REDACTED] persons and facilities, rather than to acquire communications to and from identified agents of a foreign power. Because of these differences, the authorization of bulk collection under §§ 1841-1846 should not be taken as precedent for similar collection of the full contents of communications under §§ 1801-1811.

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

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

[REDACTED] FBI investigations. In reaching this conclusion, the Court finds instructive Supreme Court precedents on when a search that is not predicated on individualized suspicion may nonetheless be reasonable under the Fourth Amendment. See Memorandum of Law and Fact at 43-48.³⁵

The Supreme Court has recognized a "longstanding principle that neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance." National Treasury Employees Union v. Von Raab, 489 U.S. 656, 665 (1989); accord, e.g., Board of Educ. of Indep. School Dist. No. 92 of Pottawatomie County v. Earls, 536 U.S. 822, 829 (2002); United States v. Martinez-Fuerte, 428 U.S. 543, 560-61 (1976). Specifically, the Court has held that, "where a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's

³⁵ For the reasons explained below at pages 59-66, the Court finds that there is no privacy interest protected by the Fourth Amendment in the meta data to be collected. Nevertheless, the Court agrees with the Government's suggestion that the balancing methodology used to assess the reasonableness of a Fourth Amendment search or seizure is helpful in applying the relevance standard to this case. Memorandum of Law and Fact at 43.

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

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

interests to determine whether it is impractical to require a warrant or individualized suspicion in the particular context." Von Raab, 489 U.S. at 665-66; accord, e.g., Earls, 536 U.S. at 829.

This balancing analysis considers "the nature of the privacy interest allegedly compromised" and "the character of the intrusion" upon that interest. Earls, 536 U.S. at 830, 832. The privacy interest in the instant meta data is not of a stature protected by the Fourth Amendment. See pages 59-66 below. Moreover, the nature of the intrusion is mitigated by the restrictions on accessing and disseminating this information, under which only a small percentage of the data collected will be seen by any person. Cf. Earls, 536 U.S. at 833 (finding that restrictions on access to drug-testing information lessen the testing program's intrusion on privacy).

The assessment of reasonableness under the Fourth Amendment also considers "the nature and immediacy of the government's concerns and the efficacy of the [program] in meeting them." Id. at 834. In this case, the Government's concern is to identify and track [REDACTED] operatives, and ultimately to thwart terrorist attacks. This concern clearly involves national

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

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

security interests beyond the normal need for law enforcement³⁶ and is at least as compelling as other governmental interests that have been held to justify searches in the absence of individualized suspicion. See, e.g., Earls (drug testing of secondary school students engaged in extracurricular activities); Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (highway checkpoints to identify drunk drivers); Von Raab (drug testing of Customs Service employees applying for promotion to sensitive positions); Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989) (drug and alcohol testing of railroad workers).³⁷ The Government's interest here has even greater "immediacy" in view of the above-described intelligence reporting and assessment regarding ongoing plans for large scale attacks within the United States.

As to efficacy under the Fourth Amendment analysis, the Government need not make a showing that it is using the least intrusive means available. Earls, 536 U.S. at 837; Martinez-

³⁶ See In Re Sealed Case, 310 F.3d 717, 744-46 (Foreign Int. Surv. Ct. Rev. 2002) (per curiam) (discussing the prevention of terrorist attacks as a special need beyond ordinary law enforcement).

³⁷ Moreover, the Government's need in this case could be analogized to the interest in discovering or preventing danger from "latent or hidden conditions," which may justify suspicionless searches. See, e.g., Von Raab, 489 U.S. at 668.

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

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

Fuerte, 428 U.S. at 556-57 n.12. Rather, the question is whether the Government has chosen "a reasonably effective means of addressing" the need. Earls, 536 U.S. at 837. In structuring a program involving suspicionless search or seizure, e.g., in positioning roadblocks at certain points, "the choice among . . . reasonable alternatives remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources." Sitz, 496 U.S. at 453-54; see also Martinez-Fuerte, 428 U.S. at 566 ("deference is to be given to the administrative decisions of higher ranking officials"). A low percentage of positive outcomes among the total number of searches or seizures does not necessarily render a program ineffective.³⁸

In this case, senior responsible officials, whose judgment on these matters is entitled to deference, see pages 30-31 above, have articulated why they believe that bulk collection and archiving of meta data are necessary to identify and monitor [REDACTED] [REDACTED] operatives whose Internet communications would

³⁸ See Sitz, 496 U.S. at 454 ("detention of the 126 vehicles that entered the checkpoint resulted in the arrest of two drunken drivers"); Martinez-Fuerte, 428 U.S. at 546 & n.1, 554 (checkpoint near border to detect illegal migrants: out of "roughly 146,000 vehicles" temporarily "'seized,'" 171 were found to contain deportable aliens).

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

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

otherwise go undetected in the huge streams of [REDACTED]

[REDACTED] These officials have also explained why they seek to collect meta data [REDACTED]

[REDACTED] identified in the application. Based on these explanations, the proposed collection appears to be a reasonably effective means to this end.

In summary, the bulk collection proposed in this case is analogous to suspicionless searches or seizures that have been upheld under the Fourth Amendment in that the Government's need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of detecting and monitoring [REDACTED] related operatives and thereby obtaining information likely to be [REDACTED] to ongoing FBI investigations. In these circumstances, the certification of relevance is consistent with the fact that only a very small proportion of the huge volume of information collected will be directly relevant to the FBI's [REDACTED] investigations.

³⁹ Cf. Martinez-Fuerte, 428 U.S. at 557 (requiring reasonable suspicion for stops at highway checkpoints "on major routes . . . would be impractical because the flow of traffic tends to be too heavy to allow the particularized study of a given car").

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

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

C. The Pertinent FBI Investigations of U.S. Persons Are Not Conducted Solely Upon the Basis of First Amendment Activities.

When the information likely to be obtained concerns a U.S. person, § 1842(c)(2) requires a certification that the "ongoing investigation . . . of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." The certification in this case states that the pertinent investigation is not being conducted on such a basis. Application at 26. The application refers to numerous FBI National Security investigations "being conducted under guidelines approved by the Attorney General pursuant to Executive Order No. 12,333."⁴⁰ Id. at 6.

Those investigations are being conducted on the basis of activities of [REDACTED] and unknown [REDACTED] affiliates in the United States and abroad, and to the extent these subjects of investigation are United States persons, not solely on the basis of activities that are protected by the First Amendment to the Constitution.

Id.

Thus, the certification and application contain the proper assurance that the relevant investigations of U.S. persons are

⁴⁰ § 1842(a)(1) permits the filing of applications for installation and use of pen register and trap and trace devices to obtain information relevant to certain investigations "under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order."

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

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

not being conducted solely on the basis of activities protected by the First Amendment. However, the unusual breadth of this collection and its relation to the pertinent FBI investigations calls for further attention to this issue. In the usual case, the FBI conducts pen register and trap and trace surveillance of a particular communications facility (e.g., a phone number or e-mail address) because it carries communications of a person who is the subject of an FBI investigation. The required certification typically varies depending on whether the subject is a U.S. person: if not, the certification will state, in the language of § 1842(c)(2), that the information likely to be obtained "is foreign intelligence information not concerning a United States person;" if the subject is a U.S. person, the certification will state that such information is "relevant to an ongoing investigation to protect against international terrorism . . . , provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This usual practice conforms to the clear statutory purpose that pen register/trap and trace information about the communications of U.S. persons will not be targeted for collection unless it is relevant to an

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

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

investigation that is not solely based upon First Amendment activities.

In this case, the initial acquisition of information is not directed at facilities used by particular individuals of investigative interest, but meta data concerning the communications of such individuals' [REDACTED]

[REDACTED] Here, the legislative purpose is best effectuated at the querying stage, since it will be at a point that an analyst queries the archived data that information concerning particular individuals will first be compiled and reviewed. Accordingly, the Court orders that NSA apply the following modification of its proposed criterion for querying the archived data: [REDACTED] will qualify as a seed

[REDACTED] only if NSA concludes, 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 that a particular known [REDACTED]

[REDACTED] is associated with [REDACTED] [REDACTED] provided, however, that an [REDACTED] believed to be used by a U.S. person shall not be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First

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

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

Amendment to the Constitution.⁴¹ For example, an e-mail account used by a U.S. person could not be a seed account if the only information thought to support the belief that the account is associated with [REDACTED] is that, in sermons or in postings on a web site, the U.S. person espoused jihadist rhetoric that fell short of "advocacy . . . directed to inciting or producing imminent lawless action and . . . likely to incite or produce such action." Brandenberg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam).

III. THE PROPOSED COLLECTION AND HANDLING OF META DATA DO NOT VIOLATE THE FIRST OR FOURTH AMENDMENTS.

Because this case presents a novel use of statutory authorities for pen register/trap and trace surveillance, the Court will also explain why it is satisfied that this surveillance comports with the protections of the Fourth Amendment and the First Amendment.

A. Fourth Amendment Issues

The foregoing analysis has observed at various points that the Fourth Amendment does not apply to the proposed collection of

⁴¹ This modification will realize more fully the Government's suggestion that "[t]he information actually viewed by any human being . . . will be just as limited - and will be based on the same targeted, individual standards - as in the case of an ordinary pen register or trap and trace device." Government's Letter of [REDACTED] at 3.

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

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

meta data. See, e.g., pages 19, 50-51 above. This section explains the basis for that conclusion.

First, as a general matter, there is no reasonable expectation of privacy under the Fourth Amendment in the meta data to be collected. This conclusion follows directly from the reasoning of Smith v. Maryland, 442 U.S. 735 (1979), which concerned the use of a pen register on a home telephone line. In that case, the Supreme Court found that it was doubtful that telephone users had a subjective expectation of privacy in the numbers they dialed, id. at 742-43, and that in any case such an expectation "is not 'one that society is prepared to recognize as reasonable.'" Id. at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)). The Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," since he "assume[s] the risk" that the third party would reveal that information to the government. Id. at 743-44.⁴² The Court found this principle applicable to dialed phone numbers, regardless of the automated means by which the call is placed and the "fortuity of whether or

⁴² This principle applies even if there is an understanding that the third party will treat the information as confidential. See SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984); United States v. Miller, 425 U.S. 435, 443 (1976).

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

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

not the phone company in fact elects to make a quasi-permanent record of a particular number dialed." Id. at 744-45.⁴³

The same analysis applies to the meta data involved in this application. Users of e-mail ██████████ ██████████ voluntarily expose addressing information for communications they send and receive to communications service providers. Having done so, they lack any legitimate expectation of privacy in such information for Fourth Amendment purposes.⁴⁴ Moreover, the relevant statutes put this form of pen register/trap and trace surveillance on a par with pen register/trap and trace surveillance of telephone calls, on the

⁴³ While Smith involved a pen register, its reasoning equally applies to trap and trace devices that capture the originating numbers of incoming calls. See, e.g., United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990).

⁴⁴ Cf. Guest v. Leis, 255 F.3d 325, 335-36 (6th Cir. 2001) (users of computer bulletin board service lacked reasonable expectation of privacy in subscriber information that they provided to systems operator); United States v. Kennedy, 81 F.Supp.2d 1103, 1110 (D. Kan. 2000) (no reasonable expectation of privacy in subscriber information provided to ISP); United States v. Hambrick, 55 F.Supp.2d 504, 508-09 (W.D. Va. 1999) (no reasonable expectation of privacy in screen name and other information provided to ISP), aff'd, 225 F.3d 656 (4th Cir. 2000) (Table).

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

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

premise that neither form of surveillance involves a Fourth Amendment search or seizure.⁴⁵

This conclusion is equally well-founded for the proposed collection of [REDACTED] Nothing in the Smith analysis depends on the fact that a telephone pen register acquires addressing information for a call while it is being placed, rather than from data [REDACTED] Indeed, the controlling principle - that voluntary disclosure of information to a third party vitiates any legitimate expectation that the third party will not provide it to the government - has been applied to records [REDACTED] See Jerry T. O'Brien, Inc., 467 U.S. at 737-38, 743 (records of prior stock

⁴⁵ The USA PATRIOT Act amended 18 U.S.C. § 3127 to clarify that its definitions of "pen register" and "trap and trace device" applied to Internet communications. See Public Law 107-56, Title II, § 216(c); 147 Cong. Rec. S11000 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) (noting that prior statutory language was "ill-equipped" for Internet communications and supporting clarification of "the statute's proper application to tracing communications in an electronic environment . . . in a manner that is technology neutral"). Authorization to install such devices requires relevance to an investigation, but not any showing of probable cause. See 18 U.S.C. § 3123(a)(1), (2) (ordinary criminal investigation); 50 U.S.C. § 1842(a)(1), (c)(2) (investigation conducted under guidelines approved under Executive Order 12333).

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

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

trading); Miller, 425 U.S. at 436-38, 443 (checks, deposit slips, and other bank records).⁴⁶

For these reasons, it is clear that, in ordinary circumstances, pen register/trap and trace surveillance of Internet communications does not involve a Fourth Amendment search or seizure. However, since this application involves unusually broad collection and distinctive modes of analyzing information, the Court will explain why these special circumstances do not alter its conclusion that no Fourth Amendment search or seizure is involved.

First, regarding the breadth of the proposed surveillance, it is noteworthy that the application of the Fourth Amendment depends on the government's intruding into some individual's reasonable expectation of privacy. Whether a large number of persons are otherwise affected by the government's conduct is irrelevant. 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."

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

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

Steagald v. United States, 451 U.S. 204, 219 (1981); accord, e.g., Rakas v. Illinois, 439 U.S. 128, 133 (1978) ("Fourth Amendment rights are personal rights which . . . may not be vicariously asserted.") (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)). Since the Fourth Amendment bestows "a personal right that must be invoked by an individual," a person "claim[ing] the protection of the Fourth Amendment . . . must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable." Minnesota v. Carter, 525 U.S. 83, 88 (1998). So long as no individual has a reasonable expectation of privacy in meta data, the large number of persons whose communications will be subjected to the proposed pen register/trap and trace surveillance is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur.

Regarding the proposed analytical uses of the archived meta data, it might be thought that [REDACTED]

[REDACTED] not immediately available from conventional pen register/trap and

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

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

trace surveillance might itself implicate the Fourth Amendment.⁴⁷ However, that suggestion would be at odds with precedent that the subsequent use of the results of a search cannot itself involve an additional or continuing violation of the Fourth Amendment. For example, in United States v. Calandra, 414 U.S. 338 (1974), it was argued that each question before a grand jury "based on evidence obtained from an illegal search and seizure constitutes a fresh and independent violation of the witness' constitutional rights," and that such questioning involved "an additional intrusion" into the privacy of the witness "in violation of the

⁴⁷ The public disclosure of aggregated and compiled data has been found to impinge on privacy interests protected under the Freedom of Information Act (FOIA), even if the information was previously available to the public in a scattered, less accessible form. See United States Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989) (FBI "rap sheets," including public-record information on arrests and disposition of criminal charges, qualified for "personal privacy" exemption from disclosure under FOIA, 5 U.S.C. § 552(b)(7)(C)); but cf. Paul v. Davis, 424 U.S. 693, 712-13 (1976) (circulating a flyer publicizing an arrest for shoplifting did not violate constitutional right to privacy). In this case, because section 1842 authorizes the Attorney General to apply for pen register/trap and trace authorities "[n]otwithstanding any other provision of law," 50 U.S.C. § 1842(a)(1), and states that the Court "shall enter an ex parte order . . . approving the installation and use of a pen register or trap and trace device" upon a finding "that the application satisfies the requirements of [section 1842]," id. § 1842(d)(1), the Court has no need to consider how other statutes, such as the Privacy Act, 5 U.S.C. § 552a, might apply to the proposed activities of the Government.

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

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

Fourth Amendment." 414 U.S. at 353 & n.9 (internal quotations omitted). The Court rejected this argument, explaining:

The purpose of the Fourth Amendment is to prevent unreasonable governmental intrusions into the privacy of one's person, house, papers, or effects. . . . That wrong . . . is fully accomplished by the original search without probable cause. Grand jury questions based on evidence obtained thereby involve no independent governmental invasion of one's person, house, papers, or effects Questions based on illegally obtained evidence are only a derivative use of the product of a past unlawful search and seizure. They work no new Fourth Amendment wrong.

414 U.S. at 354 (emphasis added); accord United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990); United States v. Leon, 468 U.S. 897, 906 (1984); see also United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information.").

In this case, sophisticated analysis of archived meta data may yield more information about a person's Internet communications than what would at first be apparent. Nevertheless, such analysis would, like the grand jury questioning in Calandra, involve merely a derivative use of information already obtained, rather than an independent governmental invasion of matters protected by the Fourth

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

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

Amendment. Accordingly, the Court finds that the proposed collection and analysis does not involve a search or seizure under the Fourth Amendment.

B. First Amendment Issues

By letter dated [REDACTED] the Court asked the Government to address "the general First Amendment implications of collecting and retaining this large volume of information that is derived, in part, from the communications of U.S. persons." In response, the Government acknowledges that surveillance that acquires "the contents of communications might in some cases implicate First Amendment interests, in particular the freedom of association," Government's Letter of [REDACTED] at 1, but denies or minimizes the First Amendment implications of surveillance that only acquires non-content addressing information.

The weight of authority supports the conclusion that Government information-gathering that does not constitute a Fourth Amendment search or seizure will also comply with the First Amendment when conducted as part of a good-faith criminal investigation. See Reporters Comm. for Freedom of the Press v. AT&T, 593 F.2d 1030, 1051 (D.C. Cir. 1978) (First Amendment protects activities "subject to the general and incidental

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

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

burdens that arise from good faith enforcement of otherwise valid criminal and civil laws that are not themselves" directed at First Amendment conduct; accordingly, subpoenas to produce reporters' telephone toll records without prior notice did not violate the First Amendment) (emphasis in original); United States v. Aguilar, 883 F.2d 662, 705 (9th Cir. 1989) (use of undercover informants "to infiltrate an organization engaged in protected first amendment activities" must be part of investigation "conducted in good faith; i.e., not for the purpose of abridging first amendment freedoms"); United States v. Gering, 716 F.2d 615, 620 (9th Cir. 1983) (mail covers targeting minister at residence and church upheld against First Amendment challenge absent showing "that mail covers were improperly used and burdened . . . free exercise or associational rights").

Conversely,

all investigative techniques are subject to abuse and can conceivably be used to oppress citizens and groups, rather than to further proper law enforcement goals. In some cases, bad faith use of these techniques may constitute an abridgment of the First Amendment rights of the citizens at whom they are directed.

Reporters Comm., 593 F.2d at 1064.⁴⁸

⁴⁸ Part of Judge Wilkey's opinion in Reporters Comm. categorically concludes that the First Amendment affords no protections against government investigation beyond what is (continued...)

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

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

Here, the proposed collection of meta data is not for ordinary law enforcement purposes, but in furtherance of the compelling national interest of identifying and tracking [REDACTED] and ultimately of thwarting terrorist attacks. The overarching investigative effort against [REDACTED] is not aimed at curtailing First Amendment activities and satisfies the "good faith" requirement described in the above-cited cases. However, the extremely broad nature of this collection carries with it a heightened risk that collected information could be subject to various forms of misuse, potentially involving abridgement of First Amendment rights of innocent persons. For this reason, special restrictions on the accessing, retention, and dissemination of such information are necessary to guard against such misuse. See pages 82-87 below. With such restrictions in place, the proposed collection of non-

⁴⁸(...continued)
provided by the Fourth and Fifth Amendments. Id. at 1053-60. However, that part of the opinion was not joined by the other judge in the majority, who opined that the result of First Amendment analysis "may not always coincide with that attained by application of Fourth Amendment doctrine." Id. at 1071 n.4 (Robinson, J.).

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

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

content addressing information does not violate the First Amendment.⁴⁹

IV. TO ENSURE LAWFUL IMPLEMENTATION OF THIS SURVEILLANCE AUTHORITY, NSA IS ORDERED TO COMPLY WITH THE PROPOSED RESTRICTIONS AND PROCEDURES, AS MODIFIED BY THE COURT.

The proposed collection involves an extraordinarily broad implementation of a type of surveillance that Congress has regulated by statute, even in its conventional, more narrowly targeted form. To ensure that this authority is implemented in a lawful manner, NSA is ordered to comply with the restrictions and procedures set out below at pages 82-87, which the Court has adapted from the Government's application.⁵⁰ Adherence to them

⁴⁹ The court in Paton v. La Prade, 469 F. Supp. 773, 780-82 (D.N.J. 1978), held that a mail cover on a dissident political organization violated the First Amendment because it was authorized under a regulation that was overbroad in its use of the undefined term "national security." In contrast, this pen register/trap and trace surveillance does not target a political group and is authorized pursuant to statute on the grounds of relevance to an investigation to protect against "international terrorism," a term defined at 50 U.S.C. § 1801(c). This definition has been upheld against a claim of First Amendment overbreadth. See United States v. Falvey, 540 F. Supp. 1306, 1314-15 (E.D.N.Y. 1982).

⁵⁰ The principal changes that the Court has made from the procedures described in the application are the inclusion of a "First Amendment proviso" as part of the "reasonable suspicion" standard for an [REDACTED] to be used as the basis for querying archived meta data, see pages 57-58 above, the adoption of a date after which meta data may not be retained, see pages 70-71 below, and an enhanced role for the NSA's Office of
(continued...)

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

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

will help ensure that this information is used for the stated purpose of its collection - the identification and tracking of [REDACTED] [REDACTED] their Internet communications - thereby safeguarding the continued validity of the certification of relevance under § 1842(c)(2). These procedures will also help effectuate 50 U.S.C. § 1845(a)(2), which directs that no information from a Court-authorized pen register or trap and trace device "may be used or disclosed by Federal officers or employees except for lawful purposes," and ensure that such use and disclosure will not abridge First Amendment rights.

The Court's letter of [REDACTED] asked the Government to explain "[f]or how long . . . the information collected under this authority [would] continue to be of operational value to the counter-terrorism investigation(s) for which it is collected." The Government's letter of [REDACTED], stated that such information "would continue to be of significant operational value for at least 18 months," based on NSA's "analytic judgment." [REDACTED] Letter at 3. During that period, meta

⁵⁰(...continued)

General Counsel in the implementation of this authority, see pages 84-85 below. The Court recognizes that, as circumstances change and experience is gained in implementing this authority, the Government may propose other modifications to these procedures.

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

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

data would be available to analysts online for authorized querying. After 18 months, NSA "believes that there continues to be operational value in retaining e-mail meta data . . . in an 'off-line' storage system," since "in certain circumstances" information of that age could "provide valuable leads for the investigation into [REDACTED]" Id. However, the value of such information "would diminish over time," so that "NSA assesses that meta data would have operational value in off-line storage for a period of three years, and could be destroyed after that time (that is, a total of four and one-half years after it was initially collected)." Id. In accordance with this assessment, NSA is ordered to destroy archived meta data collected under this authority no later than four and one-half years after its initial collection.

* * *

Accordingly, a verified application having been made by the Attorney General of the United States for an order authorizing installation and use of pen registers and trap and trace devices pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States Code (U.S.C.), §§ 1801-1811, 1841-1846, and full consideration having been given

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

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

to the matters set forth therein, the Court finds, on the grounds explained above, that:

1. The Attorney General is authorized to approve applications for pen registers and trap and trace devices under the Act and to make such applications under the Act.

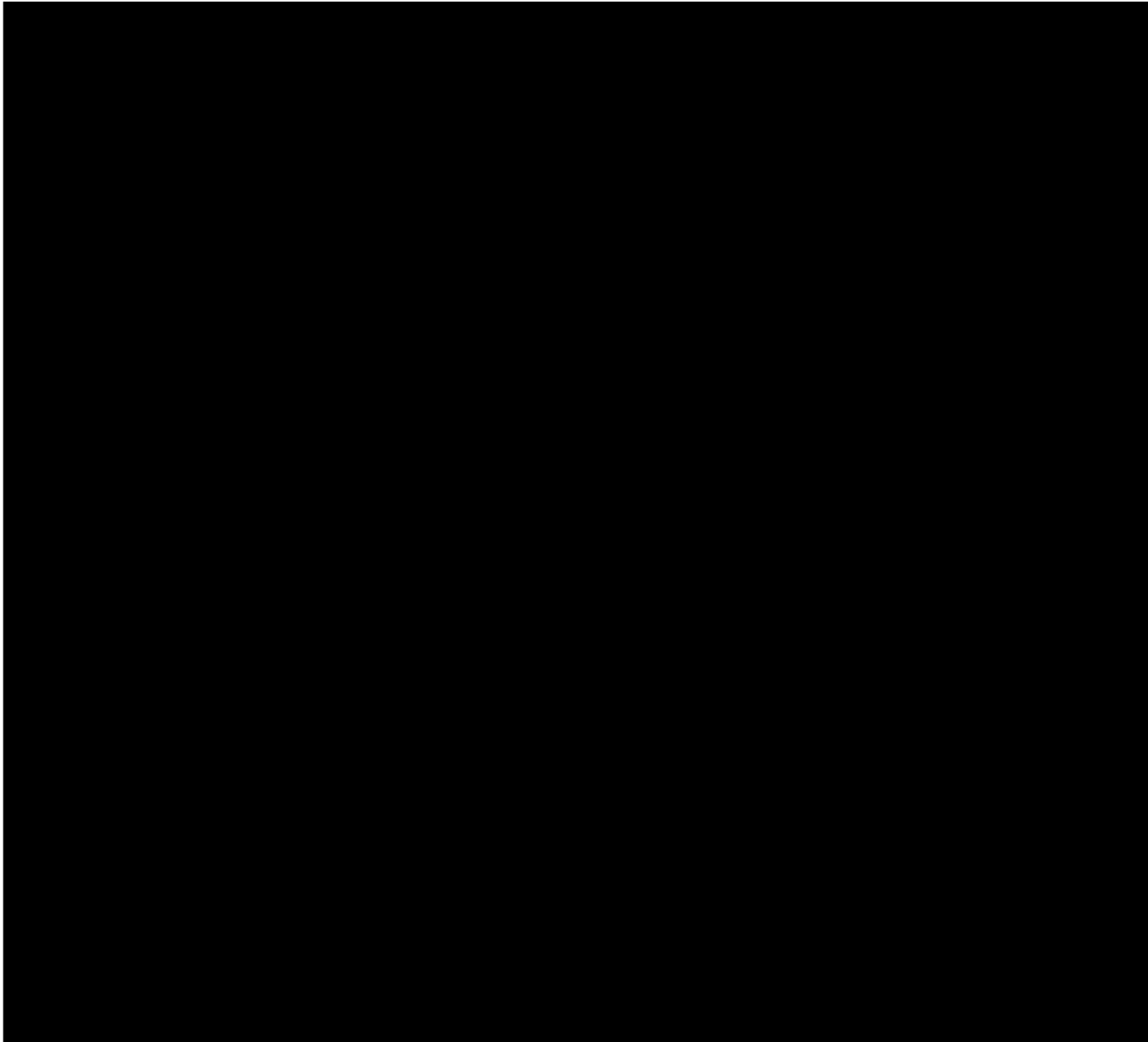
2. The applicant has certified that the information likely to be obtained from the requested pen registers and trap and trace devices is relevant to an ongoing investigation to protect against international terrorism that is not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

3. [REDACTED] in the United States and abroad are the subjects of National Security investigations conducted by the Federal Bureau of Investigation (FBI) under guidelines approved by the Attorney General pursuant to Executive Order No. 12333.

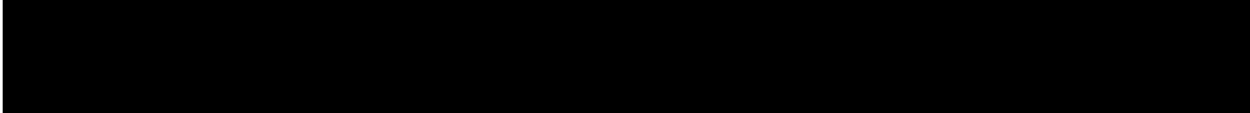
4. The pen registers and trap and trace devices [REDACTED]
[REDACTED]
[REDACTED]


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

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



⁵¹ The Government has represented that it is overwhelmingly likely that at 

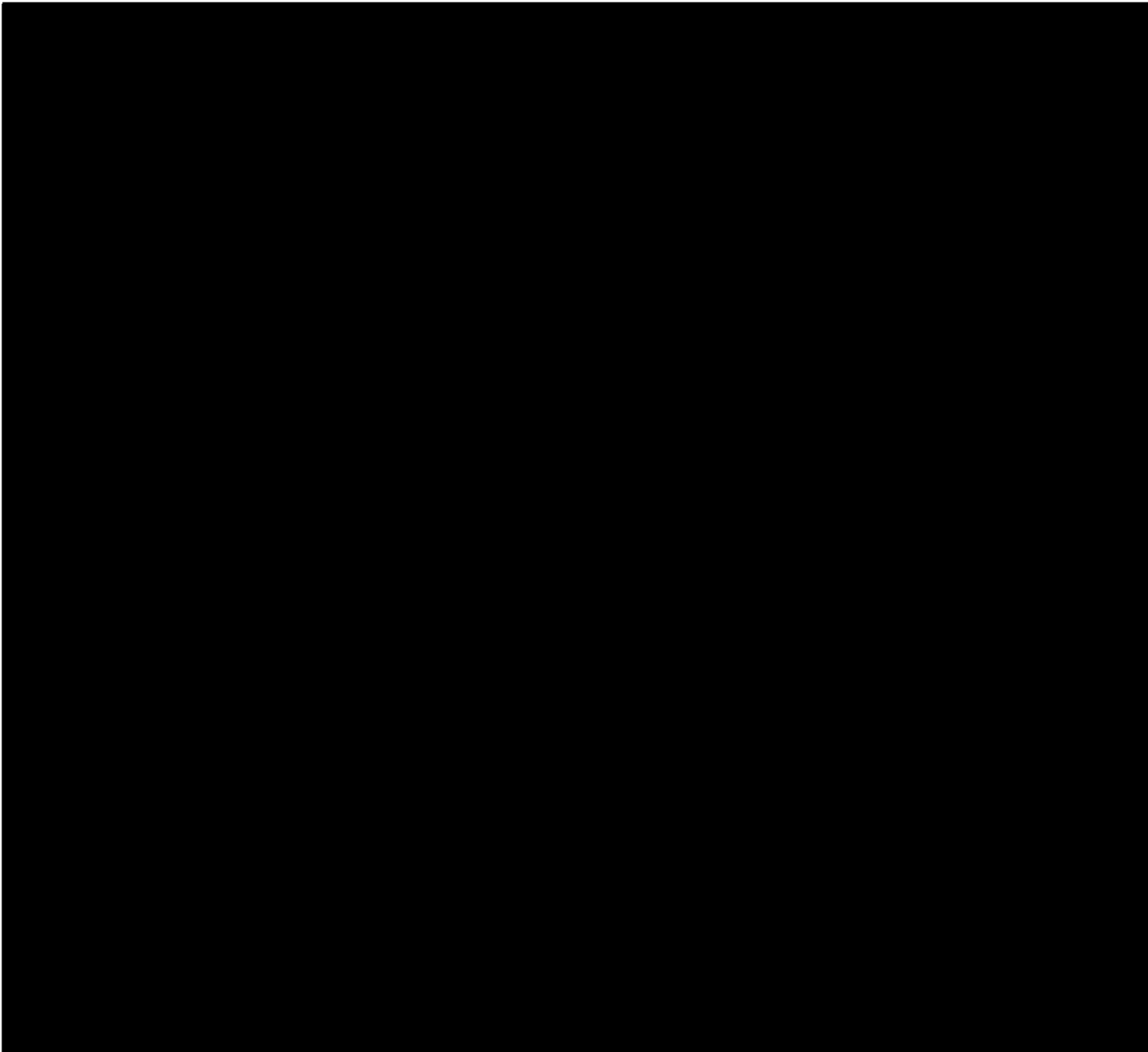


⁵² The Government has represented that it is overwhelmingly likely that 



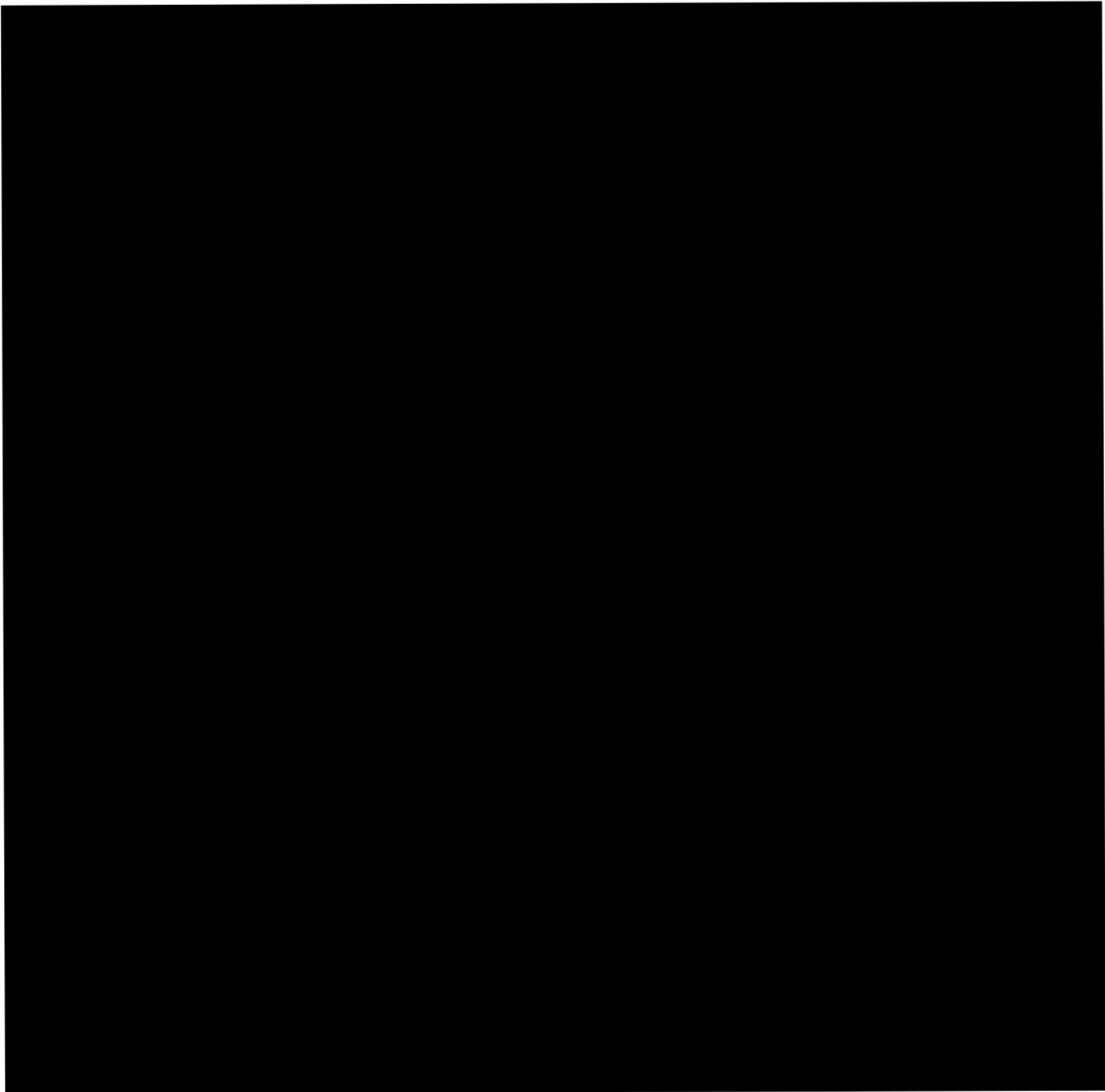
~~TOP SECRET//HCS//COMINT//NOFORN~~

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

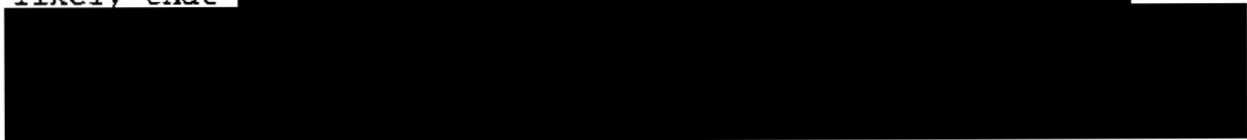


~~TOP SECRET//HCS//COMINT//NOFORN~~

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

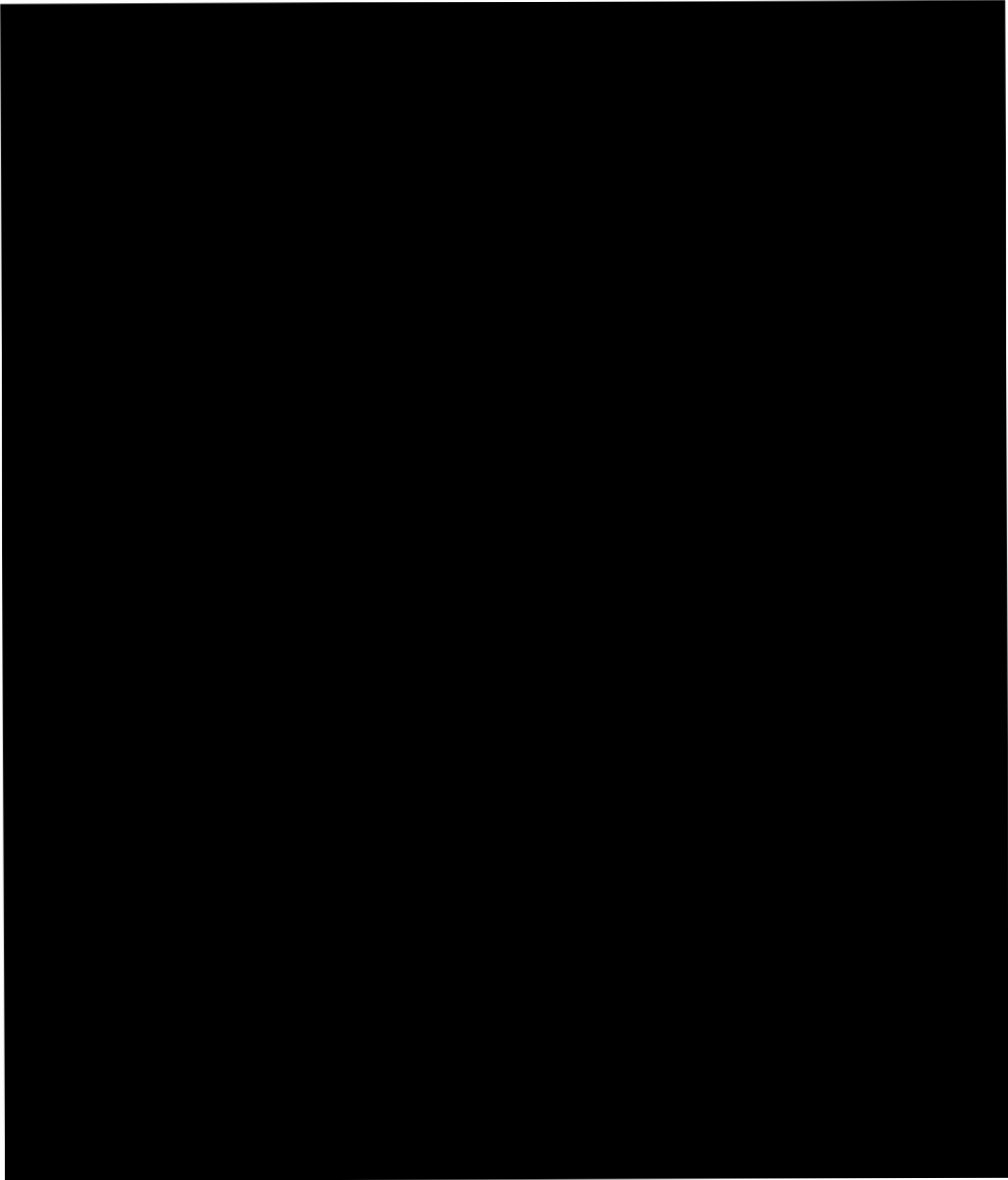


⁵³ The Government has represented that it is overwhelmingly likely that [REDACTED]



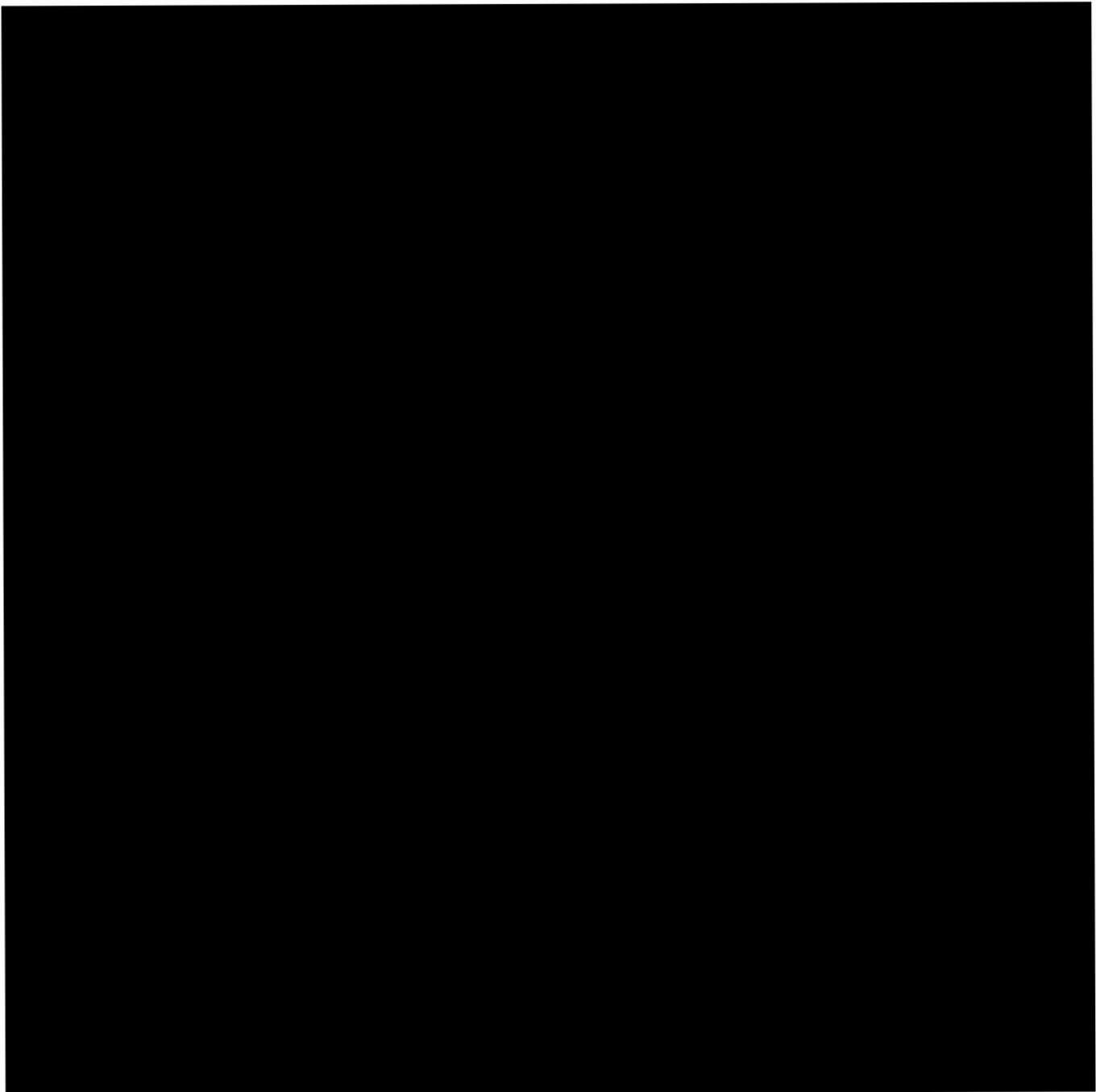
~~TOP SECRET//HCS//COMINT//NOFORN~~

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



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

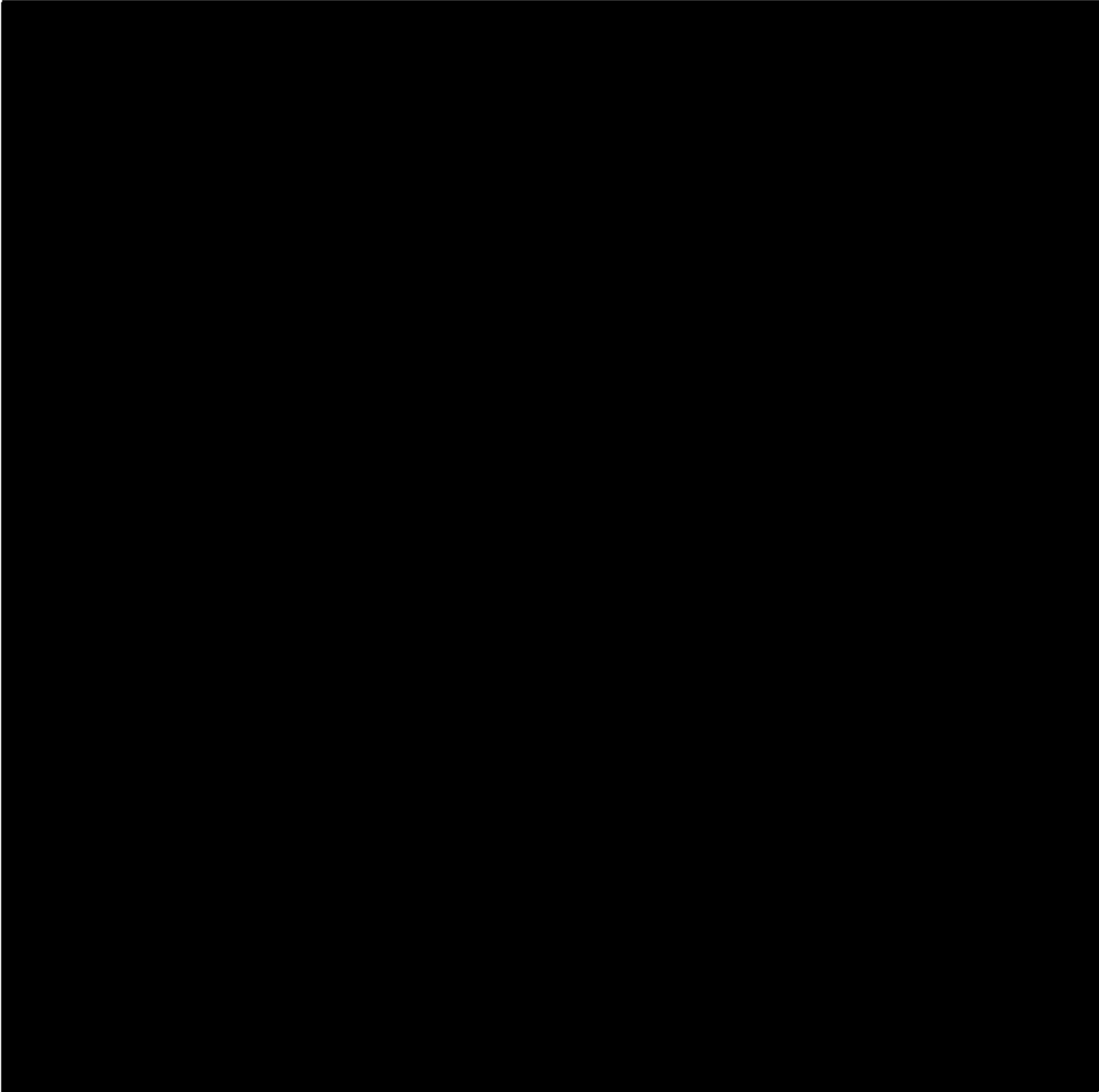
~~TOP SECRET//HCS//COMINT//NOFORN~~



⁵⁴ The Government has represented that the majority of the communications [REDACTED]

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

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



³⁵ Because electronic communications will 



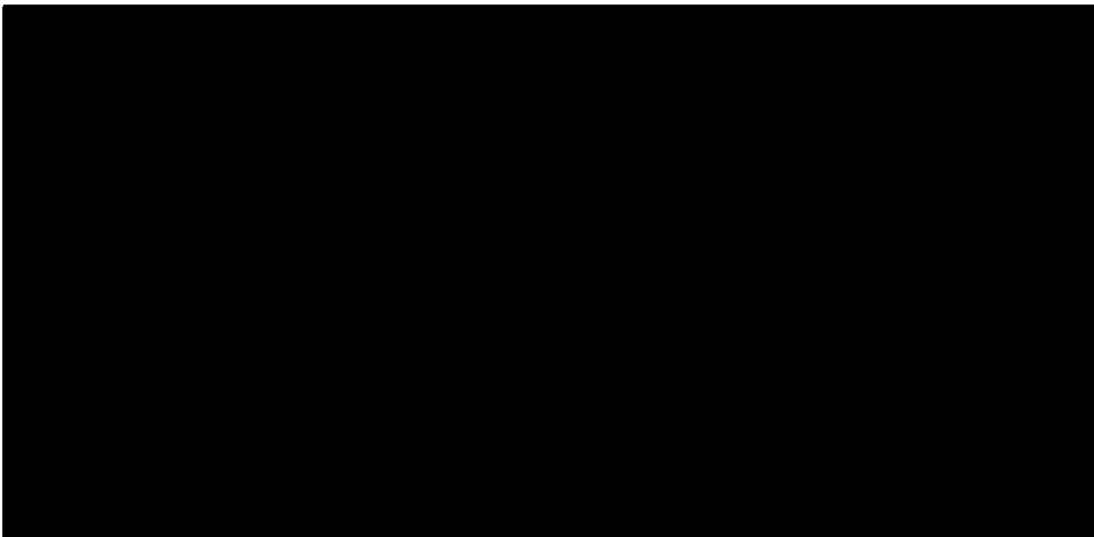
~~TOP SECRET//HCS//COMINT//NOFORN~~

TOP SECRET//HCS//COMINT//NOFORN



TOP SECRET//HCS//COMINT//NOFORN

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



WHEREFORE, the Court finds that the application of the United States [REDACTED] pen registers and trap and trace devices, as described in the application, satisfies the requirements of the Act and specifically of 50 U.S.C. § 1842 and, therefore,

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

FURTHER ORDERED, as follows:

(1) Installation and use of pen registers and trap and trace devices as requested in the Government's application is authorized for a period of **ninety days** from the date of this Opinion and Order, unless otherwise ordered by this Court, as follows: installation and use of pen registers and/or trap and

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

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

trace devices as described above to collect all addressing and routing information reasonably likely to identify the sources or destinations of the electronic communications identified above on [REDACTED] identified above, including the "to," "from," "cc," and "bcc" fields for those communications [REDACTED]

[REDACTED]

[REDACTED] Collection of the contents of such communications as defined by 18 U.S.C. § 2510(8) is not authorized.

(2) The authority granted is within the United States.

(3) As requested in the application, [REDACTED]

[REDACTED] (specified persons), are directed to furnish the NSA with

⁵⁷ Although the application makes clear that the assistance of these specified persons is contemplated, it does not expressly request that the Court direct these specified persons to assist the surveillance. However, because the application, at 24, requests that the Court enter the proposed orders submitted with the application and those proposed orders would direct the specified persons to provide assistance, the application effectively requests the Court to direct such assistance.

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

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

any information, facilities, or technical assistance necessary to accomplish the installation and operation of pen registers and trap and trace devices in such a manner as will protect their secrecy and produce a minimum amount of interference with the services each specified person is providing to its subscribers. Each specified person shall not disclose the existence of the investigation or of the pen registers and trap and trace devices to any person, unless or until ordered by the Court, and shall maintain all records concerning the pen registers and trap and trace devices, or the aid furnished to the NSA, under the security procedures approved by the Attorney General [REDACTED] [REDACTED] that have previously been or will be furnished to each specified person and are on file with this Court.

(4) The NSA shall compensate the specified person(s) referred to above for reasonable expenses incurred in providing such assistance in connection with the installation and use of the pen registers and trap and trace devices herein.

(5) The NSA shall follow the following procedures and restrictions regarding the storage, accessing, and disseminating of information obtained through use of the pen register and trap and trace devices authorized herein:

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

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


a. The NSA shall store such information in a manner that ensures that it will not be commingled with other data.

b. The ability to access such information shall be limited to ten specially cleared analysts and to specially cleared administrators. The NSA shall ensure that the mechanism for accessing such information will automatically generate a log of auditing information for each occasion when the information is accessed, to include the accessing user's login, IP address, date and time, and retrieval request.

c. Such information shall be accessed only through queries using the contact chaining [REDACTED] methods described at page 43 above. Such queries shall be performed only on the basis of a particular known [REDACTED] [REDACTED] after the NSA has concluded, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, that there are facts giving rise to a reasonable articulable suspicion that [REDACTED] is associated with [REDACTED] [REDACTED] provided, however, that [REDACTED] believed to be used by a U.S. person shall not be regarded as associated with [REDACTED]

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

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

 solely on the basis of activities that are protected by the First Amendment to the Constitution. Queries shall only be conducted with the approval of one of the following NSA officials: the Program Manager, Counterterrorism Advanced Analysis; the Chief or Deputy Chief, Counterterrorism Advanced Analysis Division; or a Counterterrorism Advanced Analysis Shift Coordinator in the Analysis and Production Directorate of the Signals Intelligence Directorate.

d. Because the implementation of this authority involves distinctive legal considerations, NSA's Office of General Counsel shall:

i) ensure that analysts with the ability to access such information receive appropriate training and guidance regarding the querying standard set out in paragraph c. above, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of such information.

ii) monitor the designation of individuals with access to such information under paragraph b. above and the functioning of the automatic logging of auditing information required by paragraph b. above.

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

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

iii) to ensure appropriate consideration of any First Amendment issues, review and approve proposed queries of meta data in online or "off-line" storage based on seed accounts used by U.S. persons.⁵⁸

e. The NSA shall apply the Attorney General-approved guidelines in United States Signals Intelligence Directive 18 (Attachment D to the application) to minimize information concerning U.S. persons obtained from the pen registers and trap and trace devices authorized herein. Prior to disseminating any U.S. person information outside of the NSA, the Chief of Customer Response in the NSA's Signals Intelligence Directorate shall determine that the information is related to counterterrorism information and is necessary to understand the counterterrorism information or to assess its importance.

f. Information obtained from the authorized pen registers and trap and trace devices shall be available

⁵⁸ The Court notes that, in conventional pen register/trap and trace surveillances, there is judicial review of the application before any [REDACTED] In this case, the analogous decision to use a particular e-mail account as a seed account takes place [REDACTED] In these circumstances, it shall be incumbent on NSA's Office of General Counsel to review the legal adequacy for the basis of such queries, including the First Amendment proviso, set out in paragraph c. above.

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

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

online for querying, as described in paragraphs b. and c. above, for eighteen months. After such time, such information shall be transferred to an "off-line" tape system, which shall only be accessed by a cleared administrator in order to retrieve information that satisfies the standard for online accessing stated in paragraph c. above and is reasonably believed, despite its age, to be relevant to an ongoing investigation of [REDACTED]

[REDACTED] Searches of meta data in "off-line" storage shall be approved by one of the officials identified in paragraph c. above.

g. Meta data shall be destroyed no later than 18 months after it is required to be put into "off-line" storage, i.e., no later than four and one-half years after its initial collection.

h. Any application to renew or reinstate the authority granted herein shall include:

i) a report discussing queries that have been made since the prior application to this Court and the NSA's application of the standard set out in paragraph c. above to those queries.

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

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

ii) detailed information regarding [redacted]
[redacted] proposed to be added to such authority.

iii) any changes in the description of the
[redacted] above or in the nature of the
communications [redacted]

iv) any changes in the proposed means of
collection, to include [redacted]
[redacted] the pen register and/or trap and trace
devices [redacted]

Signed [redacted] 10:30 a.m. E.D.T.
Date Time

This authorization regarding [redacted]
[redacted] in the United States and Abroad expires on the
[redacted] at 5:00 p.m., Eastern Daylight Time.

Colleen Kollar-Kotelly
COLLEEN KOLLAR-KOTELLY
Presiding Judge, United States Foreign
Intelligence Surveillance Court

TOP SECRET//HCS//COMINT//NOFORN

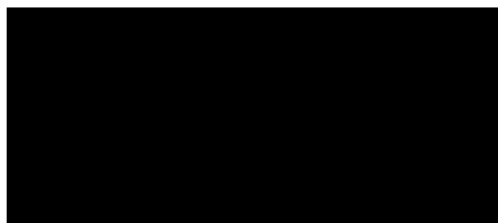


EXHIBIT R

All redacted information exempt under (b)(1) and (b)(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT



:
:
:
:
:

Docket No.: BR 08-13

SUPPLEMENTAL OPINION

This Supplemental Opinion memorializes the Court’s reasons for concluding that the records to be produced pursuant to the orders issued in the above-referenced docket number are properly subject to production pursuant to 50 U.S.C.A. § 1861 (West 2003 & Supp. 2008), notwithstanding the provisions of 18 U.S.C.A. §§ 2702-2703 (West 2000 & Supp. 2008), amended by Public Law 110-401, § 501(b)(2) (2008).

As requested in the application, the Court is ordering production of telephone “call detail records or ‘telephony metadata,’” which “includes comprehensive communications routing information, including but not limited to session identifying information . . . , trunk identifier, telephone calling card numbers, and time and duration of [the] calls,” but “does not include the substantive content of any communication.” Application at 9; Primary Order at 2. Similar productions have been ordered by judges of the Foreign Intelligence Surveillance Court (“FISC”). See Application at 17. However, this is the first application in which the government has identified the provisions of 18 U.S.C.A. §§ 2702-2703 as potentially relevant to whether such orders could properly be issued under 50 U.S.C.A. § 1861. See Application at 6-8.

Pursuant to section 1861, the government may apply to the FISC “for an order requiring the production of any tangible things (including books, records, papers, documents, and other items).” 50 U.S.C.A. § 1861(a)(1) (emphasis added). The FISC is authorized to issue the order, “as requested, or as modified,” upon a finding that the application meets the requirements of that section. Id. at § 1861(c)(1). Under the rules of statutory construction, the use of the word “any” in a statute naturally connotes “an expansive meaning,” extending to all members of a common set, unless Congress employed “language limiting [its] breadth.” United States v. Gonzales, 520 U.S. 1, 5 (1997); accord Ali v. Federal Bureau of Prisons, 128 S. Ct. 831, 836 (2008)

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

(“Congress’ use of ‘any’ to modify ‘other law enforcement officer’ is most naturally read to mean law enforcement officers of whatever kind.”).¹

However, section 2702, by its terms, describes an apparently exhaustive set of circumstances under which a telephone service provider may provide to the government non-content records pertaining to a customer or subscriber. See § 2702(a)(3) (except as provided in § 2702(c), a provider “shall not knowingly divulge a record or other [non-content] information pertaining to a subscriber or customer . . . to any governmental entity”). In complementary fashion, section 2703 describes an apparently exhaustive set of means by which the government may compel a provider to produce such records. See § 2703(c)(1) (“A governmental entity may require a provider . . . to disclose a record or other [non-content] information pertaining to a subscriber . . . or customer . . . only when the governmental entity” proceeds in one of the ways described in § 2703(c)(1)(A)-(E)) (emphasis added). Production of records pursuant to a FISC order under section 1861 is not expressly contemplated by either section 2702(c) or section 2703(c)(1)(A)-(E).

If the above-described statutory provisions are to be reconciled, they cannot all be given their full, literal effect. If section 1861 can be used to compel production of call detail records, then the prohibitions of section 2702 and 2703 must be understood to have an implicit exception for production in response to a section 1861 order. On the other hand, if sections 2702 and 2703 are understood to prohibit the use of section 1861 to compel production of call detail records, then the expansive description of tangible things obtainable under section 1861(a)(1) must be construed to exclude such records.

The apparent tension between these provisions stems from amendments enacted by Congress in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (“USA PATRIOT Act”), Public Law 107-56, October 26, 2001, 115 Stat. 272. Prior to the USA PATRIOT Act, only limited types of records, not

¹ The only express limitation on the type of tangible thing that can be subject to a section 1861 order is that the tangible thing “can 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.” Id. at § 1861(c)(2)(D). Call detail records satisfy this requirement, since they may be obtained by (among other means) a “court order for disclosure” under 18 U.S.C.A. § 2703(d). Section 2703(d) permits the government to obtain a court order for release of non-content records, or even in some cases of the contents of a communication, upon a demonstration of relevance to a criminal investigation.

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

including call detail records, were subject to production pursuant to FISC orders.² Section 215 of the USA PATRIOT Act replaced this prior language with the broad description of “any tangible thing” now codified at section 1861(a)(1). At the same time, the USA PATRIOT Act amended sections 2702 and 2703 in ways that seemingly re-affirmed that communications service providers could divulge records to the government only in specified circumstances,³ without expressly referencing FISC orders issued under section 1861.

The government argues that section 1861(a)(3) supports its contention that section 1861(a)(1) encompasses the records sought in this case. Under section 1861(a)(3), which Congress enacted in 2006,⁴ applications to the FISC for production of several categories of sensitive records, including “tax return records” and “educational records,” may be made only by the Director, the Deputy Director or the Executive Assistant Director for National Security of the Federal Bureau of Investigation (“FBI”). 18 U.S.C.A. § 1861(a)(3). The disclosure of tax return records⁵ and educational records⁶ is specifically regulated by other federal statutes, which do not by their own terms contemplate production pursuant to a section 1861 order. Nonetheless, Congress clearly intended that such records could be obtained under a section 1861 order, as demonstrated by their inclusion in section 1861(a)(3). But, since the records of telephone service providers are not mentioned in section 1861(a)(3), this line of reasoning is not directly on point. However, it does at least demonstrate that Congress may have intended the sweeping description of tangible items obtainable under section 1861 to encompass the records of telephone service providers, even though the specific provisions of sections 2702 and 2703 were not amended in order to make that intent unmistakably clear.

² See 50 U.S.C.A. § 1862(a) (West 2000) (applying to records of transportation carriers, storage facilities, vehicle rental facilities, and public accommodation facilities).

³ Specifically, the USA PATRIOT Act inserted the prohibition on disclosure to governmental entities now codified at 18 U.S.C.A. § 2702(a)(3), and exceptions to this prohibition now codified at 18 U.S.C.A. § 2702(c). See USA PATRIOT Act § 212(a)(1)(B)(iii) & (E). The USA PATRIOT Act also amended the text of 18 U.S.C.A. § 2703(c)(1) to state that the government may require the disclosure of such records only in circumstances specified therein. See USA PATRIOT Act § 212(b)(1)(C)(i).

⁴ See Public Law 109-177 § 106(a)(2) (2006).

⁵ See 26 U.S.C.A. § 6103(a) (West Supp. 2008), amended by Public Law 110-328 § 3(b)(1) (2008).

⁶ See 20 U.S.C.A. § 1232g(b) (West 2000 & Supp. 2008).

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

The Court finds more instructive a separate provision of the USA PATRIOT Act, which also pertains to governmental access to non-content records from communications service providers. Section 505(a) of the USA PATRIOT Act amended provisions, codified at 18 U.S.C.A. § 2709 (West 2000 & Supp. 2008), enabling the FBI, without prior judicial review, to compel a telephone service provider to produce “subscriber information and toll billing records information.” 18 U.S.C.A. § 2709(a).⁷ Most pertinently, section 505(a)(3)(B) of the USA PATRIOT Act lowered the predicate required for obtaining such information to a certification submitted by designated FBI officials asserting its relevance to an authorized foreign intelligence investigation.⁸

Indisputably, section 2709 provides a means for the government to obtain non-content information in a manner consistent with the text of sections 2702-2703.⁹ Yet section 2709 merely requires an FBI official to provide a certification of relevance. In comparison, section 1861 requires the government to provide to the FISC a “statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant” to a foreign intelligence investigation,¹⁰ and the FISC to determine that the application satisfies this

⁷ This process involves service of a type of administrative subpoena, commonly known as a “national security letter.” David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 19:2 (2007).

⁸ Specifically, a designated FBI official must certify that the information or records sought are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.” 18 U.S.C.A. § 2709(b)(1)-(2) (West Supp. 2008). Prior to the USA PATRIOT Act, the required predicate for obtaining “local and long distance toll billing records of a person or entity” was “specific and articulable facts giving reason to believe that the person or entity . . . is a foreign power or an agent of a foreign power.” See 18 U.S.C.A. § 2709(b)(1)(B) (West 2000).

⁹ Section 2703(c)(2) permits the government to use “an administrative subpoena” to obtain certain categories of non-content information from a provider, and section 2709 concerns use of an administrative subpoena. See note 7 supra.

¹⁰ 50 U.S.C.A. § 1861(b)(2)(A). More precisely, the investigation must be “an authorized investigation (other than a threat assessment) . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities,” id., “provided that such investigation of a United States

(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

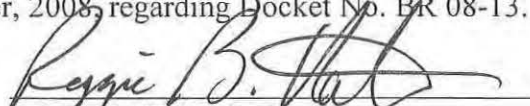
~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

requirement, see 50 U.S.C.A. § 1861(c)(1), before records are ordered produced. It would have been anomalous for Congress, in enacting the USA PATRIOT Act, to have deemed the FBI's application of a "relevance" standard, without prior judicial review, sufficient to obtain records subject to sections 2702-2703, but to have deemed the FISC's application of a closely similar "relevance" standard insufficient for the same purpose. This anomaly is avoided by interpreting sections 2702-2703 as implicitly permitting the production of records pursuant to a FISC order issued under section 1861.

It is the Court's responsibility to attempt to interpret a statute "as a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into an harmonious whole." Food & Drug Admin. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000) (internal quotations and citations omitted). For the foregoing reasons, the Court is persuaded that this objective is better served by the interpretation that the records sought in this case are obtainable pursuant to a section 1861 order.

However, to the extent that any ambiguity may remain, it should be noted that the legislative history of the USA PATRIOT Act is consistent with this expansive interpretation of section 1861(a)(1). See 147 Cong. Rec. 20,703 (2001) (statement of Sen. Feingold) (section 215 of USA PATRIOT Act "permits the Government . . . to compel the production of records from any business regarding any person if that information is sought in connection with an investigation of terrorism or espionage;" "all business records can be compelled, including those containing sensitive personal information, such as medical records from hospitals or doctors, or educational records, or records of what books somebody has taken out from the library") (emphasis added). In this regard, it is significant that Senator Feingold introduced an amendment to limit the scope of section 1861 orders to records "not protected by any Federal or State law governing access to the records for intelligence or law enforcement purposes," but this limitation was not adopted. See 147 Cong. Rec. 19,530 (2001).

ENTERED this 12th day of December, 2008, regarding Docket No. BR 08-13.


REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

¹⁰(...continued)

person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Id. § 1861(a)(1). The application must also include minimization procedures in conformance with statutory requirements, which must also be reviewed by the FISC. Id. § 1861(b)(2)(B), (c)(1), & (g).

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~