

1 CINDY COHN (SBN 145997)
 cindy@eff.org
 2 LEE TIEN (SBN 148216)
 KURT OPSAHL (SBN 191303)
 3 MARK RUMOLD (SBN 279060)
 DAVID GREENE (SBN 160107)
 4 JAMES S. TYRE (SBN 083117)
 ANDREW CROCKER (SBN 291596)
 5 ELECTRONIC FRONTIER FOUNDATION
 815 Eddy Street
 6 San Francisco, CA 94109
 Telephone: 415/436-9333; Fax: 415/436-9993
 7
 THOMAS E. MOORE III (SBN 115107)
 8 tmoore@rroyselaw.com
 ROYSE LAW FIRM, PC
 9 1717 Embarcadero Road
 Palo Alto, CA 94303
 10 Telephone: 650/813-9700; Fax: 650/813-9777

RACHAEL E. MENY (SBN 178514)
 rmeny@kvn.com
 MICHAEL S. KWUN (SBN 198945)
 BENJAMIN W. BERKOWITZ (SBN 244441)
 JUSTINA K. SESSIONS (SBN 270914)
 PHILIP J. TASSIN (SBN 287787)
 KEKER & VAN NEST, LLP
 633 Battery Street
 San Francisco, CA 94111
 Telephone: 415/391-5400; Fax: 415/397-7188
 RICHARD R. WIEBE (SBN 121156)
 wiebe@pacbell.net
 LAW OFFICE OF RICHARD R. WIEBE
 One California Street, Suite 900
 San Francisco, CA 94111
 Telephone: 415/433-3200; Fax: 415/433-6382
 ARAM ANTARAMIAN (SBN 239070)
 aram@eff.org
 LAW OFFICE OF ARAM ANTARAMIAN
 1714 Blake Street
 Berkeley, CA 94703
 Telephone: (510) 289-1626

11
12
13 *Counsel for Plaintiffs*

14 **UNITED STATES DISTRICT COURT**
 15 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
 16 **OAKLAND DIVISION**

17 FIRST UNITARIAN CHURCH OF LOS)
 ANGELES, *et al.*,)
 18)
 Plaintiffs,)
 19)
 v.)
 20)
 NATIONAL SECURITY AGENCY, *et al.*,)
 21)
 Defendants.)
 22)
 23)
 24)

Case No. 4:13-cv-03287-JSW
PLAINTIFFS' REQUEST FOR JUDICIAL NOTICE
 Courtroom 5, 2nd Floor
 The Honorable Jeffrey S. White

PLAINTIFFS' REQUEST FOR JUDICIAL NOTICE

1
2 Pursuant to Federal Rule of Evidence 201 and the inherent authority of the Court, Plaintiffs
3 respectfully request that the Court take judicial notice of a fact established by a government filing
4 in the Foreign Intelligence Surveillance Court (“FISC”) made by the National Security Division of
5 the Department of Justice, and an order of the FISC attached hereto as Exhibits A and B. The
6 documents confirm, consistent with Plaintiffs’ arguments, that AT&T, Verizon, Verizon Wireless,
7 and Sprint have participated in the NSA’s phone records program. Plaintiffs respectfully requests
8 that the Court take judicial notice of this fact.

9 The filing in Exhibit A was made in connection with a FISC proceeding, Docket Number
10 BR 10-10, in which the government requested and was granted an order compelling
11 telecommunications companies to produce telephone call records. The phone records order the
12 FISC issued in Docket Number BR 10-10 is attached hereto as Exhibit B. The filing in Exhibit A
13 identifies in its caption the following telecommunications companies that were compelled by the
14 order in BR 10-10 to produce the telephone records of their customers:

15 In Re Application of the Federal Bureau of Investigation for an Order Requiring
16 the Production of Tangible Things from AT&T, the Operating Subsidiaries of
17 Verizon Communications, Inc., and Cellco Partnership d/b/a Verizon Wireless,
and Sprint.

18 Exhibit A at 1. In other words, the letter confirms the participation of AT&T, Verizon,
19 Verizon Wireless, and Sprint in the NSA’s call-records program.

20 Exhibit A was released in response to a Freedom of Information Act lawsuit, *see*
21 Scheduling Order, *New York Times v. NSA*, ECF No. 10, No. 15-2383 (S.D.N.Y May 15, 2015),
22 and was made public on August 15, 2015. Exhibit B was released by the Director of National
23 Intelligence on his official website. It concerns a “compliance incident” in the NSA’s call-records
24 program—the same program at issue in this lawsuit.

25 In this case, the government has claimed that Plaintiffs lack standing because it “has not
26 officially acknowledged the identities of the providers from which the Government continues to
27 collect telephony metadata in bulk. Thus Plaintiffs can only speculate as to whether providers from
28 which they receive telephone service have participated in the program.” Def. Mot. to Dismiss at

1 14, n. 5, ECF No. 66. However, the attached government filing and FISC court order demonstrate
2 that the NSA has indeed collected phone records in bulk from AT&T, Verizon, Verizon Wireless,
3 and Sprint under Section 215. This is consistent with the evidence showing that Plaintiffs'
4 telephone service providers have participated in the program. *See, e.g.*, Decl. of Shahid Buttar for
5 The Bill of Rights Defense Committee ¶ 3, ECF No. 27 (Verizon subscriber); Decl. of the Rev.
6 Rick Hoyt for the First Unitarian Church of Los Angeles ¶ 9, ECF No. 37 (Verizon subscriber);
7 Decl. of Jay Jacobson for the Franklin Armory ¶ 6, ECF No. 34 (Verizon Business subscriber);
8 Decl. of Deepa Padmanabha for Greenpeace ¶¶ 12-13, ECF No. 38 (Verizon subscriber); Decl. of
9 Dinah Pokempner for Human Rights Watch ¶ 12, ECF No. 39; Decl. of Tracy Rosenberg for
10 Media Alliance ¶ 5, ECF No. 40 (AT&T subscriber); Decl. of Dale Gieringer for the California
11 Chapter of NORML ¶ 6, ECF No. 42 (Verizon subscriber); Decl. of Deborah Liu for People for the
12 American Way ¶ 8, ECF No. 43 (Verizon Business subscriber); Decl. of Rabbi Arthur Waskow for
13 The Shalom Center ¶ 3, ECF No. 46 (Verizon Wireless subscriber); Decl. of Berin Szoka on behalf
14 of Tech Freedom ¶ 3, ECF No. 48 (Verizon subscriber).

15 **LEGAL AUTHORITIES IN SUPPORT OF THIS REQUEST FOR JUDICIAL NOTICE**

16 Federal Rule of Evidence 201 authorizes this Court to take judicial notice of the fact of
17 AT&T, Verizon, Verizon Wireless, and Sprint's participation in the Section 215 phone records
18 program. That fact "is not subject to reasonable dispute because it . . . can be accurately and
19 readily determined from sources whose accuracy cannot reasonably be questioned." Fed. Rule
20 Evid. 201(b); *Singh v. Ashcroft*, 393 F.3d 903, 905 (9th Cir. 2004). "The rule instructs that where a
21 party has properly requested such notice and supplied the court with the necessary information, a
22 court 'shall take judicial notice.'" *Hotel Employees and Restaurant Employees Local 2 v. Vista Inn.*
23 *Management Co.*, 393 F. Supp.2d 972, 977 (N.D. Cal. 2005) (quoting Fed. Rule Evid. 201(d)).
24 Further, the Rule authorizes judicial notice "at any stage of the proceeding," Fed. Rule Evid.
25 201(f).

26 The fact of AT&T, Verizon, Verizon Wireless, and Sprint's participation can and should be
27 judicially noticed because it is established by sources whose accuracy cannot reasonably be
28 questioned and therefore is not subject to reasonable dispute. Both exhibits are records of the FISC

1 that have become matters of public record. Exhibit A was released by the government in response
2 to a FOIA request, making it a matter of public record. *See In re Am. Apparel, Inc. S'holder Litig.*,
3 855 F. Supp. 2d 1043, 1064 (C.D. Cal. 2012) (citation omitted). Exhibit B was publicly released
4 by the Director of National Intelligence, and remains available at
5 <http://www.dni.gov/files/documents/11714/FISC%20Order,%20BR%2010-10.pdf>.

6 **CONCLUSION**

7 Accordingly, Plaintiffs respectfully request that this Court take judicial notice that AT&T,
8 Verizon, Verizon Wireless, and Sprint have participated in the NSA's phone records program.

9 Dated: September 11, 2015

Respectfully submitted,

10 *s/ Thomas E. Moore III*
11 THOMAS E. MOORE III
12 ROYSE LAW FIRM

13 CINDY COHN
14 LEE TIEN
15 KURT OPSAHL
16 JAMES S. TYRE
17 MARK RUMOLD
18 ANDREW CROCKER
19 DAVID GREENE
20 ELECTRONIC FRONTIER FOUNDATION

21 RICHARD R. WIEBE
22 LAW OFFICE OF RICHARD R. WIEBE

23 RACHAEL E. MENY
24 MICHAEL S. KWUN
25 BENJAMIN W. BERKOWITZ
26 JUSTINA K. SESSIONS
27 PHILIP J. TASSIN
28 KEKER & VAN NEST LLP

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Counsel for Plaintiffs

Exhibit A

Exhibit A



U.S. Department of Justice

National Security Division SURVEILLANCE

2010 AUG -2 PM 4:32

TOP SECRET//COMINT//NOFORN

Washington, D.C. 20530

The Honorable John D. Bates
 United States Foreign Intelligence Surveillance Court
 U.S. Courthouse
 333 Constitution Avenue, N.W.
 Washington, D.C. 20001

Re: Compliance Incident Involving In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from AT&T, the Operating Subsidiaries of Verizon Communications Inc., and Celco Partnership d/b/a Verizon Wireless, and Sprint Relating to al Qaeda and Associated Terrorist Organizations and Unknown Persons in the United States and Abroad Affiliated with al Qaeda and Associated Terrorist Organizations and the Government of Iran and Associated Terrorist Organizations and Unknown Persons in the United States and Abroad Affiliated with the Government of Iran and Associated Terrorist Organizations, Docket Number BR 10-10. (TS)

Dear Judge Bates:

Pursuant to Rule 10(c) of the Foreign Intelligence Surveillance Court (FISC) Rules of Procedure, effective February 17, 2006, this letter further advises the Court of a compliance incident regarding docket number BR 10-10. A preliminary notice regarding the incident was filed with the Court on July 26, 2010. (S)

On February 26, 2010, in docket number BR 10-10, Judge Reggie B. Walton approved an application for tangible things. Judge Walton renewed that authority on May 14, 2010, in docket number BR 10-17, expiring on August 6, 2010. The Court's Primary Order in docket number BR 10-10 states: "The BR metadata may be accessed for the purposes of ensuring data integrity and developing and testing any technological measures designed to enable the NSA to comply with the Court's orders." Docket Number BR 10-10, Primary Order at 5. "Persons who query the BR metadata pursuant to this paragraph may only share the results of any such query with other specially-cleared NSA technical personnel," with limited exceptions, including when "a data integrity analyst [DIA] conduct[s] the query using a RAS-approved telephone identifier at the request of an analyst authorized to query the BR metadata" *Id.* at 5-6. (TS//SI/NF)

On July 16, 2010, the National Security Agency (NSA) advised the Department of Justice's National Security Division of the compliance incident described below:

TOP SECRET//COMINT//NOFORN

Classified by: David S. Kris, Assistant
Attorney General, NSD, DOJ

Reason: 1.4(c)

Declassify on: 2 August 2035

DOCID: 4230249

REF ID:A4197247

TOP SECRET//COMINT//NOFORN

- On March 9, 2010, a DIA queried the BR metadata in response to a Federal Bureau of Investigation (FBI) request for certain information relating to a United States telephone identifier referenced in a previously issued NSA report. Specifically, the FBI inquired whether the BR metadata contained information indicating that the identifier was roaming during in the [REDACTED] to [REDACTED] time frame. (TS//SI//NF)
- The reasonable, articulable suspicion (RAS) approval for the identifier expired on [REDACTED], [REDACTED], [REDACTED] before the query. (It had been RAS-approved on [REDACTED], [REDACTED].) Still, the identifier was listed on the Station Table – historically, NSA’s list of identifiers that have undergone RAS determinations – as RAS-approved until [REDACTED], [REDACTED] at which time its status was changed to “not approved.” (TS//SI//NF)
- The DIA used the identifier to conduct a single query of the BR metadata in the Transaction Database. Although the preliminary notice of this incident reported that the query was time-bounded to the period of [REDACTED] through [REDACTED], the query was not time-bounded. Rather, the DIA focused his review of the query results to the time period referenced in the FBI’s request for information. (TS//SI//NF)
- Based on the query results, the DIA determined that no roaming data was available for the identifier, and NSA provided that information to the FBI. NSA did not issue a report based on this query. (TS//SI//NF)

This incident was discovered by the staff of NSA’s Inspector General through their review of controls used to comply with the Court’s Orders in this matter. NSA confirms that it conducted no queries using the identifier after the DIA’s query described above. (TS//SI//NF)

At the time of this incident, NSA managed the RAS-approval status of identifiers on the Station Table through a periodic, manual review of those identifiers. NSA assesses that this compliance incident resulted from delays in the manual review process. NSA further assesses that a technical modification likely will prevent this sort of compliance incident from occurring in the future. In June 2010, NSA implemented a new program to manage and track requests to approve the use of identifiers that meet the RAS standard. This new program, among other things, automatically changes an identifier’s status to “not approved” if it has not been re-approved for RAS within the time frame specified by the Court’s orders. (TS//SI//NF)

[REDACTED], Global Capabilities Manager, Counterterrorism, reviewed a draft of this letter and confirmed its accuracy. (U)

Sincerely,

[REDACTED]
Section Chief, Oversight
National Security Division
U.S. Department of Justice

cc: The Honorable Reggie B. Walton

TOP SECRET//COMINT//NOFORN

Exhibit B

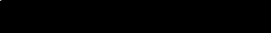
Exhibit B


~~TOP SECRET//COMINT//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 



Docket Number: BR

10-10

PRIMARY ORDER

A verified application having been made by a designee of the Director of the Federal Bureau of Investigation (FBI), the Deputy Director of the 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 production to the National Security Agency (NSA) of the tangible

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

Derived from: Pleadings in the above-captioned docket
Declassify on: 19 February 2035

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

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 09-19 and its predecessors. [50 U.S.C. § 1861(c)(1)]

Accordingly, the Court finds that the application of the United States to obtain the tangible things, as described below,

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

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

satisfies the requirements of the Act and, therefore,

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

FURTHER ORDERED, as follows:

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

B. The Custodian of Records of [REDACTED]

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

¹ For purposes of this Order "telephony metadata" includes comprehensive communications routing 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//COMINT//NOFORN~~

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

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 [REDACTED] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [REDACTED]

[REDACTED]

(2) With respect to any information the FBI receives as a result of this Order (information that 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.

Notwithstanding the requirements set forth below, Executive Branch and Legislative Branch personnel may be permitted

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

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

appropriate access to the BR metadata and certain information derived therefrom in order to facilitate their lawful oversight functions, which include, but are not limited to, those set forth below.

B. The BR metadata may be accessed for the purposes of ensuring data integrity and developing and testing any technological measures designed to enable the NSA to comply with the Court's orders. Access to the BR metadata for such purposes shall be limited to the NSA Collection Managers, Data Integrity Analysts, and System Administrators described in paragraph 16 of the Declaration of [REDACTED] Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate, the National Security Agency, filed as Exhibit A to the Application in the above-captioned docket ([REDACTED] Declaration"). Additional individuals directly involved in developing and testing technologies to be used with the BR metadata may be granted access to the BR metadata, provided such access is approved by NSA's Office of General Counsel (OGC) on a case-by-case basis. Persons who query the BR metadata pursuant to this paragraph may only share the results of any such query with other specially-cleared NSA technical personnel, unless: (i) sharing is permitted under paragraph 3(J); or (ii) a data integrity analyst conducted the query using a RAS-approved

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

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

telephone identifier at the request of an analyst authorized to query the BR metadata pursuant to paragraph 3(C) below, or an analyst authorized to receive query results pursuant to paragraph 3(I) below.² Queries performed by the persons described in this paragraph shall not be subject to the approval process and standard set forth in paragraph (3)C below. To the extent NSA personnel make copies of the BR metadata for purposes of ensuring data integrity or developing and testing technological measures, such copies shall be destroyed upon the completion of their work.


C. Subject to the restrictions and procedures below, up to 125 NSA analysts may be authorized to access the BR metadata for purposes of obtaining foreign intelligence information through contact chaining [REDACTED] ("queries") using telephone identifiers,³ as described in the [REDACTED] Declaration at paragraphs 8-13.

² The Court understands that only Data Integrity Analysts who have received the training required for access under paragraph 3(C) will be permitted to perform queries and share query results with analysts as described in (ii) above.

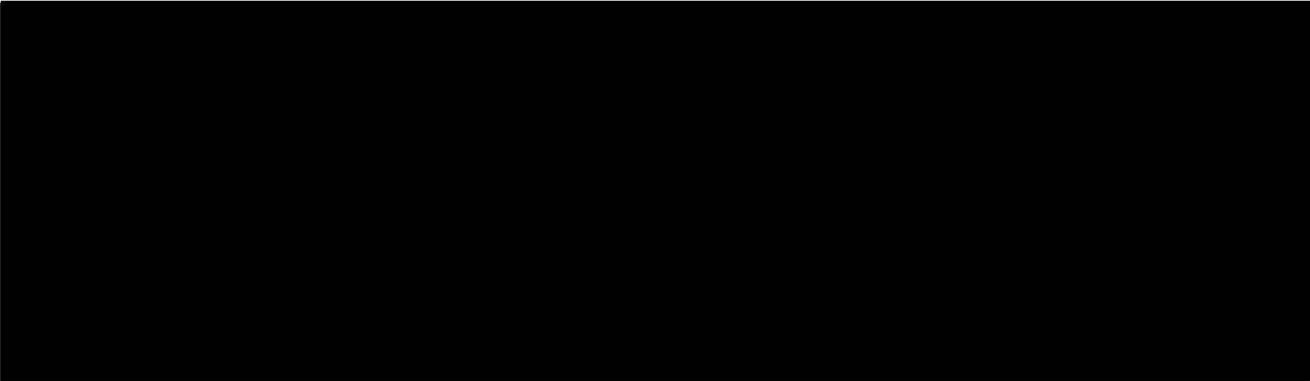
[REDACTED]

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


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

(i) Except as provided in subparagraph (ii) below, all telephone identifiers to be used for queries shall be approved by one of the following designated approving officials: the Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate; 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 that the telephone identifier to be queried is associated with 

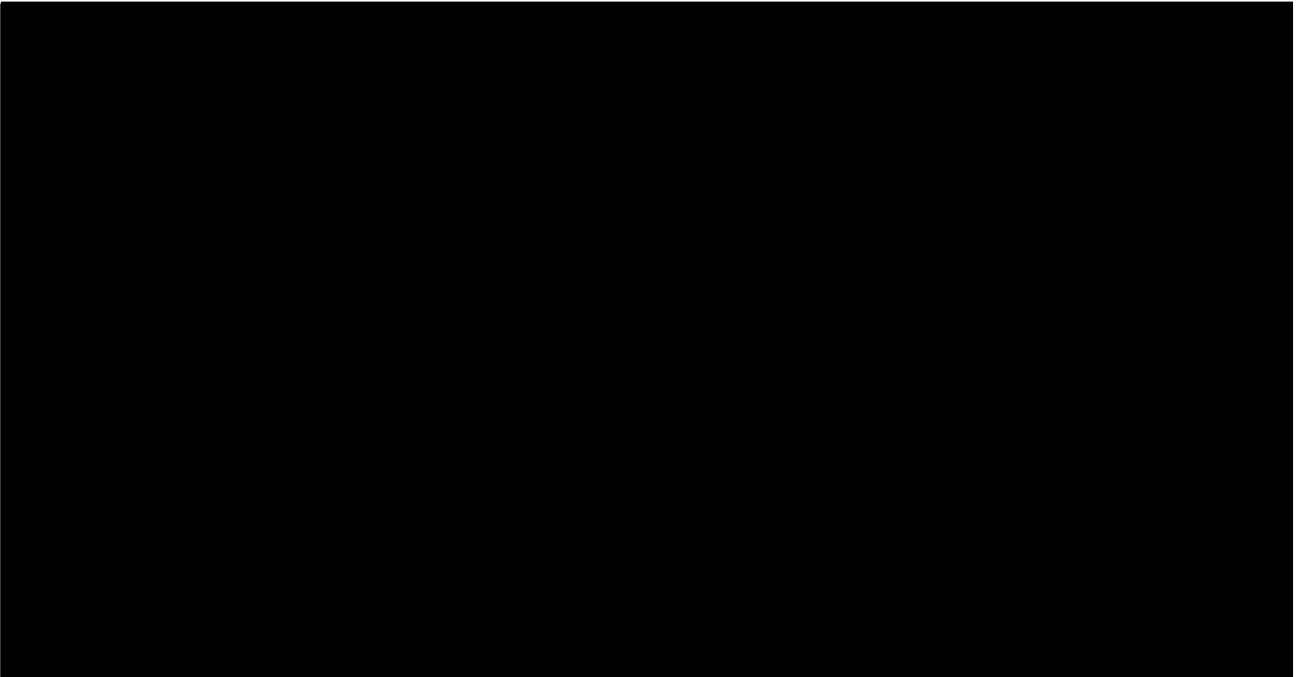
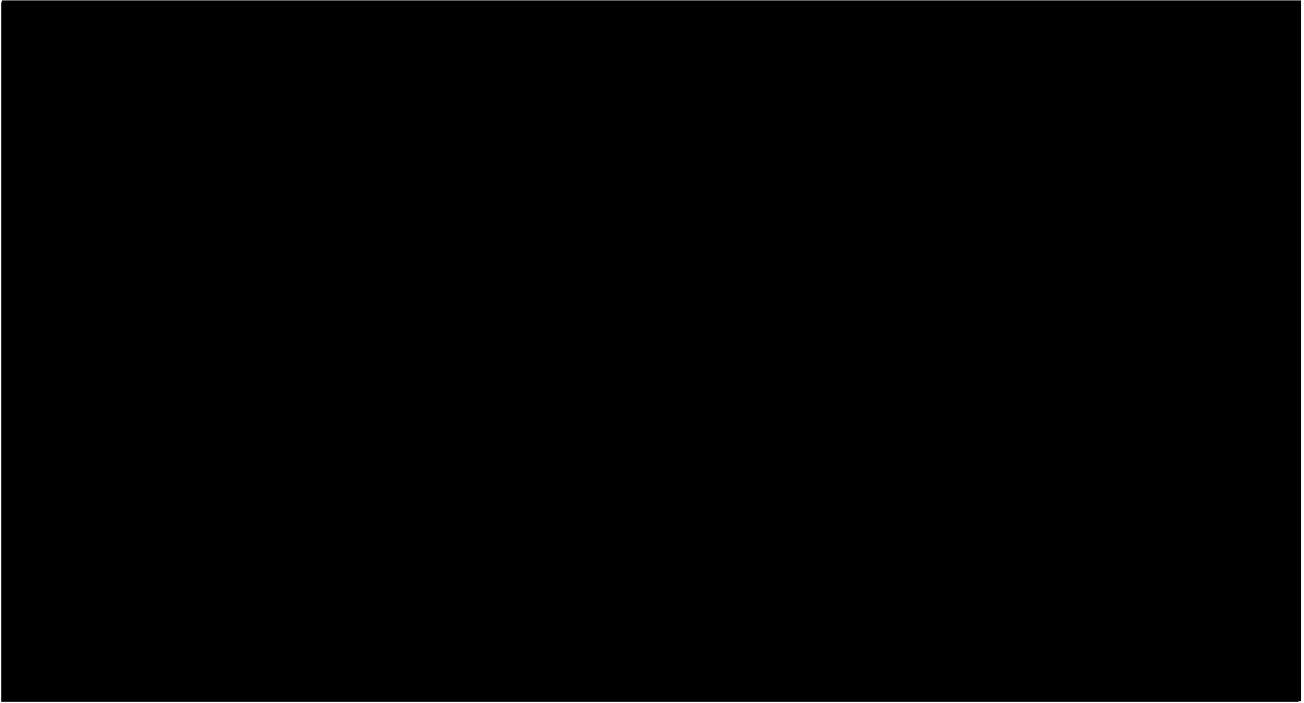
billing and/or routing communications, such as IMSI, IMEI, and calling card numbers.

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

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



provided, however, that NSA's OGC shall first determine that any telephone identifier reasonably believed to be



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

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

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.⁶

(ii) Telephone identifiers 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 agents of [REDACTED]

⁶ The Court understands that from time to time the information available to designated approving officials will indicate that a telephone identifier was, but may not presently be, or is, but was not formerly, associated with [REDACTED]

[REDACTED] In such a circumstance, so long as the designated approving official can determine that the reasonable, articulable suspicion standard can be met for a particular period of time with respect the telephone identifier, NSA may query the BR metadata using that telephone identifier. However, analysts conducting queries using such telephone identifiers must be made aware of the time period for which the telephone identifier has been associated with [REDACTED]

[REDACTED] in order that the analysis and

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

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

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 telephone identifiers under surveillance 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 telephone identifier is associated with [REDACTED]

[REDACTED] shall be effective for: one hundred eighty days for U.S. telephone identifiers and for any identifiers believed to be used by a U.S. person; one year for all other telephone identifiers.⁷

minimization of the information retrieved from their queries may be informed by that fact.

⁷ The Court understands that call detail records of foreign-to-foreign communications provided by [REDACTED] pursuant to this Order

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

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

D. The Director of the NSA shall continue to maintain mandatory procedures to strictly control access to and use of the BR metadata, in accordance with this Court's orders. NSA's OGC shall continue to promptly provide NSD with copies of these mandatory procedures (and all replacements, supplements or revisions thereto in effect now or adopted in the future). The Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate; Chief and Deputy Chief, Homeland Security Analysis Center; and the Homeland Mission Coordinators shall maintain appropriate management controls (e.g., records of all tasking decisions, audit and review procedures) for access to the metadata.

E. The NSA shall obtain the BR metadata from [REDACTED] [REDACTED] via secure lines, and shall store and process the BR metadata on a secure internal network that NSA

will not be used to make chain summary records. Further, such records will be used solely for technical purposes, including use by NSA's data integrity analysts to correctly interpret and extract contact information in [REDACTED] international records. In the event that an NSA analyst performs an authorized query that includes a search of the BR metadata, and the results of that query include information from [REDACTED] foreign-to-foreign call detail records, NSA shall handle and minimize the information in those records in accordance with the minimization procedures in this Order, regardless of the authority pursuant to which NSA obtained the record. In contrast, if the analyst's query does not include a search of the BR metadata, and the results of that query include information from [REDACTED] foreign-to-foreign call

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

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

exclusively will operate.

F. Any processing by technical personnel of the BR metadata acquired pursuant to this order shall be conducted through the NSA's secure internal network, which shall be accessible only to authorized personnel, using accounts authorized by a user authentication service, based on user login and password.

G. Access to the metadata shall be controlled by user name and password. NSA's Oversight and Compliance Office shall monitor the designation of individuals with access to the BR metadata. When the BR metadata is accessed through queries under paragraphs (3)B or (3)C above, a software interface shall limit access to the BR metadata to authorized personnel, and the user's login, Internet Protocol (IP) address, date and time, and retrieval request shall be automatically logged for auditing capability.⁸ When the BR metadata is accessed through any other means under paragraph (3)B above, the user's login, date and time shall be automatically logged for auditing capability.

detail records, then the minimization procedures in this Order shall not be applied to the information in those records.

⁸ In addition, the Court understands from the Declaration of Lieutenant General Keith B. Alexander, Director of NSA (Ex. A to the Report of the United States filed in docket number BR 09-09 on August 17, 2009) that NSA has made a number of technical modifications that will prohibit analysts: a) from inadvertently accessing the BR metadata in [REDACTED]; b) from querying the BR metadata in [REDACTED] with non-RAS-approved identifiers; and c)

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

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

NSA's Office of Oversight and Compliance shall monitor the functioning of this automatic logging capability. All persons authorized for access to the BR metadata and other NSA personnel who are authorized to receive query results shall receive appropriate and adequate training concerning the authorization granted by this Order, the limited circumstances in which the BR metadata may be accessed, and/or other procedures and restrictions regarding the retrieval, storage, and dissemination of the metadata. NSA's OGC shall ensure that such training is provided.

H. NSA shall treat information from queries of the BR metadata in accordance with USSID 18 and shall apply USSID 18 to minimize and disseminate information concerning U.S. persons obtained from the records produced pursuant to the authorities granted herein. Additionally, before the NSA disseminates any U.S. person identifying information, the Chief of Information Sharing Services in the Signals Intelligence Directorate, the Senior Operations Officer at NSA's National Security Operations Center, the Signals Intelligence Directorate Director, the Deputy Director of the NSA, or the Director of the NSA must determine that the information identifying the U.S. person is in

from going beyond three "hops" from an identifier used to query the BR metadata in [REDACTED]

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

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

fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance. Notwithstanding the above requirements, NSA may share certain information, as appropriate, derived from the BR metadata, including U.S. person identifying information, with Executive Branch and Legislative Branch personnel in order to enable them to fulfill their lawful oversight functions, and, in the case of Executive Branch personnel, to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings. By 5:00 p.m. each Friday following the authorization requested herein, the government shall file a report listing each instance during the seven-day period ending the previous Friday in which NSA has shared, in any form, information obtained or derived from the BR metadata with anyone outside NSA. For each such instance, the government shall specify the date on which the information was shared, the recipient of the information, and the form in which the information was communicated (e.g., written report, e-mail, oral communication, etc.). For each such instance in which U.S. person information has been shared, except those involving Executive Branch personnel seeking to identify discoverable information, the Chief of Information Sharing Services in the

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


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


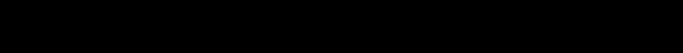
Signals Intelligence Directorate shall certify that one of the authorized officials identified above determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand the counterterrorism information or to assess its importance. This paragraph's reporting requirement is not intended to apply to instances in which BR metadata and information derived therefrom is shared with Executive Branch or Legislative Branch personnel in order to facilitate their lawful oversight functions.

I. Personnel authorized to query the BR metadata in paragraph (3)C above may use and share the results of authorized queries of the BR metadata among themselves and with NSA personnel, including those who are not authorized to access the BR metadata pursuant to paragraph (3)C, provided that all NSA personnel receiving such query results in any form (except for information properly disseminated outside NSA) shall first receive appropriate and adequate training and guidance regarding the rules and restrictions governing the use, storage, and dissemination of such information. NSA's Oversight and Compliance Office shall monitor the designation of individuals who have received the training and guidance necessary to receive the results of queries of the BR metadata.

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

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

J. Authorized personnel also may use and share the identity of high-volume telephone identifiers and 


 that they discover or have discovered as a result of access authorized under paragraphs (3)B and (3)C or as a result of technical personnel access under prior docket numbers in this matter, among themselves and with other NSA personnel, including those who are not authorized to access the BR metadata, for purposes of metadata reduction and management. The training requirements set forth in paragraph (3)I above for NSA personnel receiving query results shall not apply to personnel receiving such identifiers, which may have been identified through queries, so long as they are received solely for purposes of metadata reduction and management.

K. The BR metadata collected under this Court's Orders may be kept online (that is, accessible for queries) for five years from the date of acquisition, at which time it shall be destroyed.

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

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

L. At least twice before the expiration of the authorities granted herein, NSA's OGC shall conduct a random spot check, consisting of an examination of a sample of call detail records obtained, to ensure that NSA is receiving only data as authorized by the Court and not receiving the substantive content of communications.

M. At least twice before the expiration of the authorities granted herein, the Department of Justice's National Security Division (NSD) will review NSA's access to the BR metadata under paragraph (3)C above. Such reviews shall include a sample of the justifications designated approving officials relied upon to approve telephone identifiers for querying the BR metadata, and a review of the queries conducted.

N. NSA's OGC shall consult with NSD on all significant legal opinions that relate to the interpretation, scope, and/or implementation of the authorizations granted by the Court in this matter. When operationally practicable, such consultation shall occur in advance; otherwise, NSD shall be notified as soon as practicable.

O. NSA's OGC shall promptly provide NSD with copies of all formal briefing and/or training materials (including all revisions thereto) currently in use or prepared and used in the future to brief/train NSA personnel concerning the

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

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

authorizations granted by this Order.

P. At least once before the expiration of the authorities granted herein, a meeting for the purpose of assessing compliance with this Court's orders in this matter shall be held with representatives from NSA's OGC, NSD, and appropriate individuals from NSA's Signals Intelligence Directorate. 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 authorities granted herein.

Q. At least once before the expiration of the authorities granted herein, NSD shall meet with NSA's Office of Inspector General (OIG) to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders in this matter.

R. Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC, NSD, and the Court.

S. Within forty-five days of the issuance of this Order, NSA shall file a report with the Court describing the queries made since end of the reporting period of the last report filed pursuant to the Court's order in docket number BR 09-19. Additionally, any application to renew or reinstate the

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

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

authority granted herein shall include a report describing: (i) the queries made since the end of the reporting period of the last report filed with the Court; (ii) the manner in which NSA applied the procedures set forth in paragraph (3)C above; and (iii) any proposed changes in the way in which the call detail records would be received from the carriers and any significant changes to the systems NSA uses to receive, store, process, and disseminate BR metadata.

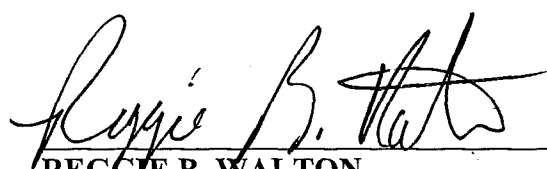
This authorization regarding [REDACTED]

[REDACTED] and unknown persons in the United States and abroad affiliated with [REDACTED]

[REDACTED] and unknown persons in the United States and abroad affiliated with [REDACTED]

[REDACTED] expires on the 21st day of May, 2010, at 5:00 p.m., Eastern Time.

Signed _____ Eastern Time
Date 02-25-2010 Time 3:36 ^{acd}


REGGIE B. WALTON
Judge, United States Foreign Intelligence Surveillance Court

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

[REDACTED] Deputy Clerk
I hereby certify that this document is a true and correct copy of the original [REDACTED]