

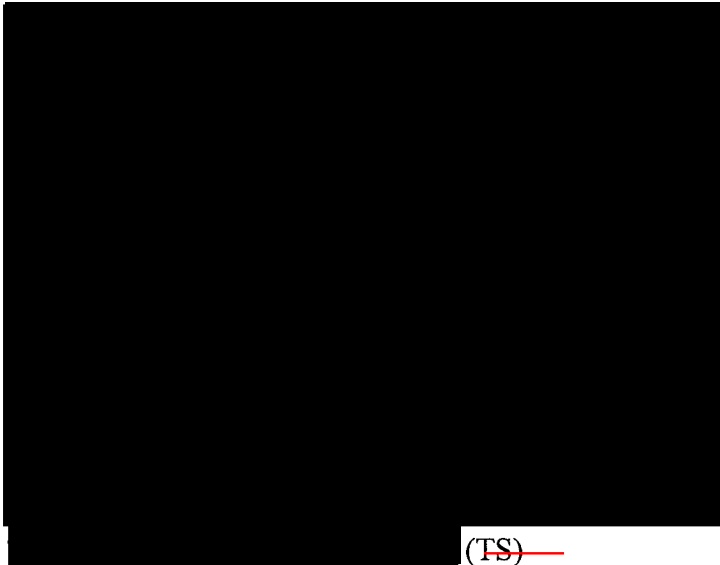
~~TOP SECRET//COMINT//NOFORN~~

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 [REDACTED]



Docket Number: BR 09-01

(TS)

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, as amended, (FISA), 50 U.S.C. §1861, requiring the production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the

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

matters set forth therein, as well as the government's filings in Docket Number BR 08-13 (the prior renewal of the above-captioned matter), 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 substantively the same as the minimization procedures proposed by the government in the prior application and approved and adopted as binding by the order of this Court in Docket Number BR 08-13. However, for the reasons set forth in this Court's Order entered on March 2, 2009, in Docket Number BR 08-13 ("March 2nd Order"), the Court found that the NSA has so frequently and systemically violated such procedures that it can fairly be said that this critical element of the overall business records regime has never functioned effectively. March 2nd Order at 11.

Nevertheless, the Court permitted the government to continue to acquire the tangible things sought, but ordered the government to follow additional minimization procedures identified in its March 2nd Order, and set forth herein. Id. at 18-20.

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 that the application is GRANTED IN PART, and it is FURTHER ORDERED, as follows:

1. The Custodians of Records of [REDACTED]

[REDACTED] shall produce to the 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” created by [REDACTED]. Telephony metadata shall include 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 the time and duration of call. Telephony metadata shall 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.

2. With respect to any information the FBI receives as a result of this order (information that is passed or “tipped” to the FBI by the 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 the NSA receives as a result of this order, the NSA shall strictly adhere to the following minimization procedures:

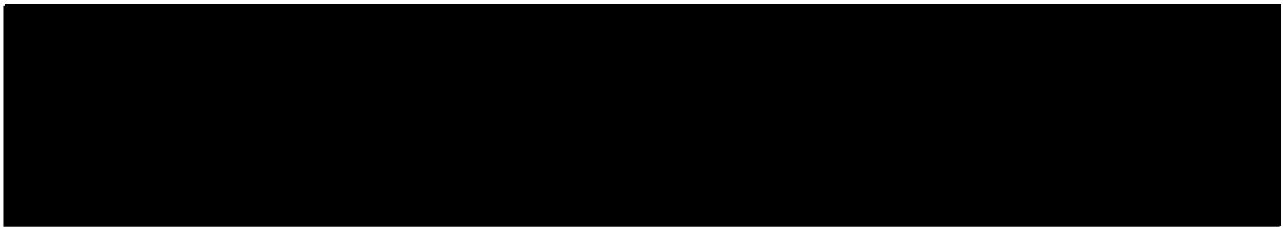
A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. 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 paragraphs 17-18 of the Declaration of [REDACTED] Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate, the National Security Agency, filed on March 4, 2009, in the above-captioned docket ("[REDACTED] Declaration").

Additional individuals directly involved in developing and testing any technological measures designed to enable the NSA to comply with the Court's orders may be granted access, provided such access is approved by NSA's Office of General Counsel (OGC) on a case-by-case basis.

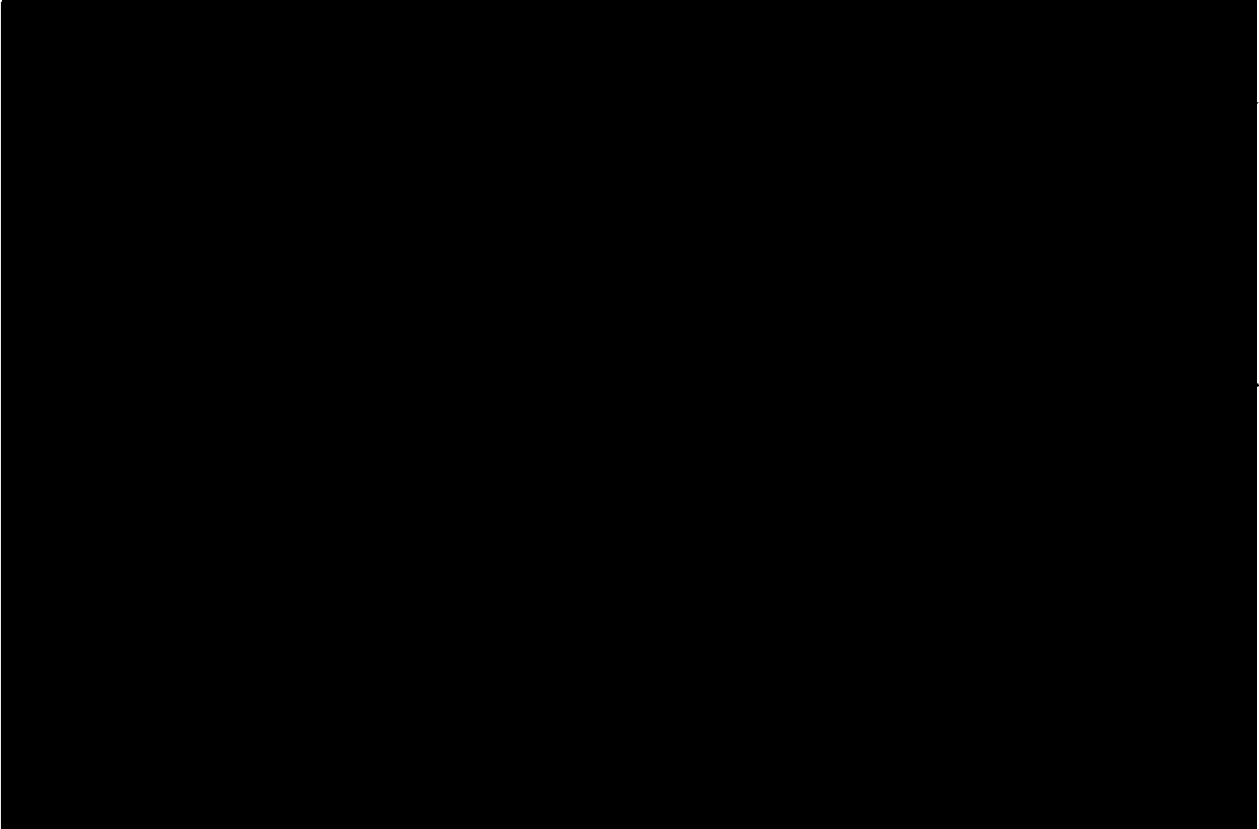
C. The government may request through a motion, permission from the Court to use

specific telephone identifiers¹ that satisfy the reasonable articulable suspicion standard² to query

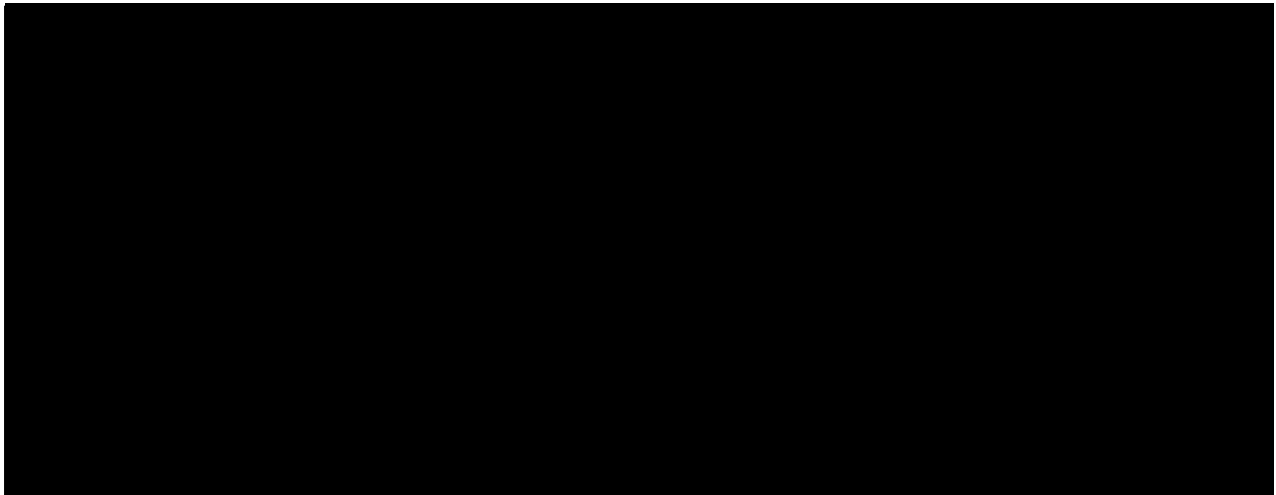


²The reasonable articulable suspicion standard is met when, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone identifier is associated with [REDACTED], provided, however, that any telephone identifier 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 Amendment to the Constitution.

For purposes of this order, [REDACTED]



the BR metadata for purposes of obtaining foreign intelligence through contact chaining [REDACTED] [REDACTED] as described in the [REDACTED] Declaration at 6-7, on a case-by-case basis. In addition, if the government determines that immediate querying of the BR metadata through contact chaining [REDACTED] is necessary to protect against an imminent threat to human life, the government may query the BR metadata for such purpose. In each such case falling under this latter category, the government shall notify the Court of the access, in writing, no later than 5:00 p.m., Eastern Time on the next business day after such access. Any submission to the Court under this paragraph shall, at a minimum, specify the telephone identifier for which access is sought or was granted, provide the factual basis for the NSA's belief that the reasonable articulable suspicion standard has been met with regard to that identifier,³ and, if the access has



³For telephone identifiers that are currently the subject of this Court's authorized electronic surveillance, pursuant to 50 U.S.C. §1805, based on this Court's finding of probable cause to believe that they are used by [REDACTED] including those used by U.S. persons, the government's submission need only provide the target's name, docket number, and

already taken place, a statement of the immediate threat necessitating such access. Only 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 shall be authorized to access the BR metadata for purposes of implementing this sub-paragraph.

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.

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

F. Any processing by technical personnel of the BR metadata acquired pursuant to this order shall be conducted through the NSA's private network, which shall be accessible only via select machines and only to cleared technical personnel, using secured encrypted communications.

G. Access to the BR metadata shall be accomplished through a software interface that shall limit access to this data to authorized personnel. The NSA's Office of General Counsel (OGC) shall monitor the designation of individuals with access to the BR metadata. Access to the metadata shall be controlled by user name and password. When the metadata is accessed, the _____
date of expiration of this Court's most recent authorization of electronic surveillance.

user's login, Internet Protocol (IP) address, date and time, and retrieval request shall be automatically logged for auditing capability. The NSA's OGC shall monitor the functioning of this automatic logging capability. Persons authorized to access the BR metadata shall be briefed by the NSA's OGC concerning the authorization granted by this order and the limited circumstances in which queries to the metadata are permitted, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of the metadata.

H. Any dissemination of U.S. person information by the NSA shall follow the standard NSA minimization procedures found in the Attorney General-approved guidelines (USSID 18). Before information identifying a U.S. person may be disseminated outside of the NSA, a judgment must be made that the identity of the U.S. person is necessary to understand the foreign intelligence information or to assess its importance. Prior to the dissemination of any U.S. person identifying information, the Chief of Information Sharing Services in the Signals Intelligence Directorate 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. A record shall be made of every such determination.

I. At least twice every ninety days, the NSA's OGC shall conduct random spot checks, consisting of an examination of a sample of call detail records obtained, to ensure that the NSA is receiving only data as authorized by the Court and not receiving the substantive content of communications.

J. 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.

K. The Chief, FISA Office, Signals Intelligence Directorate (SID) Program Management Office for Counterterrorism Special Projects, Analysis and Production; 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 and shall use the Attorney General-approved guidelines (USSID 18) to minimize the information reported concerning U.S. persons.

L. Any application to renew or reinstate the 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; and (ii) any proposed changes in the way in which the call detail records would be received from the carriers.

M. The government shall implement the additional oversight mechanisms described in paragraph 10 of its application. Application at 25-26.

N. As previously ordered on March 2, 2009, upon completion of the government's end-to-end system engineering and process reviews, described in Memorandum of the United States In Response to the Court's Order Dated January 28, 2009, Tab 1, Declaration of Lieutenant General Keith B. Alexander, United States Army, Director of the NSA, filed February 17, 2009 at 21, the government shall file a report with the Court, that shall, at a minimum, include:

(i). an affidavit by the Director of the FBI, and affidavits by any other official responsible for national security that the government deems appropriate, describing the value of the BR metadata to the national security of the United States and certifying that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities, and that such investigation of a U.S. person is not conducted solely on the basis of activities protected by the First Amendment;

(ii). a description of the results of the NSA's end-to-end system engineering and process reviews, including any additional instances of non-compliance identified therefrom;

(iii). a full discussion of the steps taken to remedy any additional non-compliance as well as the incidents described herein, and an affidavit attesting that any technological remedies have been tested and demonstrated to be successful; and

(iv). the minimization and oversight procedures the government proposes to employ should the Court decide to authorize the government's resumption of regular access to the BR metadata.

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

This authorization to acquire the tangible things described herein regarding [REDACTED]

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

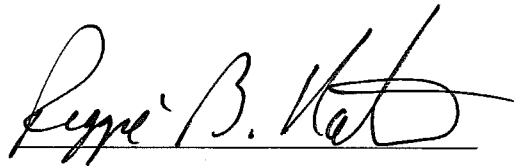
[REDACTED]

[REDACTED] and unknown persons in the United States and

abroad [REDACTED] expires

on the 29th day of May, 2009, at 5 p.m., Eastern Time. All other provisions of the Order shall remain in effect until otherwise ordered by the Court.

IT IS SO ORDERED, this 5th day of March, 2009.



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

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

[REDACTED] Deputy Clerk
FISC, certify that this document
is a true and correct copy of
the original. [REDACTED]