

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 (b)(1) and (b)(3)

(b)(1) and (b)(3)



Docket Number: BR:

09-09

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 production to the National Security Agency (NSA) of the tangible things described below, and full consideration

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

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

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 09-06 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) The Custodians of Records of (b)(1) and (b)(3)

(b)(1) and (b)(3)

(b)(1) and (b)(3)

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 (b)(1) and (b)(3)

(b)(1) and (b)(3)

for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. (b)(1) and (b)(3)

(b)(1) and (b)(3)

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~~

(2) With respect to any information the FBI receives as a result of this Order (information that is passed or "tipped" 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, the government 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 paragraph 14 of the Declaration of (b)(1) and (b)(3) 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 ((b)(1) and Declaration"). Additional individuals directly involved in

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

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

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. Except as provided in paragraph (3)K, persons who query the BR metadata pursuant to this subparagraph shall not share in any form the results of any such query of the BR metadata with any of the persons authorized to use or share the results of queries pursuant to paragraphs (3)C or (3)J below.

C. The government may request through a motion, permission from the Court to use specific telephone identifiers² that satisfy the reasonable articulable suspicion standard³ to query

²

³ The 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

; provided, however, that any telephone identifier believed to be used by a U.S. person shall not be regarded as (b)(1) and (b)(3)

solely on the basis of activities that are protected by the First Amendment to the Constitution.

For purposes of this Order, (b)(1) and (b)(3)


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

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

(b)(1) and (b)(3)



For purposes of this Order,



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

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

the BR metadata for purposes of obtaining foreign intelligence information through contact chaining ~~(b) (1) and (b)(3)~~¹⁾ as described in the ~~(b)(1)~~_{b d} 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 ~~(b)(1) (1) and (b)(3)~~_d ~~(b)(1) and (b)~~ is necessary to protect against an imminent threat to human life, the government may query the BR metadata for such purpose. In any case falling into 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 identifier⁴ and, if such access has already taken place, a statement of the immediate threat necessitating such access. Only the Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals

⁴ For telephone identifiers that are currently subject to Court-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 ~~(b)(1) and (b)(3)~~

~~(b)(1) and (b)(3)~~ including those used by U.S. persons, the government's submission need only provide the target's name, docket number, and date of expiration of this Court's most recent authorization of electronic surveillance.

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

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

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. For the duration of the authorization granted by this Order, the NSA may use certain telephone identifiers previously approved by the Court in Docket Number BR 09-06, specifically, only those (b) telephone identifiers described in Tab 1 to the (b)(1) Declaration, to conduct queries of the BR metadata for purposes of obtaining foreign intelligence information through contact chaining (b)(1) and (b)(3) in accordance with this Order. If NSA has knowledge of the discontinued use of any such identifier, its analysis and minimization of information retrieved from the queries based on any such identifier should be informed by the knowledge of discontinued use of the identifier.

E. 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 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,

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

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

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.

F. The NSA shall obtain the BR metadata from (b)(1) and (b)(3) and shall store and process the BR metadata on a secure internal network that NSA exclusively will operate.

G. 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.

H. 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

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

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

capability. 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. NSA's OGC shall monitor the functioning of this automatic logging capability. All persons authorized for access to the BR metadata shall be briefed by NSA's OGC concerning the authorization granted by this Order and the limited circumstances in which the BR metadata may be accessed, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of the metadata.

I. Any dissemination of U.S. person information shall follow the standard NSA minimization procedures found in USSID 18. 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 fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance. By 5:00 p.m. each Friday following the authorization requested herein, the government shall file a report listing each

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

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

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, the Chief of Information Sharing Services in the 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.

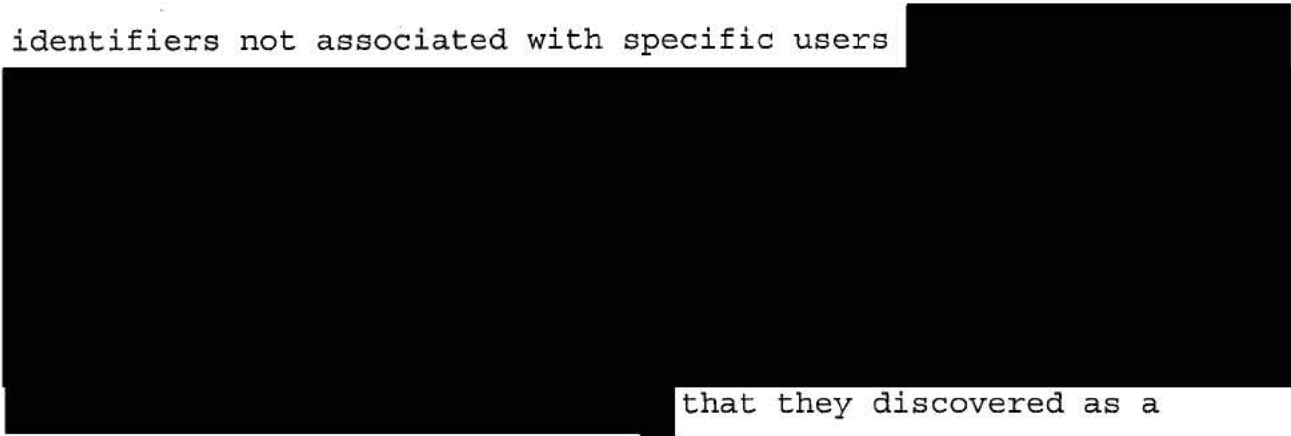
J. Personnel authorized to query the BR metadata in paragraph (3)C above may use and share the results of authorized queries of the BR metadata among themselves and with NSA personnel, including those who are not authorized to access the BR metadata pursuant to paragraph (3)C, provided that all NSA personnel receiving such query results in any form shall first receive training and guidance regarding all rules and restrictions governing the use, storage, and dissemination of such information. NSA's Oversight and Compliance Office shall

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

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

monitor the designation of individuals who have received the training and guidance necessary to receive the results of queries of the BR metadata.

K. Authorized personnel also may use and share the identity of high-volume telephone identifiers and other types of identifiers not associated with specific users



that they discovered as a result of access authorized under paragraphs (3)B and (3)C, 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)J 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. ~~(TS//SI//NF)~~

L. 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

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

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

destroyed.

M. At least once 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.

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 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

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

TOP SECRET//COMINT//NOFORN

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. 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. In addition, if the government files the report required under paragraph (3)T after 5:00 p.m. Eastern Time on Monday August 17, 2009, any such application shall provide the factual basis for the NSA's belief that the reasonable articulable suspicion standard continues to be met for any telephone identifier for which the government seeks permission to

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

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

query the BR metadata for purposes of obtaining foreign intelligence information through contact chaining or pattern analysis.

T. 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-

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

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

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 in the Court's Order of March 2, 2009 in docket number BR 08-13, and an affidavit attesting that any technological remedies have been tested and demonstrated to be successful; and

(iv) additional 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.

Furthermore, as required by the Court's Order dated June 22, 2009, in docket numbers PR/TT [REDACTED] and BR 09-06, the government's submission regarding the results of the end-to-end review shall include a full explanation of why the government has permitted dissemination outside NSA of U.S. person information in violation of the Court's Orders in this matter.

In addition, the government's submission shall include:

- a full explanation of the extent to which NSA has acquired [REDACTED]

(b)(1) and (b)(3) [REDACTED] pursuant to orders of the FISC, and whether the NSA's storage, handling, and

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

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

dissemination of information in those records, or derived therefrom, complied with the Court's orders; and

- either (i) a certification that any overproduced information, as described in footnote 11 of the government's application, has been destroyed, and that any such information acquired pursuant to this Order is being destroyed upon recognition; or (ii) a full explanation as to why it is not possible or otherwise feasible to destroy such information.

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

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

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

This authorization regarding [REDACTED]

[REDACTED]

expires on the 4th day of September, 2009, at 5:00

p.m., Eastern Time.

Signed 07-09-2009 P05:11 Eastern Time
Date Time



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

(b)(1) and (b)(3) Deputy Clerk
FISC, certify that this document
is a true and correct copy of
the original.

(b)(1) and (b)(3)

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