

~~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

10 - 70

~~(TS//NF)~~

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//COMINT//NOFORN~~

Derived from: Pleadings in the above-captioned docket
Declassify on: 22 October 2035

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 10-49 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, 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 (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.

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 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

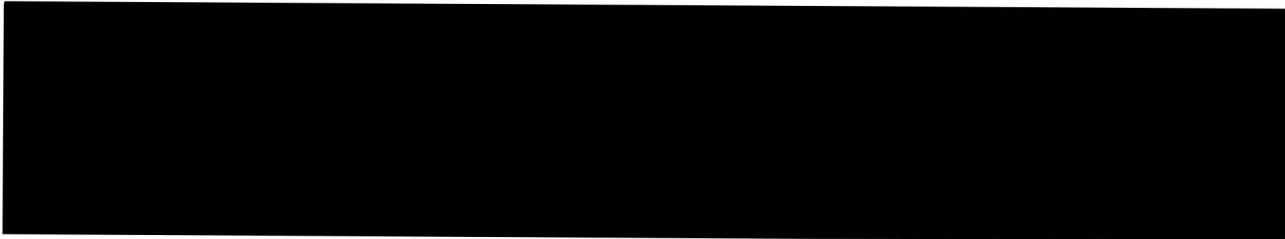
² The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA will ensure that any access or use of the BR metadata in the event of any natural disaster, man-

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 identifiers⁴ 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, but the results of any such queries will not be used for intelligence analysis purposes.

An authorized technician may query the BR metadata with a non-RAS-approved identifier to determine whether that identifier is a high volume identifier. If so, the technician may share the results of that query, i.e., the identifier and the fact that it is a

made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

³ The Court understands that certain technical personnel, specifically the 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.



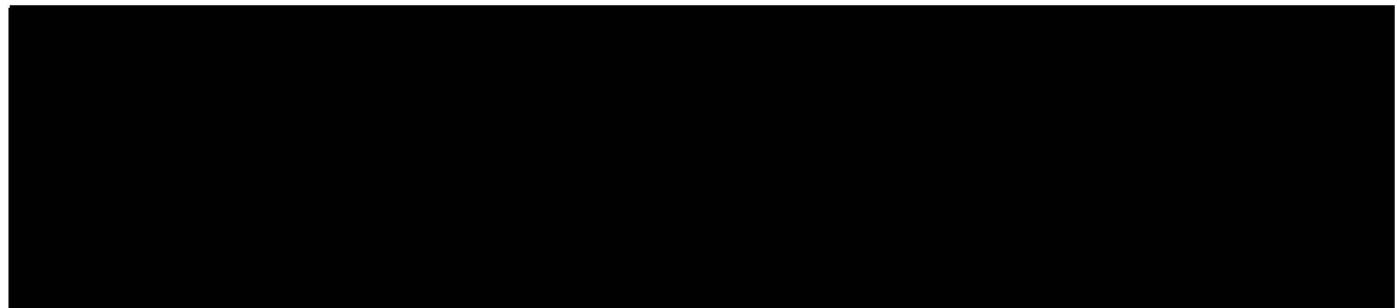
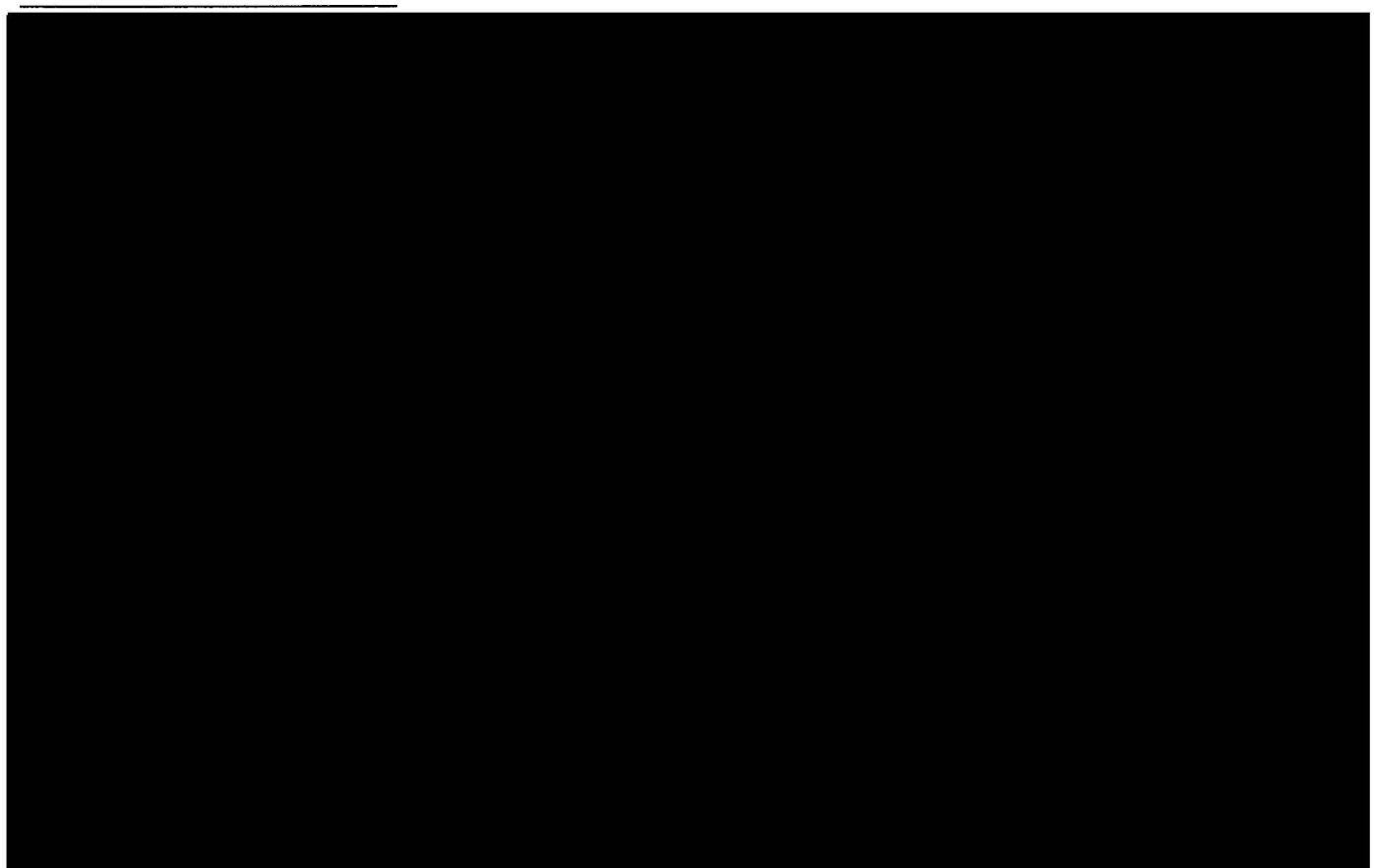
high volume identifier, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that query for intelligence analysis purposes.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through contact chaining queries of the BR metadata using identifiers approved as "seeds" pursuant to the RAS approval process described below, as described in the [REDACTED] Declaration at paragraph 17. NSA shall ensure, through adequate and appropriate technical and management controls, that queries of ~~BR raw~~ metadata for intelligence analysis purposes will be initiated using only an identifier 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.

(i) Except as provided in subparagraph (ii) below, all identifiers 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

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

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 identifier to be queried is associated with [REDACTED]
[REDACTED]



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

provided, however, that NSA's OGC shall first determine that any identifier 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.⁷

(ii) 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 [REDACTED]

[REDACTED]
[REDACTED] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic

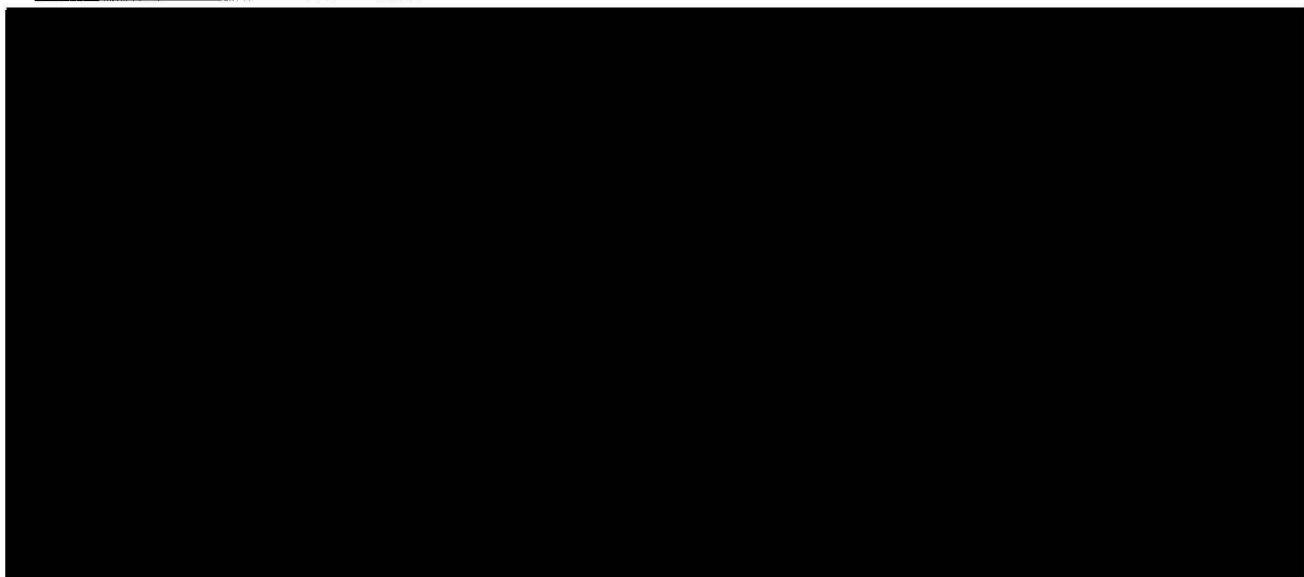
⁷ The Court understands that from time to time the information available to designated approving officials will indicate that an identifier is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the identifier is or was associated with a Foreign Power will be specified so that analysts conducting queries using that identifier can properly minimize information that may be returned within query results that fall outside of that timeframe.

surveillance without review and approval by a designated approving official.

The preceding sentence shall not apply to 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 an identifier is associated with [REDACTED]

[REDACTED] shall be effective for:
one hundred eighty days for U.S. identifiers and for any identifiers believed to be used by a U.S. person; one year for all other identifiers.⁸



D. Results derived from 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 receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.⁹ NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) to any results from queries of the BR metadata disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, one of the officials listed in Section 7.3(c) of USSID 18 (i.e., 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 Operation 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

⁹ 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.

counterterrorism information or assess its importance.¹⁰ Notwithstanding the above requirements, NSA may share results derived from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch 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

¹⁰ 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.

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.¹¹ OGC shall provide NSD/DoJ with copies 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.

¹¹ 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 information derived therefrom.

- (iv) At least once during the authorization period, NSA's OGC shall review 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.
- (v) 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 the Court's orders. 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.
- (vi) 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.
- (vii) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for identifiers used to query the BR metadata.
- (viii) 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 the queries made since the last report and NSA's application of the RAS standard. 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, information derived from the BR metadata 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 counterterrorism information or to assess its importance.

-- *Remainder of page left intentionally blank.* --

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

This authorization regarding [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] expires on the 21st day

of January, 2011, at 5:00 p.m., Eastern Time.

10-29-2010 110:14
Signed _____ Eastern Time
Date Time



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

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

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