

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION OF
TANGIBLE THINGS FROM [REDACTED]

[REDACTED]

Docket Number: BR 13-158

MEMORANDUM

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

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

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

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

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

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

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

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

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

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


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

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

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

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

ENTERED this 11th day of October, 2013.


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

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

Page 6

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

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Docket Number: BR

13 - 158

PRIMARY ORDER

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

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

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

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

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number BR 13-109 and its predecessors. [50 U.S.C. § 1861(c)(1)]

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

Accordingly, and as further explained in the accompanying Memorandum, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

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

FURTHER ORDERED, as follows:

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

B. The Custodian of Records of [REDACTED]

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

¹ For purposes of this Order "telephony metadata" includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer. Furthermore, this Order does not authorize the production of cell site location information (CSLI).

thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or “telephony metadata” created by [REDACTED] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [REDACTED]

[REDACTED]

[REDACTED]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

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

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.² The BR metadata shall carry unique markings such

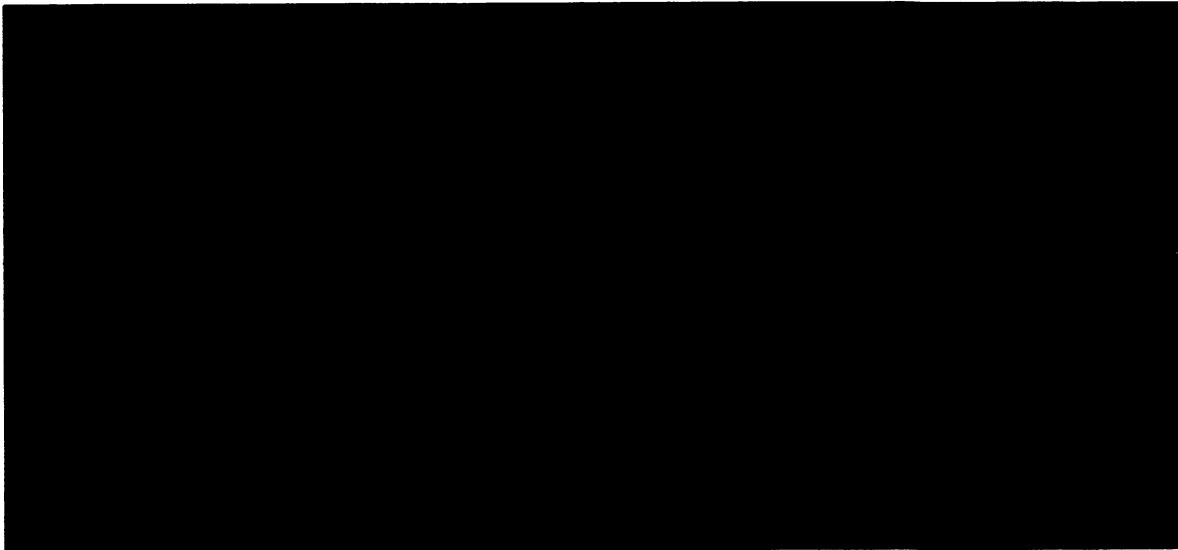
² The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.³

Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms⁴ that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

³ The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.



but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through queries of the BR metadata to obtain contact chaining information as described in paragraph 17 of the Declaration of [REDACTED] [REDACTED] attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.⁵ NSA shall ensure,


⁵ For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.

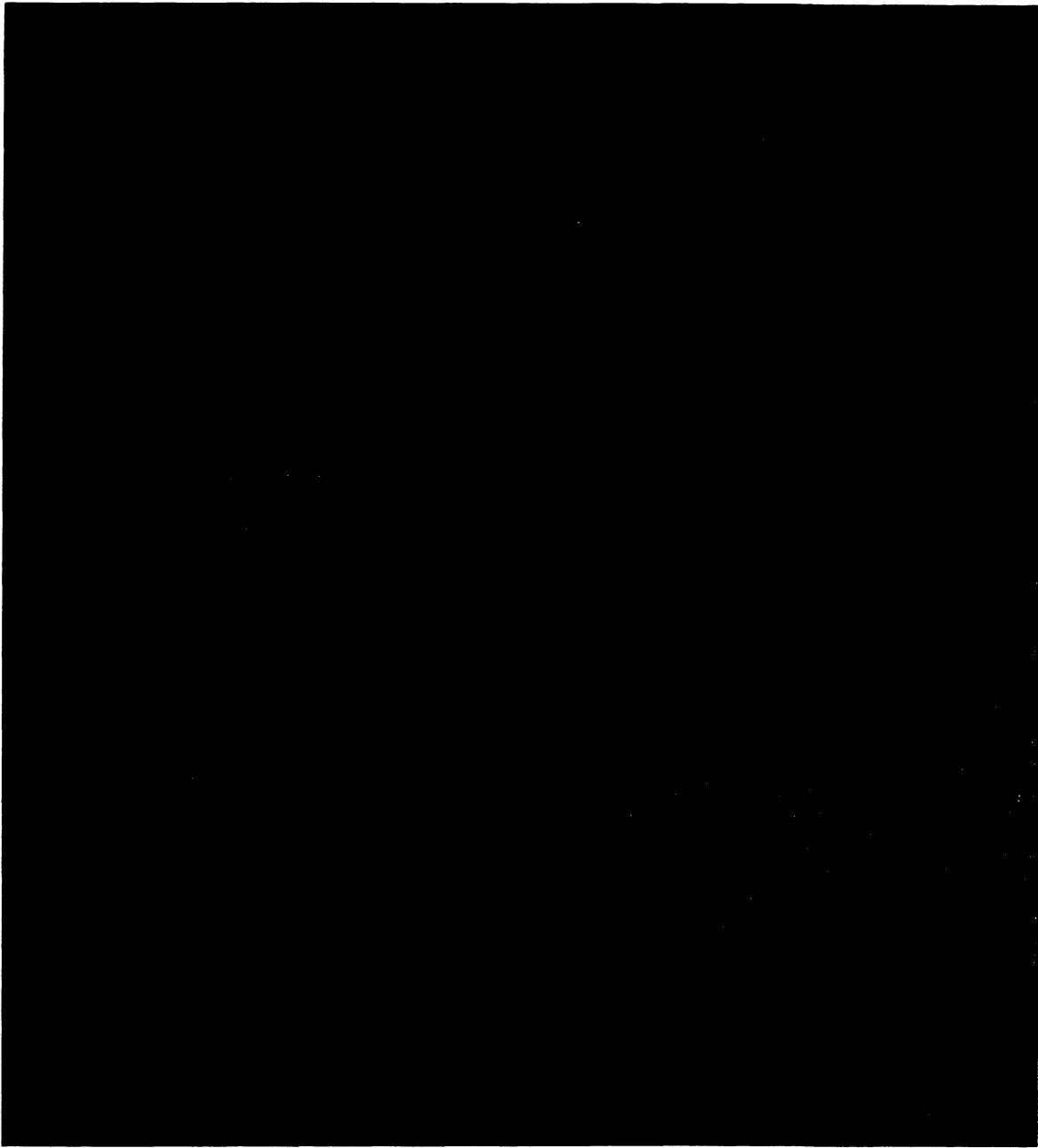
through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.⁶

(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [REDACTED]

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

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

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



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

shall first determine that any selection term reasonably believed to be used by a

United States (U.S.) person is not regarded as associated with [REDACTED]

[REDACTED]

[REDACTED] solely on the basis of activities that are protected by the

First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [REDACTED]

[REDACTED]

[REDACTED] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official.

The preceding sentence shall not apply to selection terms under surveillance

[REDACTED]

pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated with [REDACTED] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.^{9,10}

⁹ The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the selection term is or was associated with a Foreign Power shall be specified. The automated query process described in the [REDACTED] Declaration limits the first hop query results to the specified time frame. Analysts conducting manual queries using that selection term shall continue to properly minimize information that may be returned within query results that fall outside of that timeframe.

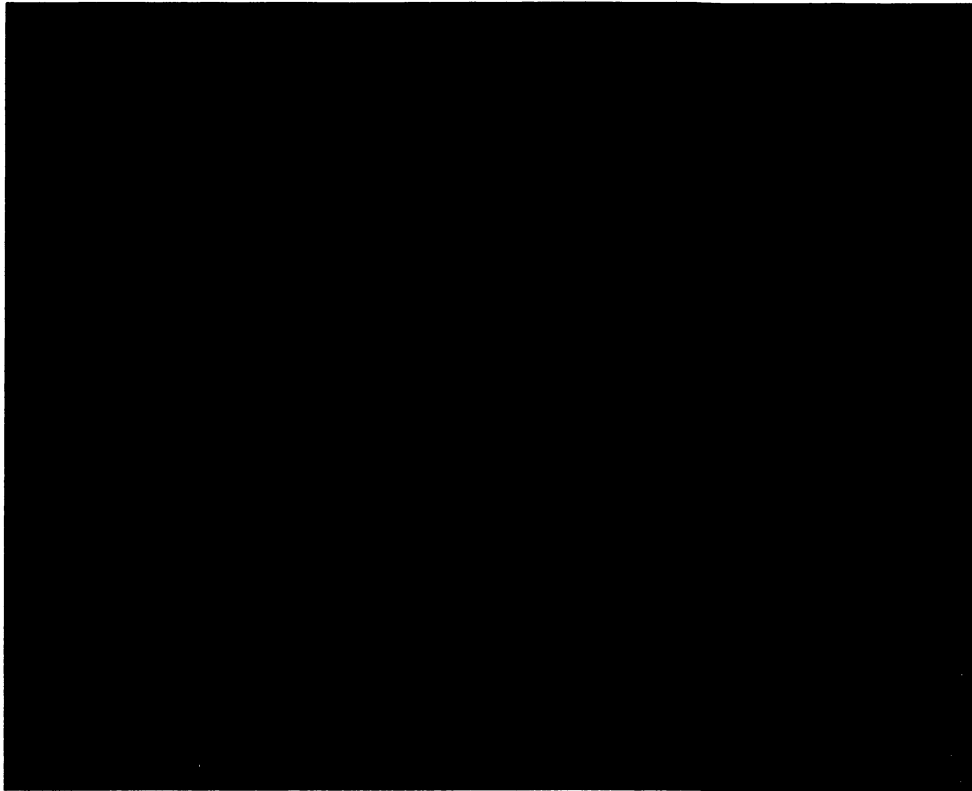
¹⁰ The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to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

(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.¹¹ This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns the hop-limited results from those queries to a "corporate store." The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms. The specifics of the automated query process, as described in the [REDACTED] Declaration, are as follows:



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

¹² As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms have not expired. This step does not use expired RAS-approved selection terms to create the list of "authorized query terms" (described below) regardless of whether the list of RAS-approved selection terms is up-to-date.



D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first



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

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.¹⁵ NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.¹⁶ Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch

¹⁵ In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

¹⁶ In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

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

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

personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.¹⁷ OGC shall provide NSD/DoJ with copies

¹⁷ The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

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

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

of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

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

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.

(vii) Other than the automated query process described in the [REDACTED] Declaration and this Order, prior to implementation of any new or modified automated query processes, such new or modified processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

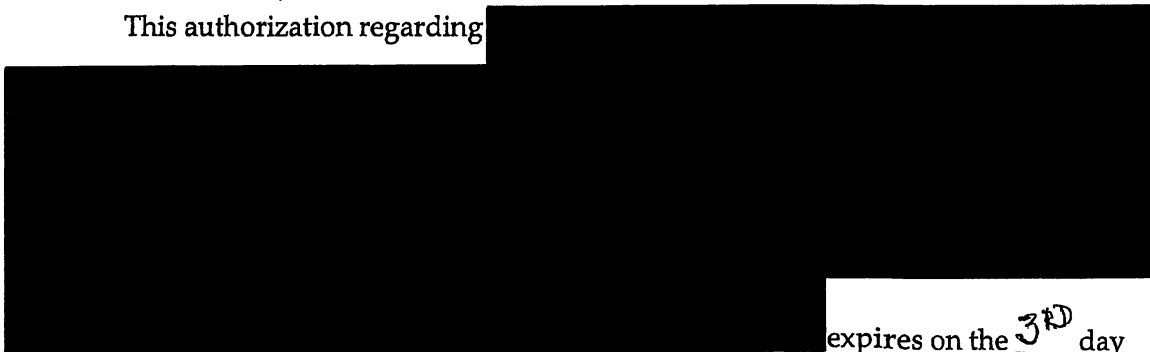
G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of NSA's application of the RAS standard, as well as NSA's implementation and operation of the automated query process. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

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

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

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

This authorization regarding

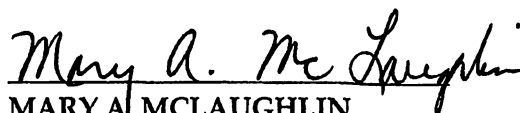


expires on the 3rd day

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

Signed _____ Eastern Time
Date Time

10-11-2013 P12:05



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

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

