

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

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

IN RE PRODUCTION OF TANGIBLE THINGS
FROM [REDACTED]

Docket Number: BR 08-13

ORDER

On December 12, 2008, the Foreign Intelligence Surveillance Court ("FISC" or "Court") re-authorized the government to acquire the tangible things sought by the government in its application in the above-captioned docket ("BR 08-13"). Specifically, the Court ordered [REDACTED] to produce, on an ongoing daily basis for the duration of the order, an electronic copy of all call detail records or "telephony metadata" created by [REDACTED] BR 08-13, Primary Order at 4. The Court found reasonable grounds to believe that the tangible things sought are relevant to authorized investigations being conducted by the Federal Bureau of Investigation ("FBI") to protect against international terrorism, which investigations are not being conducted solely upon the basis of First Amendment protected activities, as required by 50 U.S.C. §§1861(b)(2)(A) and (c)(1). *Id.* at 3. In making this finding, the Court relied on the

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

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

assertion of the National Security Agency ("NSA") that having access to the call detail records "is vital to NSA's counterterrorism intelligence mission" because "[t]he only effective means by which NSA analysts are able continuously to keep track of [REDACTED]

[REDACTED] and all affiliates of one of the aforementioned entities [who are taking steps to disguise and obscure their communications and identities], is to obtain and maintain an archive of metadata that will permit these tactics to be uncovered." BR 08-13, Application Exhibit A, Declaration of [REDACTED]

Signals Intelligence Directorate Deputy Program Manager [REDACTED]

NSA, filed Dec. 11, 2008 ("[REDACTED] Declaration") at 5. NSA

also averred that

[t]o be able to exploit metadata fully, the data must be collected in bulk.... The ability to accumulate a metadata archive and set it aside for carefully controlled searches and analysis will substantially increase NSA's ability to detect and identify members of [REDACTED]

Id. at 5-6.

Because the collection would result in NSA collecting call detail records pertaining to [REDACTED] of telephone communications, including call detail records pertaining to communications of United States ("U.S.") persons located within the U.S. who are not the subject of any FBI investigation and whose metadata could not otherwise be legally captured in bulk, the government proposed stringent minimization procedures that strictly controlled the

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

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

acquisition, accessing, dissemination, and retention of these records by the NSA and the FBI.¹ BR 08-13, Application at 12, 19-28. The Court's Primary Order directed the government to strictly adhere to these procedures, as required by 50 U.S.C. 1861(c)(1). Id. at 4-12. Among other things, the Court ordered that:

access to the archived data shall occur only when NSA has identified a known telephone identifier for which, 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]

[REDACTED] provided, however, that a telephone identifier believed to be used by a U.S. person shall not be regarded as associated with [REDACTED]

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

Id. at 8 (emphasis added).

In response to a Preliminary Notice of Compliance Incident dated January 15, 2009, this Court ordered further briefing on the non-compliance incident to help the Court assess whether its Orders should be modified or rescinded; whether other remedial steps should be directed; and whether the Court should take action regarding persons responsible for any misrepresentations to the Court or violations of its Orders. Order Regarding Preliminary Notice of Compliance Incident Dated January 15, 2009, issued Jan. 28, 2009, at 2. The government timely filed its Memorandum in Response to the Court's Order on February 17, 2009. Memorandum of the United States In Response to the Court's Order Dated January 28, 2009 ("Feb. 17, 2009

¹The Court notes that the procedures set forth in the government's application and the Declaration are described in the government's application as "minimization procedures." BR 08-13, Application at 20.

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

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

Memorandum”).

A. NSA’s Unauthorized Use of the Alert List

The government reported in the Feb. 17, 2009 Memorandum that, prior to the Court’s initial authorization on May 24, 2006 (BR 06-05), the NSA had developed an “alert list process” to assist the NSA in prioritizing its review of the telephony metadata it received. Feb. 17, 2009 Memorandum at 8. Following the Court’s initial authorization, the NSA revised this alert list process so that it compared the telephone identifiers on the alert list against incoming FISC-authorized Business Record metadata (“BR metadata”) and SIGINT collection from other sources, and notified NSA’s counterterrorism organization if there was a match between an identifier on the alert list and an identifier in the incoming data. Feb. 17, 2009 Memorandum at 9-10. The revised NSA process limited any further analysis of such identifiers using the BR metadata to those telephone identifiers determined to have met the “reasonable articulable suspicion” standard (hereafter “RAS-approved identifiers”) set forth above. *Id.* at 10-11. However, because the alert list included all identifiers (foreign and domestic) that were of interest to counterterrorism analysts who were charged with tracking [REDACTED]

[REDACTED], most of the telephone identifiers compared against the incoming BR metadata were not RAS-approved.² Feb. 17, 2009 Memorandum at 10-11. Thus, since the earliest days of the FISC-authorized collection of call-detail records by the NSA, the

²As an example, the government reports that as of January 15, 2009, only 1,935 of the 17,835 identifiers on the alert list were RAS-approved. Feb. 17, 2009 Memorandum at 11.

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

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

NSA has on a daily basis, accessed the BR metadata for purposes of comparing thousands of non-RAS approved telephone identifiers on its alert list against the BR metadata in order to identify any matches. Such access was prohibited by the governing minimization procedures under each of the relevant Court orders, as the government concedes in its submission. Feb. 17, 2009 Memorandum at 16.

The government's submission suggests that its non-compliance with the Court's orders resulted from a belief by some personnel within the NSA that some of the Court's restrictions on access to the BR metadata applied only to "archived data," i.e., data residing within certain databases at the NSA. Feb. 17, 2009 Memorandum, Tab 1, Declaration of Lieutenant General Keith B. Alexander, United States Army, Director of the NSA ("Feb. 17, 2009 Alexander Declaration") at 10-11. That interpretation of the Court's Orders strains credulity. It is difficult to imagine why the Court would intend the applicability of the RAS requirement - a critical component of the procedures proposed by the government and adopted by the Court - to turn on whether or not the data being accessed has been "archived" by the NSA in a particular database at the time of the access. Indeed, to the extent that the NSA makes the decision about where to store incoming BR metadata and when the archiving occurs, such an illogical interpretation of the Court's Orders renders compliance with the RAS requirement merely optional.

The NSA also suggests that the NSA OGC's approval of procedures allowing the use of non-RAS-approved identifiers on the alert list to query BR metadata not yet in the NSA's "archive" was not surprising, since the procedures were similar to those used in connection with

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

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

other NSA SIGINT collection activities. Feb 17, 2009 Alexander Declaration at 11, n.6. If this is the case, then the root of the non-compliance is not a terminological misunderstanding, but the NSA's decision to treat the accessing of all call detail records produced by [REDACTED] no differently than other collections under separate NSA authorities, to which the Court-approved minimization procedures do not apply.

B. Misrepresentations to the Court

The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions of the alert list process to the FISC. Due to the volume of U.S. person data being collected pursuant to the Court's orders, the FISC's orders have all required that any renewal application include a report on the implementation of the Court's prior orders, including a description of the manner in which the NSA applied the minimization procedures set forth therein. See, e.g., BR 08-13, Primary Order at 12.

In its report to the FISC accompanying its first renewal application that was filed on August 18, 2006, the government described the alert list process as follows:

NSA has compiled through its continuous counter-terrorism analysis, a list of telephone numbers that constitutes an "alert list" of telephone numbers used by members of [REDACTED] This alert list serves as a body of telephone numbers employed to query the data....

[...] Each of the foreign telephone numbers that comes to the attention of the NSA as possibly related to [REDACTED] is evaluated to determine whether the information about it provided to NSA satisfies the reasonable articulable suspicion standard. If so, the foreign telephone number is placed on the alert list; if not, it is not placed on the alert list.

The process set out above applies also to newly discovered domestic

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

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

telephone numbers considered for addition to the alert list, with the additional requirement that NSA's Office of General Counsel reviews these numbers and affirms that the telephone number is not the focus of the analysis based solely on activities that are protected by the First Amendment....

....

As of the last day of the reporting period addressed herein, NSA had included a total of 3980 telephone numbers on the alert list, which includes foreign numbers and domestic numbers, after concluding that each of the foreign telephone numbers satisfied the [RAS standard], and each of the domestic telephone numbers was either a FISC approved number or in direct contact with a foreign seed that met those criteria.[³]

To summarize the alert system: every day new contacts are automatically revealed with the 3980 telephone numbers contained on the alert list described above, which themselves are present on the alert list either because they satisfied the reasonable articulable suspicion standard, or because they are domestic numbers that were either a FISC approved number or in direct contact with a number that did so. These automated queries identify any new telephone contacts between the numbers on the alert list and any other number, except that domestic numbers do not alert on domestic-to-domestic contacts.

NSA Report to the Foreign Intelligence Surveillance Court, Docket no. BR 06-05, filed Aug. 18, 2006 at 12-15 (emphasis added). This description was included in similar form in all subsequent reports to the Court, including the report submitted to this Court on December 11, 2008. Feb. 17, 2009 Memorandum at 13.

The NSA attributes these material misrepresentations to the failure of those familiar with

³The report further explained that identifiers within the second category of domestic numbers were not used as "seeds." NSA Report to the Foreign Intelligence Surveillance Court, Docket no. BR 06-05, filed Aug. 18, 2006 at 14. Moreover, rather than conducting daily queries of the RAS-approved foreign telephone identifier that originally contacted the domestic number, the domestic numbers were included in the alert list as "merely a quicker and more efficient way of achieving the same result..." *Id.* at 14 n.6. In November 2006, the NSA reported that it ceased this activity on August 18, 2006. Feb. 17, 2009 Alexander Declaration at 7 n.1.

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

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

the program to correct inaccuracies in a draft of the report prepared in August 2006 by a managing attorney in the NSA's Office of General Counsel, despite his request that recipients of the draft "make sure everything I have said (sic) is absolutely true."⁴ Feb. 17, 2009 Alexander Declaration at 16-17; see also id. at Exhibit D. Further, the NSA reports:

it appears there was never a complete understanding among the key personnel who reviewed the report for the SIGINT Directorate and the Office of General Counsel regarding what each individual meant by the terminology used in the report. Once this initial misunderstanding occurred, the alert list description was never corrected since neither the SIGINT Directorate nor the Office of General Counsel realized there was a misunderstanding. As a result, NSA never revisited the description of the alert list that was included in the original report to the Court.

Feb. 17, 2009 Alexander Declaration at 18. Finally, the NSA reports that "from a technical standpoint, there was no single person who had a complete technical understanding of the BR FISA system architecture. This probably also contributed to the inaccurate description of the alert list that NSA included in its BR FISA reports to the Court." Id. at 19.

Regardless of what factors contributed to making these misrepresentations, the Court finds that the government's failure to ensure that responsible officials adequately understood the NSA's alert list process, and to accurately report its implementation to the Court, has prevented,

⁴The Court notes that at a hearing held on August 18, 2006, concerning the government's first renewal application (BR 06-08), the NSA's affiant testified as follows:

THE COURT: All right. Now additionally, you have cause to be -- well at least I received it yesterday -- the first report following the May 24 order, which is a 90-day report, _____ and some 18 pages and I've reviewed that and you affirm that that's the best report or true and accurate to the best of your knowledge and belief.

I do, sir.

Transcript of Proceedings before the Hon. Malcolm J. Howard, U.S. FISC Judge, Docket No. BR 06-08, Aug. 18, 2006, at 12.

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

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

for more than two years, both the government and the FISC from taking steps to remedy daily violations of the minimization procedures set forth in FISC orders and designed to protect

call detail records pertaining to telephone communications of U.S. persons located within the United States who are not the subject of any FBI investigation and whose call detail information could not otherwise have been legally captured in bulk.

C. Other Non-Compliance Matters

Unfortunately, the universe of compliance matters that have arisen under the Court's Orders for this business records collection extends beyond the events described above. On October 17, 2008, the government reported to the FISC that, after the FISC authorized the NSA to increase the number of analysts authorized to access the BR metadata to 85, the NSA trained those newly authorized analysts on Court-ordered procedures. Sixty-Day Report for Filing in Docket Number BR 08-08, filed Oct. 17, 2008 at 7. Despite this training, however, the NSA subsequently determined that 31 NSA analysts had queried the BR metadata during a five day period in April 2008 "without being aware they were doing so." Id. (emphasis added). As a result, the NSA analysts used 2,373 foreign telephone identifiers to query the BR metadata without first determining that the reasonable articulable suspicion standard had been satisfied. Id.

Upon discovering this problem, the NSA undertook a number of remedial measures, including suspending the 31 analysts' access pending additional training, and modifying the NSA's tool for accessing the data so that analysts were required specifically to enable access to

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

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

the BR metadata and acknowledge such access. Id. at 8. Despite taking these corrective steps, on December 11, 2008, the government informed the FISC that one analyst had failed to install the modified access tool and, as a result, inadvertently queried the data using five identifiers for which NSA had not determined that the reasonable articulable suspicion standard was satisfied. Preliminary Notice of Compliance Incident, Docket no. BR 08-08, filed Dec. 11, 2008 at 2; see also Notice of Compliance Incident Involving Docket Number BR 08-08, filed Jan. 22, 2009. Then, on January 26, 2009, the government informed the Court that, from approximately December 10, 2008, to January 23, 2009, two NSA analysts had used 280 foreign telephone identifiers to query the BR metadata without determining that the Court's reasonable articulable suspicion standard had been satisfied. Notice of Compliance Incident, Docket No. BR 08-13, filed January 26, 2009 at 2. It appears that these queries were conducted despite full implementation of the above-referenced software modifications to the BR metadata access tool, as well as the NSA's additional training of its analysts.⁵ And, as noted below with regard to the NSA's routine use of the [] tool from May 2006 until February 18, 2009, the NSA continues to uncover examples of systemic noncompliance.

In summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how

⁵On October 17, 2008, the government reported that all but four analysts who no longer required access to the BR metadata had completed the additional training and were provided access to the data. Sixty-Day Report for Filing in Docket Number BR 08-08, filed Oct. 17, 2008 at 8 n.6.

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

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

the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively.

D. Reassessment of BR Metadata Authorization

In light of the foregoing, the Court returns to fundamental principles underlying its authorizations. In order to compel the production of tangible things to the government, the Court must find that there are reasonable grounds to believe 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, provided that such investigation of a U.S. person is not conducted solely on the basis of activities protected by the First Amendment. 50 U.S.C. § 1861.

The government's applications have all acknowledged that, of the _____ of call detail records NSA receives per day (currently over _____ per day), the vast majority of individual records that are being sought pertain neither to _____

_____. See, e.g., BR 08-13, Application at 19-20. In other words,

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

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

nearly all of the call detail records collected pertain to communications of non-U.S. persons who are not the subject of an FBI investigation to obtain foreign intelligence information, are communications of U.S. persons who are not the subject of an FBI investigation to protect against international terrorism or clandestine intelligence activities, and are data that otherwise could not be legally captured in bulk by the government. Ordinarily, this alone would provide sufficient grounds for a FISC judge to deny the application.

Nevertheless, the FISC has authorized the bulk collection of call detail records in this case based upon: (1) the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and include specific oversight requirements. Given the Executive Branch's responsibility for and expertise in determining how best to protect our national security, and in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of U.S. persons as required by applicable minimization procedures. To approve such a program, the Court must have every confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders. The Court no longer has such confidence.

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

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

With regard to the value of the BR metadata program, the government points to the 275 reports that the NSA has provided to the FBI identifying 2,549 telephone identifiers associated with the targets. Feb. 17, 2009 Alexander Declaration at 42. The government's submission also cites three examples in which the FBI opened three new preliminary investigations of persons in the U.S. based on tips from the BR metadata program. *Id.*, FBI Feedback on Report, Exhibit J. However, the mere commencement of a preliminary investigation, by itself, does not seem particularly significant. Of course, if such an investigation led to the identification of a previously unknown terrorist operative in the United States, the Court appreciates that it would be of immense value to the government. In any event, this program has been ongoing for nearly three years. The time has come for the government to describe to the Court how, based on the information collected and analyzed during that time, the value of the program to the nation's security justifies the continued collection and retention of massive quantities of U.S. person information.

Turning to the government's implementation of the Court-ordered minimization procedures and oversight regime, the Court takes note of the remedial measures being undertaken by the government as described in its recent filings. In particular, the Court welcomes the Director of the NSA's decision to order "end-to-end system engineering and process reviews (technical and operational) of NSA's handling" of BR metadata. Feb. 17, 2009 Alexander Declaration at 21. However, the Court is very disturbed to learn that this ongoing exercise has identified additional violations of the Court's orders, including the routine accessing of BR

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

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

metadata from May 2006 to February 18, 2009, through another NSA analytical tool known as [] using telephone identifiers that had not been determined to meet the reasonable articulable suspicion standard. BR 08-13, Notice of Compliance Incident, filed Feb. 26, 2009 ("Feb. 26, 2009 Notice").

In its last submission, the government describes technical measures implemented on February 20, 2009, designed to prevent any recurrences of the particular forms of non-compliance uncovered to date. This "technical safeguard" is intended to prevent "any automated process or subroutine," such as [] "from accessing the BR FISA data," and to prevent "analysts from performing manual chaining⁶] on numbers that have not been marked as RAS approved." See Supplemental Declaration of Lieutenant General Keith B. Alexander, United States Army, Director of NSA, filed Feb. 26, 2009 ("Feb. 26, 2009 Alexander Declaration") at 7 & n.2. On the strength of these measures, the government submits that "the Court need not take any further remedial action." Feb. 26, 2009 Notice at 6. After considering these measures in the context of the historical record of non-compliance and in view of the Court's authority and responsibility to "determine [and] enforce compliance" with Court orders and Court-approved procedures, 50 U.S.C. § 1803(i), the Court has concluded that further action is, in fact, necessary.

The record before the Court strongly suggests that, from the inception of this FISA BR

⁶ In context, "chaining" appears to refer to the form of querying the BR metadata known as "contact chaining." See [] Declaration at 6.

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

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

program, the NSA's data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures. From inception, the NSA employed two separate automated processes – the daily alert list and the [] tool – that routinely involved queries based on telephone identifiers that were not RAS-approved. See supra pp. 4-6, 13-14. As for manual queries, the minimization procedures required analysts to use RAS-approved identifiers whenever they accessed BR metadata, yet thousands of violations resulted from the use of identifiers that had not been RAS-approved by analysts who were not even aware that they were accessing BR metadata. See supra pp. 9-10.

Moreover, it appears that the NSA – or at least those persons within the NSA with knowledge of the governing minimization procedures – are still in the process of determining how the NSA's own systems and personnel interact with the BR metadata. Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures. In fact, the government acknowledges that, as of August 2006, "there was no single person who had a complete understanding of the BR FISA system architecture." Feb. 17, 2009 Alexander Declaration at 19. This situation evidently had not been remedied as of February 18, 2009, when "NSA personnel determined," only as a result of the "end-to-end review of NSA's technical infrastructure" ordered by the Director of the NSA on January 15, 2009, that the [] tool accessed the BR metadata on the basis of telephone identifiers that had not been RAS-approved. Feb. 26, 2009 Alexander Declaration at 2-3.

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

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

This end-to-end review has not been completed. Id. at 10. Nonetheless, the government submits that the technical safeguards implemented on February 20, 2009 “should prevent recurrences” of the identified forms of non-compliance, id. at 9 (emphasis added), and “expect[s] that any further problems NSA personnel may identify with the infrastructure will be historical,” rather than current, id. at 10 (emphasis added). However, until this end-to-end review has been completed, the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation – on February 18, 2009 – will be the last. Nor does the Court share the government’s optimism that technical safeguards implemented to respond to one set of problems will fortuitously be effective against additional problems identified in the future.

Moreover, even with regard to the particular forms of non-compliance that have been identified, there is reason to question whether the newly implemented safeguards will be effective. For example, as discussed above, the NSA reported on October 17, 2008, that it had deployed software modifications that would require analysts to specifically enable access to BR metadata when performing manual queries, but these modifications did not prevent hundreds of additional violations by analysts who inadvertently accessed BR metadata through queries using telephone identifiers that had not been RAS-approved. See supra pp. 9-10; Feb. 26, 2009 Alexander Declaration at 4. The Court additionally notes that, in a matter before another judge of the FISC, _____

_____ the mere existence of software solutions was not sufficient to ensure their efficacy:

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

- “NSA’s representations to the Court in the August 27, 2008, hearing did not explicitly account for the possibility that system configuration errors (such as those discussed in the government’s response to question 10 below) might render NSA’s overcollection filters ineffective, which was the root cause for some of the non-compliance incidents.” _____

_____ Government’s Response to the Court’s Order of January 16, 2009,
answer no. 8 at 13.

- “Troubleshooting has since revealed that a software patch that might have prevented the [compliance incident] was not present on the recently deployed selection system.” Id.,
answer no. 10 at 14.

- “NSA further determined [in January 2009] that the overcollection filter had not been functioning since this site was activated on July 30, 2008.” Id.

In light of what appear to be systemic problems, this Court cannot accept the mere introduction of technological remedies as a demonstration that a problem is solved. More is required. Thus, notwithstanding the remedial measures undertaken by the government, the Court believes that more is needed to protect the privacy of U.S. person information acquired and retained pursuant to the FISC orders issued in this matter. However, given the government’s repeated representations that the collection of the BR metadata is vital to national security, and in light of the Court’s prior determinations that, if the program is conducted in compliance with appropriate minimization procedures, such collection conforms with 50 U.S.C. §1861, the Court concludes it would not be prudent to order that the government’s acquisition of the BR metadata cease at this

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

time. However, except as authorized below, the Court will not permit the government to access the data collected until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data.

Accordingly, it is HEREBY ORDERED:

1. The NSA may continue to acquire all call detail records of "telephony metadata" created by [REDACTED] in accordance with the orders entered in the above-captioned docket on December 12, 2008;

2. The government is hereby prohibited from accessing BR metadata acquired pursuant to FISC orders in the above-captioned docket and its predecessors for any purpose except as described herein. The data may be accessed for the purpose of ensuring data integrity and compliance with the Court's orders. Except as provided in paragraph 3, access to the BR metadata shall be limited to the team of NSA data integrity analysts described in footnote 5 of the _____ Declaration, and individuals directly involved in developing and testing any technological measures designed to enable the NSA to comply with previously approved procedures for accessing such data;

3. The government may request through a motion that the Court authorize querying of the BR metadata for purposes of obtaining foreign intelligence on a case-by-case basis. However, if the government determines that immediate access is necessary to protect against an imminent threat to human life, the government may access the BR metadata for such purpose. In

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

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

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 determination that the reasonable articulable suspicion standard has been met with regard to that identifier, and, if the access has already taken place, a statement of the immediate threat necessitating such access;

4. Upon completion of the government's end-to-end system engineering and process reviews, the government shall file a report with the Court, that shall, at a minimum, include:

a. 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;

b. 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;

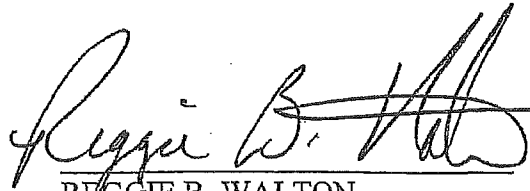
~~TOP SECRET//COMINT//NOFORN//MR~~

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

c. 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

d. 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.

IT IS SO ORDERED, this 2nd day of March, 2009.



REGGIE B. WALTON

Judge, United States Foreign Intelligence
Surveillance Court

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