

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

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



MEMORANDUM OPINION

This matter is before the Foreign Intelligence Surveillance Court ("FISC" or "Court") on the "Government's Ex Parte Submission of Amendments to DNI/AG 702(g) [REDACTED] Ex Parte Submission of Amended Minimization Procedures," which was filed on November 15,

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

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

2013 ("November 15 Submission"). Through the November 15 Submission, the government requests approval of amendments to all of [REDACTED] to permit the use of revised minimization procedures. For the reasons set forth below, the Court concludes that [REDACTED], as amended by the November 15 Submission, [REDACTED] the required statutory elements and that the revised minimization procedures are consistent with the applicable statutory requirements and the Fourth Amendment. Accordingly, the government's request for approval is granted.

I. PROCEDURAL BACKGROUND

The amendments that are included as part of the November 15 Submission were executed by the Attorney General ("AG") and the Director of National Intelligence ("DNI") pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which is codified at 50 U.S.C. § 1881a (2008). They are accompanied by three sets of revised minimization procedures for use by the National Security Agency ("NSA"), the Federal Bureau of Investigation ("FBI"), and the Central Intelligence Agency ("CIA"), respectively. The purpose of the amendments, which became effective immediately upon their execution, is to authorize the use of these revised minimization procedures in connection with information acquired under [REDACTED]

[REDACTED]

By operation of law, the amendments included as part of the November 15 Submission supersede the amendments that were submitted by the government on July 31, 2013, and which, as discussed below, were still pending before this Court for review on November 15. See 50

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

Page 2

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

U.S.C. § 1881a(i)(1)(C). The Court has 30 days from the date of submission to complete its review of the new amendments and issue an order and supporting written statement as required by Section 702. See id. §§ 1881a(i)(1)(C), (i)(3).

II. REVIEW OF THE AMENDMENTS

Under the judicial review procedures that apply to amendments by virtue of Section 1881a(i)(1)(C), the Court must review each of the amended certifications “to determine whether the certification contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court has previously determined that [REDACTED] filed in all of the above-captioned dockets, as originally submitted to the Court and previously amended, contained all the required elements. Like the prior certifications and amendments, the amendments now before the Court were executed under oath by the AG and the DNI, as required by Section 1881a(g)(1)(A), and submitted to the Court within the time allowed under Section 1881a(i)(1)(C). See Amendment to [REDACTED]

[REDACTED] Pursuant to Section 1881a(g)(2)(A)(ii), the latest amendments include the attestations of the AG and the DNI that the accompanying amended NSA, FBI, and CIA minimization procedures satisfy the statutory definition of minimization procedures, are consistent with the requirements of the Fourth Amendment, and will be submitted to the Court for approval. See [REDACTED]

[REDACTED] The latest amendments also include effective dates that comply with Section 1881a(i)(1). See [REDACTED]

[REDACTED] All other

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

Page 3

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

aspects of [REDACTED] in the above-captioned dockets – including the further attestations made therein in accordance with Section 1881a(g)(2)(A), the targeting procedures submitted therewith in accordance with Section 1881a(g)(2)(B), and the affidavits executed in support thereof in accordance with Section 1881a(g)(2)(C) – are unaltered by the latest amendments. In light of the foregoing, the Court finds that the above-captioned certifications, as amended, each contain all the required statutory elements. 50 U.S.C. § 1881a(i)(2)(A).

III. REVIEW OF THE REVISED MINIMIZATION PROCEDURES

The Court is required to review the revised NSA, FBI, and CIA minimization procedures to determine whether they are consistent with the requirements of Section 1881a(e)(1). See 50 U.S.C. § 1881a(i)(2)(C). Section 1881a(e)(1) requires that the minimization procedures “meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4).”¹ Further,

¹Sections 1801(h) and 1821(4) define “minimization procedures” in pertinent part as:

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance [or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;[]

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s identity is necessary to understand foreign intelligence information or assess its importance; [and]

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for

(continued...)

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

Page 4

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

under Section 1881a(i)(3)(A), the Court must determine whether the minimization procedures are consistent with the requirements of the Fourth Amendment.

The revised minimization procedures are, in most respects, identical to the corresponding procedures that this Court recently approved for use [REDACTED]

[REDACTED] In its August 30, 2013 Memorandum Opinion ("August 30 Opinion" or "Aug. 30 Op."), this Court concluded that the prior versions of these minimization procedures satisfied the definition set forth in footnote 1 above and the requirements of the Fourth Amendment. See Aug. 30 Op. at 15-25. As discussed in more detail below, the only changes to the procedures include: (1) new provisions in the NSA, FBI, and CIA minimization procedures requiring additional analysis to confirm the "foreignness" of the target before certain categories of previously-acquired communications may be used in any manner; and (2) a new provision in the FBI minimization procedures allowing the limited use of "ad hoc" storage systems to house FISA-acquired information. Accordingly, the Court incorporates by reference herein its August 30 Opinion and focuses the discussion below on the new provisions and whether those provisions alter the Court's recent conclusion that the NSA, FBI, and CIA minimization procedures satisfy the requirements of Section 1801(h) and the Fourth Amendment.

¹(...continued)
law enforcement purposes[.]

50 U.S.C. § 1801(h); see also id. § 1821(4). The definitions of "minimization procedures" set forth in these provisions are substantively identical (although Section 1821(4)(A) refers to "the purposes . . . of the particular physical search") (emphasis added). For ease of reference, subsequent citations refer only to the definition set forth in Section 1801(h).

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

Page 5

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

A. The New "Foreignness" Check Provisions of the NSA, FBI, and CIA Minimization Procedures

The first change mentioned above (the addition of new provisions requiring foreignness checks) was prompted by two recent noncompliance incidents, both of which involve the post-tasking checks that NSA conducts pursuant to its targeting procedures to ensure that telephone numbers tasked under Section 702 have not roamed into the United States.

1. [REDACTED]

The first noncompliance incident, which the Court discussed in its August 30 Opinion, was initially reported after [REDACTED] were filed on July 31, 2013. In notices submitted to the Court on August 13, 2013 ("August 13 Notice" or "[REDACTED] Notice") and [REDACTED] 2013 ("[REDACTED] Notice" or "[REDACTED] Notice"), the government explained that [REDACTED]

[REDACTED]

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

Page 6

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

[REDACTED]

By

NSA may determine

that a tasked telephone identifier is being used from inside the United States. See id. at 29; see also Docket No. [REDACTED] Exh. A (NSA Targeting Procedures) at 6.

[REDACTED]

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

Page 7

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

[REDACTED]
[REDACTED] From that point in time until [REDACTED]

[REDACTED] appears to have been totally ineffective in alerting NSA to uses of Section 702-tasked telephone numbers from locations within the United States. [REDACTED]

At the August 28 hearing, the government provided additional information regarding NSA's [REDACTED] 2013 "fix" of the [REDACTED] process. Representatives of NSA

[REDACTED]

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

Page 8

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

Based upon the information then available, the Court determined in the August 30 Opinion that NSA was prepared to comply with the "Post-Targeting Analysis" provisions of the NSA minimization procedures with respect to the information to be acquired pursuant to [REDACTED] See Aug. 30 Op. at 10. Accordingly, the Court concluded that the noncompliance problem discussed above did not preclude it from finding, for purposes of the 2013 [REDACTED] that NSA's targeting procedures were "reasonably designed" to "ensure that any acquisition authorized under [the 2013 [REDACTED] is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." See *id.* at 10-11 (citing Section 1881a(d)(1)).

However, NSA's past noncompliance with the post-tasking analysis requirements of its targeting procedures substantially affected the Court's review of the amendments to the prior Section 702 certifications that were included as part of the July 31 Submission. See *id.* at 11 n.7. As a result of the noncompliance, it appeared likely that NSA had failed totally to detask certain facilities that were no longer eligible for Section 702 collection, and had failed to detask others in a timely fashion. See *id.* Those failures, in turn, likely resulted in NSA's acquisition of communications falling outside the scope of Section 702, as NSA no longer had a reasonable belief that the users of such facilities were located outside the United States. See, e.g., [REDACTED] Notice at 2-3 (disclosing two such situations). It also appeared that other communication [REDACTED]

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

Page 9

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

[REDACTED]
[REDACTED] were not identified by NSA as “domestic communications,” which generally are subject to prompt deletion under NSA’s minimization procedures, but were instead incorrectly retained in NSA’s systems as “foreign communications.” See, e.g. [REDACTED]

[REDACTED] (NSA Minimization Procedures) at 7 (§ 3(c)(1)) (rules for retention of raw data); id. at 8-10 (§ 5) (rules for retention of domestic communications); id. at 10-13 (§§ 6-7) (rules for handling foreign communications).

At the time of the August 30, 2013 deadline for Court action, the government was still investigating these matters, and the record concerning them remained incomplete. See Aug. 30 Op. at 30 at 11 n.7. Accordingly, the Court was unable to complete its required review of the amendments at that time. See id. Until the scope of the past overcollection was determined, for example, the Court could not adequately assess whether, for purposes of information acquired under past certifications, the then-proposed minimization procedures satisfied FISA’s definition of minimization procedures, which requires, among other things, “specific procedures” that are “reasonably designed . . . to minimize the . . . retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” See id. (citing 50 U.S.C. § 1801(h)(1)). Furthermore, because the acquisition of telephone communications to or from persons located inside the United States is likely to constitute “electronic surveillance” within the meaning of Section 1801(f), the Court observed that any overcollection resulting from NSA’s noncompliance with its targeting procedures

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

Page 10

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

implicates FISA's prohibition on the use or disclosure of information with knowledge or reason to know that such information was obtained through unauthorized electronic surveillance. See id. (citing 50 U.S.C. § 1809(a)(2)). To permit full consideration of these issues on a complete record, the Court granted the government's motion to extend until October 25, 2013, the time for the Court to complete its review of the then-pending amendments. See id.

Thereafter, the government filed a series of bi-weekly reports regarding its investigation and remediation of the overcollection resulting from this compliance incident. In the first report, the government described its four-part framework for identifying [REDACTED] roaming by targets into the United States. The first step was to [REDACTED]

[REDACTED]

Second, when a potential roaming incident was discovered, NSA investigated further to determine whether a roaming incident had actually occurred – i.e., whether NSA had facilities for a Section 702 target tasked for acquisition during a period of roaming within the United States. See id. at 3. Third, when NSA discovered an actual roaming incident, it worked to determine whether the full scope of the incident had already been identified through NSA's other post-tasking procedures. See id. [REDACTED]

[REDACTED]

Fourth, and finally, when NSA discovered a previously unidentified instance of [REDACTED]

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

Page 11

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

acquisition while a target was inside the United States, NSA purged all the acquired data. See id.

The government ultimately reported that NSA had identified, to the extent feasible, all of the roaming incidents that it had missed due to the above-described problem [REDACTED]

[REDACTED]

[REDACTED] All of this data has been purged by the agencies that received it, and no reporting was produced based thereon. See id. at 3.

However, the above-described process was only a partial solution to the problem.

[REDACTED]

[REDACTED]. Accordingly, NSA could not [REDACTED] to identify instances of roaming that occurred from [REDACTED] NSA therefore adopted internal procedures requiring analysts seeking to use any communication acquired during this period to confirm through other means that there are reasonable grounds to believe that the target was located outside the United States at the time of acquisition. [REDACTED]

[REDACTED]

[REDACTED] The current versions of these procedures are discussed in more detail below.

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

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

2. [REDACTED] Problem

In the fourth of the biweekly reports described above, which was submitted on [REDACTED] 2013 (the Court's extended deadline for review of the then-pending amendments), the government disclosed another possible noncompliance problem [REDACTED]

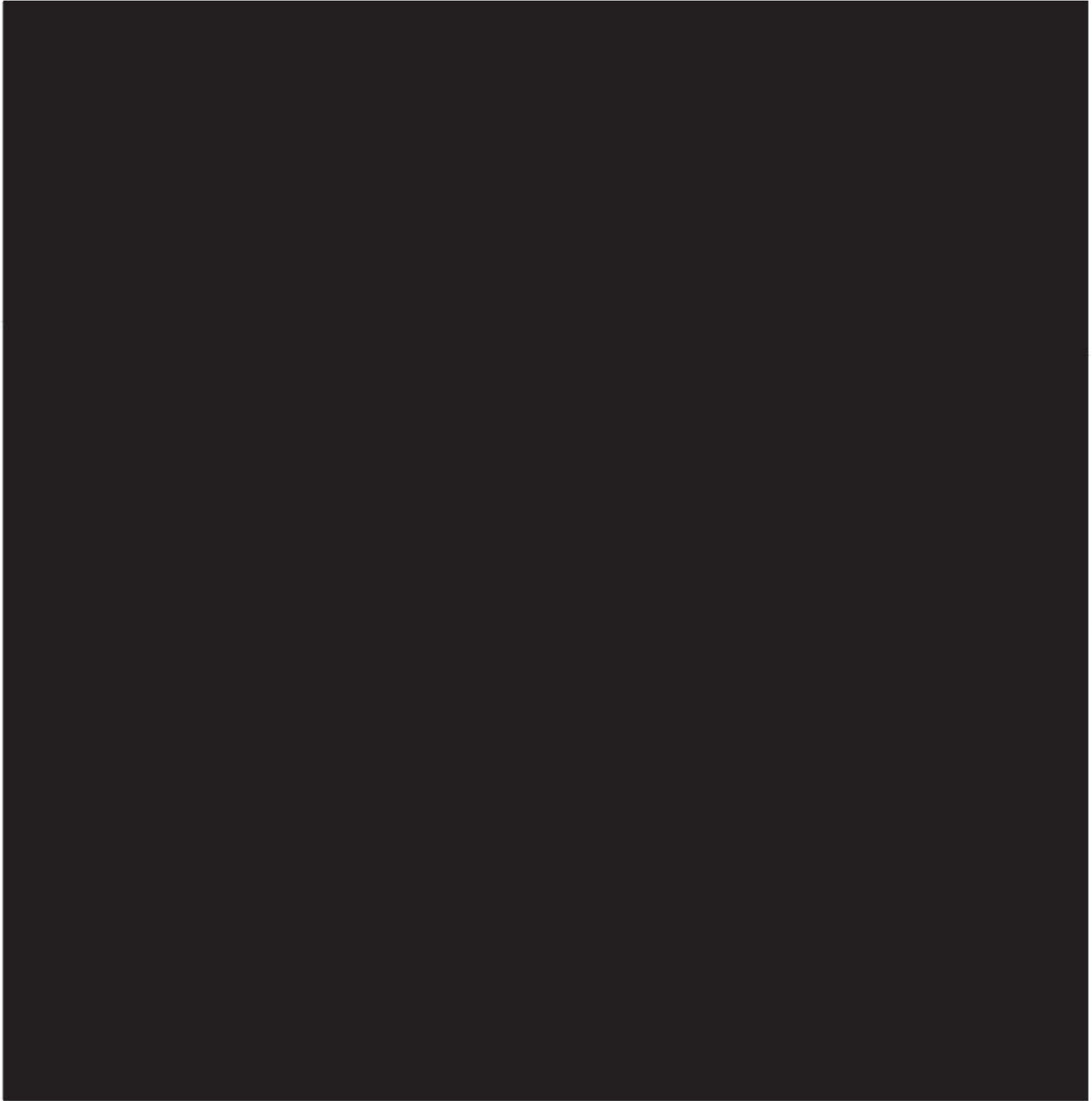
[REDACTED] Because of the lack of information regarding the nature or scope of the new problem and its possible effect on the Court's assessment of the then-pending amendments, the Court entered an order further extending the deadline for its review until [REDACTED] 2013, and scheduling a hearing on the matter for November 5, 2013. Oct. 29, 2013 Order at 3-4.

At the November 5 hearing and in letters submitted on [REDACTED] 2013 [REDACTED] Notice" or [REDACTED] Notice") and [REDACTED] 2013 (" [REDACTED] Notice" or [REDACTED] Notice"), the government described the new problem, [REDACTED]

[REDACTED]

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

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



2



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

Page 14

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

[REDACTED] By [REDACTED], NSA had implemented system modifications [REDACTED]

[REDACTED] Additionally, NSA [REDACTED] adopted internal procedures requiring analysts to conduct the foreignness checks (the same checks that are described above in connection with the first incident) before using potentially-affected communications acquired pursuant to Section 702. See id. at 2. Pursuant to these procedures, an analyst cannot use any such communication without first confirming that there are reasonable grounds to believe that the target was outside the United States at the time of acquisition. [REDACTED]

On November 8, 2013, the Court granted the government's motion to further extend the deadline for judicial review of the pending amendments that were filed as part of the July 31 Submission until November 15, 2013. See Nov. 8 Order at 6. On November 15, 2013, the government submitted the new amendments and revised minimization procedures that are now before the Court, which, as noted above, superseded the amendments submitted on July 31, 2013, and triggered a new 30-day period for judicial review.

3. The Foreignness Check Requirement

As noted above, the primary change to all three sets of revised procedures (and the only change to the NSA and CIA procedures) is the addition of a provision requiring each agency to conduct the "foreignness" determinations described above. Each contains the following new language:

[REDACTED]

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

Page 15

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

section 702 during a time period when there is uncertainty about the location of the target of the acquisition because the [REDACTED] post-tasking checks described in NSA's section 702 targeting procedures were not functioning properly, [agency] will follow its internal procedures for determining whether such information may be used (including, but not limited to, in FISA applications, section 702 targeting, and disseminations). Except as necessary to assess location under this provision, [agency] may not use or disclose any information acquired pursuant to section 702 during such time period unless [agency] determines, based on the totality of the circumstances, that the target is reasonably believed to have been located outside the United States at the time the information was acquired. If [agency] determines that the target is reasonably believed to have been located inside the United States at the time the information was acquired, such information will not be used and will be promptly destroyed.

Revised NSA Minimization Procedures at 8 (§ 3(e)); Revised FBI Minimization Procedures at 16-17 (§ III.F.1); Revised CIA Minimization Procedures at 7-8 (§ 9).³

The government has submitted a copy of each agency's internal implementing procedures, which the Court has reviewed. The NSA internal procedures apply to [REDACTED] information, each of which corresponds [REDACTED] non-compliance incidents discussed above. [REDACTED]

³ [REDACTED]

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

Page 16

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

classified at a level higher than TOP SECRET//SI//NOFORN. See id. (specifying six covered classification markings).

Pursuant to NSA's internal procedures, an analyst seeking to use information [REDACTED] must first "conduct additional verification of the target's location at the time the data was acquired." [REDACTED]. Analysts are first directed to assess whether the content of the communication sought to be used [REDACTED] provides a reasonable basis for believing that the target was outside the United States at the time. [REDACTED] If so, the determination and its basis must be documented [REDACTED]

[REDACTED]

[REDACTED] in the event that an analyst determines that there is a reasonable basis for believing that the target was inside the United States at the time of acquisition, the communication must be "promptly destroyed." [REDACTED]

[REDACTED]

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

Page 17

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

The Court is satisfied that the new foreignness check provisions of the NSA, FBI, and CIA minimization procedures, as implemented pursuant to each agency's internal operating procedures, are adequate to address the compliance problems discussed above and that the revised minimization procedures satisfy the requirements of FISA. As noted above, the applicable definition of "minimization procedures" requires, in pertinent part:

⁴ The FBI Internal Procedures apply by their terms to Section 702-acquired information residing in **exempt under b(7)E** that the Court understands to be the principal FBI repositories for such information. The internal procedures direct FBI personnel who encounter "Section 702 products from the affected time period . . . residing outside" **exempt under b(7)E** to contact the Office of General Counsel for separate guidance. See FBI Internal Procedures at 5. The Court emphasizes that all Section 702-acquired information falling within the terms of Section III.F.1 of the Revised FBI Minimization Procedures must be handled in accordance therewith, regardless of where it is stored.

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

Page 18

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

specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information”

50 U.S.C. § 1801(h).

The “purpose . . . of the particular surveillance” at issue here – collection under Section 702 – is to acquire information concerning non-United States persons who are reasonably believed to be located outside the United States at the time of acquisition. See 50 U.S.C. 1881a(a)-(b). It is principally the function of the applicable targeting procedures to ensure that collection is so limited. See id. § 1881a(d). To that end, NSA’s targeting procedures require NSA, among other things, to establish before tasking a facility that the target of collection is a non-United States person reasonably believed to be located outside the United States and thereafter to conduct ongoing post-tasking analysis to ensure that those circumstances have not changed. See [REDACTED] (NSA Targeting Procedures) at 1-7. Here, however, due to the two noncompliance problems discussed above, NSA was not fully effective in applying the post-tasking provisions of its targeting procedures. As a result of the first problem, and possibly also as a result of the second, NSA acquired the communications of targets while they were located inside the United States. The Court must consider this overcollection in assessing whether the revised minimization procedures are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign

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

Page 19

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

intelligence information” and whether they are consistent with the Fourth Amendment.

Section 702 targets located inside the United States are more likely than those outside the United States to communicate with other persons located inside the United States, including United States persons.⁵ For example, [REDACTED]

[REDACTED] Many of those communications are likely to contain information concerning United States persons – or other persons in the United States who are entitled to Fourth Amendment protection – and to lack any foreign intelligence value.

The Court is satisfied that the revised minimization procedures are reasonably designed to minimize the retention and prohibit the dissemination of such communications. Through [REDACTED] [REDACTED], NSA was able to identify and purge a number of roamer communications from government systems. [REDACTED] Any additional roamer communications that are discovered through the foreignness checks required by the revised procedures will be purged. Other communications obtained during the affected period cannot be used unless and until the government has documented a basis for believing that the target was outside the United States at the time of acquisition. Once such a determination has been made, United States-person information included in the communication is subject to the

⁵

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

Page 20

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

rules for retention and dissemination that the Court has previously approved.⁶ In light of the foregoing, the Court concludes that the revised provisions for foreignness checks are consistent with Section 1801(h) and the Fourth Amendment.⁷

⁶ As noted above, the Court concluded in the August 30 Opinion that any overcollection resulting from NSA's noncompliance with its targeting procedures implicates FISA's criminal prohibition on the use or disclosure of information with knowledge or reason to know that such information was obtained through unauthorized electronic surveillance. See Aug. 30 Op. at 11 n.7 (citing 50 U.S.C. § 1809(a)(2)).

The Court is satisfied that foreignness checks mandated by the revised minimization procedures are reasonably designed to enable the government to identify [REDACTED] communications that may have been acquired and to avoid the use or disclosure of such communications in accordance with Section 1809(a)(2).

⁷

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

Page 21

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

B. Storage of Unminimized FISA-Acquired Information in "Ad Hoc" FBI Databases

The Revised FBI Minimization Procedures contain a second new provision that was prompted by another compliance-related matter that is discussed in the August 30 Opinion. See Aug. 30 Op. at 19-22. On [REDACTED] 2013, the government submitted a Notice of Compliance Incident Regarding Storage of Raw FISA-Acquired Information [REDACTED] Notice") in which it reported potentially substantial noncompliance by the FBI with provisions of the FBI Standard Minimization Procedures ("SMPs") for electronic surveillance and physical search. Because the FBI minimization procedures for Section 702 contain similar provisions, the Court noted that the [REDACTED] Notice had potential implications in the Section 702 context. See Aug. 30 Op. at 19.

The FBI SMPs for electronic surveillance and physical search require, among other things, that FBI electronic storage systems have certain capabilities: for example, such systems must be able to track how personnel access raw data and record query terms that they use, see FBI SMPs §§ III.B.3, III.D, and to permit appropriate personnel to mark reviewed data as foreign

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

Page 22

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

intelligence information, necessary to understand foreign intelligence information, or evidence of a crime, see id. § III.C. The FBI's Section 702 minimization procedures submitted by the government on July 31, 2013, and prior versions of the procedures, contained similar corresponding provisions. See [REDACTED] (FBI Minimization Procedures) §§ III.B.3, III.C & III.D. The markings required by these provisions enable the FBI to implement access restrictions and destruction requirements that apply to raw information that has never been reviewed or that has been reviewed but not found pertinent. See, e.g., FBI SMPs § III.G.1.

In the July 17 Notice, the government disclosed various types of FBI systems that:

generally are not configured to apply [REDACTED] minimization markings. These systems also do not track queries or information that has been exported from these systems. And, [REDACTED] these systems generally do not log or track accesses. Furthermore, there are no FBI policies regarding the above systems containing raw FISA-acquired information, as required by the FBI SMPs.

[REDACTED] Notice at 3. These systems range from an individual laptop onto which an agent may download raw FISA-acquired information "in order to more easily manipulate and analyze the data," id. at 2, to [REDACTED] system that is generally available within the FBI.

[REDACTED]

On [REDACTED] 2013, the government submitted a Supplemental Notice Regarding Storage of Raw FISA-Acquired Information by the FBI ([REDACTED] Notice" or "[REDACTED]

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

Page 23

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

Notice”), in which it clarified that the instances of noncompliance that were the subject of the [REDACTED] Notice were limited to information acquired pursuant to either Title I or III of FISA. See [REDACTED] Notice at 2. The [REDACTED] Notice further explained that the FBI stores raw Section 702-acquired information [REDACTED] compliant with the applicable minimization procedures. See id. at 1-2. The government also informed the Court that, in its investigation of this matter to date, the Department of Justice’s Office of Intelligence “ha[d] not identified instances of FISA Section 702-acquired information being stored in systems not compliant with the FBI [minimization procedures].” Id. at 2. According to the government, the FBI was in the process of surveying field offices regarding the manner in which FISA-acquired information, including Section 702 information, was being stored. Id. The government committed to furnish the Court with updated information. Id.

In light of the information provided by the government before the issuance of the August 30 Opinion, the Court concluded that the FBI was prepared to comply with the marking, auditing, and notification requirements of its Section 702 minimization procedures with respect to the information to be acquired pursuant to [REDACTED] Op. at 22. Accordingly, the Court concluded that the noncompliance described in the [REDACTED] Notice did not preclude it from finding that the amended FBI minimization procedures meet the requirements of Section 1801(h). Id.

Thereafter, on [REDACTED] 2013, the government notified the Court that additional investigation had revealed that copies of Section 702-acquired information had in fact been placed in non-compliant FBI systems [REDACTED]. See Supplemental Notice

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

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

Regarding Storage of FISA-Acquired Information by the Federal Bureau of Investigation, filed on [REDACTED] 2013 at 1-2. It generally appears that the FBI moved such information to noncompliant systems to allow personnel to work with it using tools not available on compliant systems [REDACTED] See id. The government reported that the FBI had sequestered the Section 702-acquired information already stored on non-compliant systems and directed that no additional information be placed on such systems. See id. at 2. The government further reported that the FBI was prepared to comply with the marking, auditing, and notification requirements of the Section 702 minimization procedures with respect to the information acquired pursuant to [REDACTED]

[REDACTED] See id.⁸

The revised FBI minimization procedures contain a new Section IV that permits the FBI, in some circumstances, to retain, review, and analyze unminimized FISA-acquired information in databases or systems that do not comply with the requirements of Section III. See Revised FBI Minimization Procedures at 22-26. Section IV permits the use of such “ad hoc databases” in cases where FBI personnel engaged in a particular investigation are unable to fully and completely review or analyze raw Section 702-acquired information in a compliant system. See id. at 22. FISA-acquired information in ad hoc databases is subject to the dissemination and disclosure provisions set forth in Section V, and the oversight provisions in Section VI, all of

⁸ Separately, the government has provided the Court with additional information, both in writing and during two recent hearings, regarding the steps being taken by the government to address the FBI’s noncompliance with the similar provisions of its SMPs for electronic surveillance and physical search.

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

Page 25

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

which have previously been approved by this Court. See id.

Section IV imposes a number of additional requirements on the use of such “ad hoc” systems, including access limitations, retention restrictions, query limitations and auditing requirements, and procedures for handling privileged attorney-client communications. See id. at 22-26. Access to raw FISA-acquired information contained in an ad hoc database must be limited to those individuals who are engaged in the particular investigation or responsible for assessing or analyzing the information in question. See id. at 22. The FBI is required to maintain a record of employees who have access to each ad hoc database, and it must identify such databases in a manner sufficient to alert users that FISA-acquired information is contained therein. See id. at 22-23. Raw FISA-acquired information that is believed to contain information concerning unconsenting United States persons may be placed in an ad hoc database for the purpose of allowing FBI to determine whether it contains foreign intelligence information, information necessary to understand foreign intelligence information, or evidence of a crime. See id. at 23.

FISA-acquired United States-person information that has not been determined to be foreign intelligence information, necessary to understand foreign intelligence information, or evidence of a crime must be destroyed no later than five years from the expiration of the certification authorizing the collection of the information unless a specified supervisory official determines in writing that an extension of up to one year is necessary to further analyze the information. See id. Raw FISA-acquired information that appears to be encrypted or to contain secret meaning may be retained longer for the purpose of enabling cryptanalysis. See id. at 24.

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

Page 26

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

FBI personnel who are authorized to have access to raw FISA-acquired information in an ad hoc database are permitted to “analyze the data to find, extract, review, translate, and assess whether such information reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information, or evidence of a crime.” See id. Such personnel may also query the information using keyword searches that are reasonably designed to find and extract foreign intelligence information or evidence of a crime. See id. The FBI must document the analytical techniques and keyword searches used in connection with FISA-acquired information in ad hoc databases. See id.

Finally, Section IV contains special rules for the retention of attorney-client privileged communications in ad hoc databases. See id. at 25-26. Generally, such communications must be removed from ad hoc databases



In light of the foregoing, the Court is satisfied that Section IV is narrowly tailored to meet the government’s legitimate foreign-intelligence needs and that it adequately ensures that United States person information housed in ad hoc systems will be retained and disseminated in accordance with the requirements of Section 1801(h) and the Fourth Amendment.

IV. CONCLUSION

For the foregoing reasons, the Court finds that amendments submitted as part of the

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

Page 27

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

November 15 Submission contain all the required statutory elements and that the revised minimization procedures adopted in connection with those amendments are consistent with 50 U.S.C. §1881a(e) and with the Fourth Amendment. An order approving the amendments and the use of the accompanying procedures is being entered contemporaneously herewith.

ENTERED this 13th day of December 2013



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

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

Page 28

exempt under b(6) Chief Deputy
Clerk, FISC, certify that this document
is a true and correct copy of the
original exempt
under
b(6)

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.



ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds pursuant to 50 U.S.C.

§ 1881a(i)(3)(A) that [REDACTED] referenced above, as amended, [REDACTED] all the required statutory elements and that the revised minimization procedures adopted for use in connection

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

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

with [REDACTED] consistent with the requirements of Section 1881a(e) and with the Fourth Amendment.

Accordingly, it is hereby ORDERED pursuant to Section 1881a(i)(3)(A) that the

[REDACTED] and the use of such procedures are approved.

ENTERED this 13th day of December, 2013 [REDACTED]
[REDACTED]


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

[REDACTED] exempt
under b(6) Chief Deputy
Clerk, FISC, certify that this document
is a true and correct copy of the
original [REDACTED] exempt
under b(6)

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

Page 2