UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

MEMORANDUM OPINION

These matters are before the Foreign Intelligence Surveillance Court ("FISC" or "Court") on: [redacted]

[redacted]. Through these filings (all of which were submitted on October 31, 2011, and hereinafter will be referred to collectively as the "October 31 Submissions"), the government seeks approval of amended minimization procedures for the National Security Agency ("NSA"), which reflect changes that are intended to correct the deficiencies identified by the Court in its October 3, 2011 Memorandum Opinion ("October 3 Opinion"). For the reasons stated below, the Court concludes that with regard to information acquired pursuant to Certifications [redacted], the government has adequately corrected the deficiencies identified in the October 3 Opinion, and the request for approval is therefore granted.

I. BACKGROUND

In the October 3 Opinion, the Court concluded that one aspect of the collection conducted under past Section 702 certifications and proposed under Certifications [redacted] – NSA's "upstream collection" of Internet transactions containing multiple communications, or MCTs – was, in some respects, deficient on statutory and constitutional grounds. The Court found in pertinent part that NSA's minimization procedures, as the government proposed to apply them to MCTs as to which the "active user" is not known to be a tasked selector, did not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention, and that NSA's targeting and minimization procedures, as the government proposed to apply them to such MCTs, were inconsistent with the requirements of the Fourth Amendment. See October 3 Opinion at 2, 59-63, 69-80. Pursuant to 50 U.S.C. § 1881a(i)(3)(B), the Court directed the government, at its election, to correct the deficiencies identified in the October 3 Opinion

within 30 days, or to cease the problematic portion of the collection. See October 3, 2011 Order at 3-4. The government has chosen to attempt to correct the deficiencies by submitting and implementing the amended NSA minimization procedures that are now before the Court.

II. REVIEW OF AMENDED CERTIFICATIONS

The government executed and submitted the amendments to Certifications [redacted], including the amended NSA minimization procedures, pursuant to 50 U.S.C. § 1881a(i)(1)(C), which provides that:

> The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting and minimization procedures adopted in accordance with subsections (d) and (e) as necessary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.

The government submitted the amendments within the time allowed by the statute, and the Attorney General and the Director of National Intelligence properly authorized the use of the amended minimization procedures pending the Court's review. See Amendment to [redacted] at 3.[1]

---

[1] The government has confirmed that "NSA is fully complying with the amended minimization procedures" with respect to information acquired pursuant to Certifications [redacted] See Government's Responses to FISC Questions Re: Amended 2011 Section 702 Certifications ("Nov. 15 Submission") at 1. As discussed more fully below, the government has not yet formally amended the NSA minimization procedures applicable to information collected under the prior Section 702 certifications, but NSA is applying a modified

Under the judicial review provisions that are incorporated by reference into Section 1881a(i)(C), the Court must review the certifications, as amended, to determine whether they contain all the required elements. The Court concluded in the October 3 Opinion that Certifications [redacted], as originally submitted, contained all the required elements. See October 3 Opinion at 11-12. Like the original certifications, the amendments now before the Court were executed under oath by the Attorney General and the Director of National Intelligence, as required by 50 U.S.C. § 1881a(g)(1)(A). See Amendment to [redacted] at 4-5. Pursuant to Section 1881a(g)(2)(A)(ii), the amendments include the attestation of the Attorney General and the Director of National Intelligence that the amended NSA minimization procedures meet the statutory definition of minimization procedures and have been submitted to the FISC for approval. See Amendment to Certification [redacted] The amendments state that "[a]ll other aspects" of the certifications, as originally submitted, "remain unaltered and are incorporated herein." See Amendment to Certification [redacted] Accordingly, the Court finds that Certifications [redacted], as amended, contain all the required elements.

---

version of the amended NSA minimization procedures to Internet transactions acquired pursuant to those certifications.

III. REVIEW OF AMENDED NSA MINIMIZATION PROCEDURES

The Court also must review the amended NSA minimization procedures included as part of the October 31 Submissions to determine whether they satisfy FISA's statutory definition of minimization procedures[2] and are consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(2)(C), (i)(3)(A). For the reasons set forth below, the Court concludes that NSA's amended minimization procedures satisfy the applicable requirements and thus correct the deficiencies found by the Court in its October 3 Opinion with respect to information acquired pursuant to Certifications [redacted].

1. The Deficiencies Identified by the Court in the October 3 Opinion

In the October 3 Opinion, the Court concluded that the NSA minimization procedures, as the government proposed to apply them to Internet transactions containing multiple communications, did not satisfy FISA's definition of minimization procedures with respect to the retention of information concerning United States persons. See Oct. 3 Opinion at 59-63. The NSA minimization procedures generally require that, "[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime," see Amended NSA Minimization Procedures at 4 (§ 3(b)(4)), so that it can be promptly

---

[2] FISA's definition of minimization procedures requires, in pertinent part, "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." 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A).

afforded the appropriate treatment under the procedures. The measures previously proposed by the government for MCTs, however, largely dispensed with the requirement of prompt disposition upon initial review by an analyst. Rather than attempting to identify and segregate information not relevant to the authorized purpose of the acquisition or to destroy such information promptly following acquisition, NSA's proposed handling of MCTs tended to maximize the retention of such information, including information of or concerning United States persons with no direct connection to any target. Except in the case of MCTs recognized by analysts as containing at least one wholly domestic communication, which would be destroyed, MCTs that had been reviewed by analysts would remain available to other analysts in NSA's repositories without any marking to identify them as MCTs or as containing non-target information of or concerning United States persons. See Oct. 3 Opinion at 59-60. All MCTs except those identified as containing one or more wholly domestic communication would be retained for a minimum of five years. See id.

The Court explained that the net effect of the government's proposal was that thousands of wholly domestic communications (those that are never reviewed and those that are not recognized by analysts as being wholly domestic), and thousands of other discrete communications that are not to or from a targeted selector but that are to, from, or concerning a United States person, would be retained by NSA for at least five years, despite the fact that they had no direct connection to a targeted selector and, therefore, were unlikely to contain foreign intelligence information. See id. at 60-61. Accordingly, the Court concluded that the NSA minimization procedures, as NSA proposed to apply them to MCTs, were not reasonably

designed to "minimize the . . . retention . . . 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." Id. at 62-63 (quoting 50 U.S.C. § 1801(h)(1)). For largely the same reasons, the Court concluded that the procedures previously proposed by the government for handling MCT's were inconsistent with the requirements of the Fourth Amendment. See Oct. 3 Opinion at 78-79.

2. Overview of NSA's New Process for Handling MCTs

The measures now before the Court for handling MCTs contain three main elements: (1) the post-acquisition segregation of those types of transactions that are most likely to contain non-target information concerning United States persons or persons in the United States; (2) special handing and marking requirements for transactions that have been removed from or that are not subject to segregation; and (3) a two-year default retention period for all upstream acquisitions. Each of these elements is described more fully in the following discussion.

Under the amended NSA minimization procedures, NSA must segregate and restrict access to certain portions of its upstream collection following acquisition.[3] Section 3(b)(5)(a) requires NSA to

> take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the [user of] the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably

[3] The Court understands that NSA will not share unminimized communications acquired through its upstream collection pursuant to Section 6(c) or Section 8 of the amended NSA minimization procedures. See Nov. 15 Submission at 3.

believed to [redacted].

Amended NSA Minimization Procedures at 4; see also Nov. 15 Submission at 1. Transactions that are segregated pursuant to this provision

> will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States.

Amended NSA Minimization Procedures at 4 (§ 3(b)(5)(a)(1)). No segregated Internet transaction (and no information contained in a segregated Internet transaction) may be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete wholly domestic communication. Id. at 4 (§ 3(b)(5)(a)(1)(a)). Any segregated transaction that is identified as containing a wholly domestic communication "will be destroyed upon recognition." Id.

All transactions that are moved or copied from the segregated repository into repositories more generally accessible to NSA analysts must be "marked, tagged, or otherwise identified" as having previously been segregated pursuant to Section 3(b)(5)(a). Id. at 5 (§ 3(b)(5)(a)(1)(c)). In addition, all MCTs acquired through NSA's upstream collection, including those that have been copied or moved from segregation, are subject to special handling rules on top of the other applicable provisions of the minimization procedures. Pursuant to the special handling provisions, which are set forth in Sections 3(b)(5)(b)(1) and (b)(2), NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications

must first make a series of determinations, see id. at 5-6 (§ 3(b)(5)(b)(1)-(b)(2)), each of which must be documented if the discrete communication is used, see id. at 6 (§ 3(b)(5)(b)(3)).

The analyst must first determine whether or not the discrete communication sought to be used is a wholly domestic communication. See id. at 5 (§ 3(b)(5)(b)(1)). To the extent reasonably necessary to make that determination, the analyst will "perform checks to determine the locations of the sender and intended recipients." Id. If the discrete communication sought to be used is a wholly domestic communication, the entire transaction must be destroyed. See Nov. 15 Submission at 1.

If the discrete communication that the analyst seeks to use is not a wholly domestic communication, the analyst must determine whether the discrete communication is to, from, or about a tasked selector. See Amended NSA Minimization Procedures at 5-6 (§ 3(b)(5)(b)(2)). If the analyst determines that it is not, but that it is "to or from an identifiable U.S. person or a person reasonably believed to be located in the U.S.," then the discrete communication "cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations)." Id. at 5-6 (§ 3(b)(5)(b)(2)(c)).[4] In addition, if it is "technically possible or reasonable feasible" to do so, the analyst must document in the relevant analytic repository or tool his or her determination that the transaction contains a discrete communication that is not to, from, or about a tasked selector but that is to or from an identifiable United States person or a person reasonably believed to be located in the United

[4] NSA must report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which must promptly notify the FISC of such use. See Amended NSA Minimization Procedures at 6 (§ 3(b)(5)(b)(2)(c)).

States. See id.[5] A record of the analyst's determination will remain associated with the transaction in NSA's systems and will be visible to any other analyst who later uses the same repository or tool to view the transaction.

If the discrete communication that the analyst wishes to use is determined to be to, from, or about a tasked selector, the transaction (including any United States person information contained therein) must be handled in accordance with the remainder of the minimization procedures. Id. at 5 (§ 3(b)(5)(b)(2)(a)). The same is true of a discrete communication that is not to, from, or about a tasked selector but that is determined not to be to or from an identifiable United States person or a person reasonably believed to be located in the United States. Id. at 5 (§ 3(b)(5)(b)(2)(b)). An analyst seeking to use (e.g., in a FISA application, in an intelligence report, or in a Section 702 targeting decision) a discrete communication within an Internet transaction that contains multiple discrete communications must document each of the determinations required by the special handling provisions at Sections 3(b)(5)(b)(1) and (b)(2). Id. at 6 (§ 3(b)(5)(b)(3)).

Finally, the government has shortened the default retention period for Internet communications acquired by NSA through its upstream collection from five years to two years. Section 3(c)(2) of the amended NSA minimization procedures provides as follows:

---

[5] The government has explained that some, but not all, of the analytic repositories and tools used by its analysts are enabled to record comments by analysts. The documentation requirement in Section 3(b)(5)(b)(2)(c) will only apply when the analytic repository or tool being used is enabled to accept analyst comments. See Nov. 15 Submission at 2-3. In light of the large volume of non-target communications being acquired, it is the Court's expectation that NSA will, over time, work to expand its capability to record analyst comments, particularly in any new systems that will be used to handle information acquired through NSA's upstream collection.

> Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. All Internet transactions may be retained no longer than two years from the expiration date of the certification authorizing the collection in any event. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications.[6] Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and processed only in accordance with the standards set forth in subsection 3(b)(5) of these procedures.

Id. at 7 (emphasis added.) Under this provision, any Internet transaction that has not been destroyed sooner will "age off" two years after the expiration of the certification authorizing the collection. See Nov. 15 Submission at 3.

3. The Amended Procedures for Handling MCTs Satisfy the Applicable Requirements

The amended NSA minimization procedures mark a substantial improvement over the measures previously proposed by the government for handling MCTs. The revised process is more consistent with the overall framework of the minimization procedures, which, as noted above, generally require NSA promptly to identify and segregate information not relevant to the authorized purpose of the acquisition and to destroy such information promptly following acquisition. Unlike the measures previously proposed by the government for MCTs, the new procedures require NSA, following acquisition, to identify and segregate the two categories of

---

[6] The Court understands this sentence to refer only to Internet transactions that contain wholly domestic communications but that are not recognized as such by NSA. All such transactions will be destroyed two years after expiration of the certification authorizing their collection. See Nov. 15 Submission at 3.