Filed
United States Foreign
Intelligence Surveillance Court

APR 26 2017

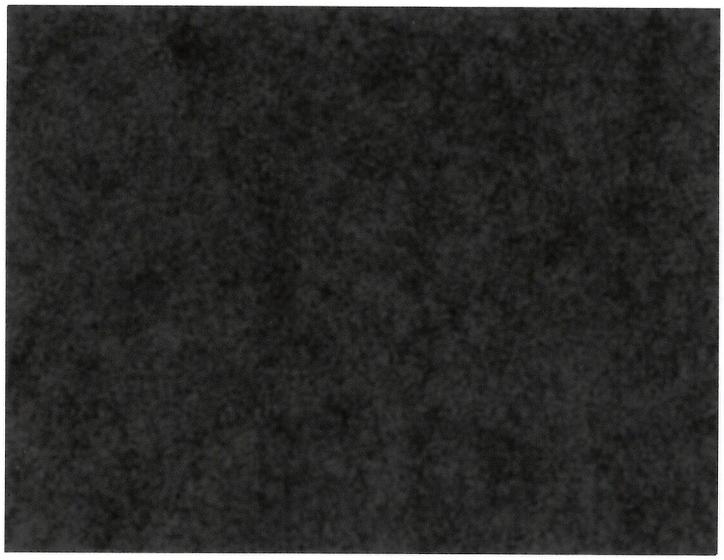
LeeAnn Flynn Hall, Clerk of Court

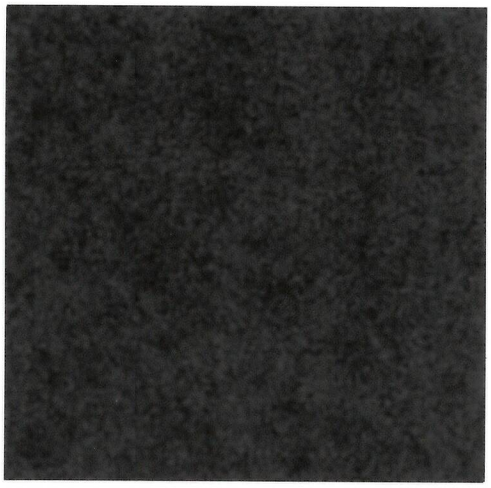
~~TOP SECRET//SI//ORCON/NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.





MEMORANDUM OPINION AND ORDER

These matters are before the Foreign Intelligence Surveillance Court ("FISC" or "Court") on the "Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications," which was filed on September 26, 2016 ("September 26, 2016 Submission"), and the "Government's Ex Parte Submission of Amendments to DNI/AG 702(g) Certifications and Ex Parte Submission of Amended Targeting and Minimization Procedures," which was filed on March 30, 2017 ("March 30, 2017 Submission"). (Collectively, the September 26, 2016 and March 30, 2017 Submissions will be

referred to herein as the "2016 Certification Submissions.") For the reasons explained below, the government's request for approval of the certifications and procedures accompanying the September 26, 2016 Submission, as amended by the March 30, 2017 Submission, is granted, subject to certain reporting requirements. The Court's approval of the amended certifications and accompanying targeting and minimization procedures is set out in separate orders, which are being entered contemporaneously herewith.

I. BACKGROUND

A. The Initial 2016 Certifications

The September 26, 2016 Submission included [redacted] certifications that 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" or "the Act"), which is codified at 50 U.S.C. § 1881a [redacted] Each of the [redacted] certifications submitted in September (collectively referred to as "the Initial 2016 Certifications") was accompanied by the supporting affidavits of the Director of the National Security Agency ("NSA"), the Director of the Federal Bureau of Investigation ("FBI"), the Director of the Central Intelligence Agency ("CIA"), and the Director of the National Counterterrorism Center ("NCTC"); two sets of targeting procedures, for use by the NSA and FBI respectively;[1] and four sets of minimization procedures, for use by the

[1] The targeting procedures for each of the Initial 2016 Certifications are identical. The (continued...)

NSA, FBI, CIA, and NCTC respectively.[2] The September 26, 2016 Submission also included an explanatory memorandum prepared by the Department of Justice ("DOJ") ("September 26, 2016 Memorandum").

The Court was required to complete its review of the Initial 2016 Certifications within 30 days of their submission, i.e., by October 26, 2016. See 50 U.S.C. § 1881a(i)(1)(B). The Court may extend this period, however, "as necessary for good cause in a manner consistent with national security." See 50 U.S.C. § 1881a(j)(2). The Court has issued two such extensions in these matters.

---

[1](...continued)
targeting procedures for the NSA ("NSA Targeting Procedures") appear as Exhibit A to each of the 2016 Certifications and the March 30, 2017 Submission includes identical amendments to those procedures for each of the certifications. (Unless otherwise specified, references to those targeting procedures shall refer to the procedures as amended, as discussed below, in the March 30, 2017 Submission.) The targeting procedures for the FBI ("FBI Targeting Procedures") appear as Exhibit C to each of the 2016 Certifications and are not amended by the March 30, 2017 Submission.

[2] The minimization procedures for each of the Initial 2016 Certifications are identical. The minimization procedures for the NSA ("NSA Minimization Procedures") appear as Exhibit B to each of the 2016 Certifications and the March 30, 2017 Submission includes identical amendments to those procedures for each of the certifications. (Unless otherwise specified, references to those minimization procedures shall refer to the procedures as amended, as discussed below, in the March 30, 2017 Submission.) The minimization procedures for the FBI ("FBI Minimization Procedures") appear as Exhibit D to each of the 2016 Certifications. The minimization procedures for the CIA ("CIA Minimization Procedures") appear as Exhibit E to each of the 2016 Certifications. The minimization procedures for the NCTC ("NCTC Minimization Procedures") appear as Exhibit G to each of the 2016 Certifications. The minimization procedures for the FBI, CIA, and NCTC are not amended by the March 30, 2017 Submission.

On October 24, 2016, the government orally apprised the Court of significant non-compliance with the NSA's minimization procedures involving queries of data acquired under Section 702 using U.S. person identifiers. The full scope of non-compliant querying practices had not been previously disclosed to the Court. Two days later, on the day the Court otherwise would have had to complete its review of the certifications and procedures, the government made a written submission regarding those compliance problems, see October 26, 2016, Preliminary and Supplemental Notice of Compliance Incidents Regarding the Querying of Section 702-Acquired Data ("October 26, 2016 Notice"), and the Court held a hearing to address them. The government reported that it was working to ascertain the cause(s) of those compliance problems and develop a remedial plan to address them. Without further information about the compliance problems and the government's remedial efforts, the Court was not in a position to assess whether the minimization procedures accompanying the Initial 2016 Certifications, as they would be implemented, would comply with statutory standards and were consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A)-(B). Accordingly, the Court found good cause to extend the time limit for its review of the Initial 2016 Certifications through January 31, 2017, and, based on the government's representations, found that such extension was consistent with national security.[3] See Docket Nos [redacted] Order entered on Oct. 26, 2016 ("October 26, 2016 Order").

[3] By operation of the statute, the predecessors to each of the Initial 2016 Certifications and the procedures accompanying them remained in effect during the extended periods for the Court's consideration of the 2016 Certifications. See 50 U.S.C. § 1881a(i)(3)(A)-(B).

On January 3, 2017, the government made a further submission describing its efforts to ascertain the scope and causes of those compliance problems and discussing potential solutions to them. See January 3, 2017, Supplemental Notice of Compliance Incidents Regarding the Querying of Section 702-Acquired Data ("January 3, 2017 Notice"). The Court was not satisfied that the government had sufficiently ascertained the scope of the compliance problems or developed and implemented adequate solutions for them and communicated a number of questions and concerns to the government. The government submitted another update on January 27, 2017, in which it informed the Court that, due to the complexity of the issues involved, NSA would not be in a position to provide thorough responses to the Court's questions and concerns by January 31, 2017. See January 27, 2017, Letter In re: DNI/AG 702(g) Certifications [redacted] and their Predecessor Certifications ("January 27, 2017 Letter"). The government submitted that a further extension, through May 26, 2017, was necessary for it to address those issues and that such extension would be consistent with national security. The Court granted a shorter extension, through April 28, 2017, for reasons stated in its order approving the extension. See Docket Nos. [redacted] Order entered on Jan. 27, 2017 ("January 27, 2017 Order").

B. The 2017 Amendments

On March 30, 2017, the Attorney General and Director of National Intelligence, acting pursuant to 50 U.S.C. § 1881a(i)(1)(C), executed Amendments to each of the [redacted] Initial 2016 Certifications. See Amendment to [redacted]

[redacted] (collectively, the "2017 Amendments").[4] As discussed below, those amendments substantially change how NSA will conduct certain aspects of Section 702 collection, and largely resolve the compliance problems mentioned above. The March 30, 2017 Submission included the 2017 Amendments, a revised supporting affidavit by the Director of NSA, and revised targeting and minimization procedures for NSA, which replace Exhibits A and B, respectively, to each of the Initial 2016 Certifications. That submission also included an explanatory memorandum prepared by DOJ ("March 30, 2017 Memorandum").

C. Subject Matter of the Certifications

Each of the 2016 Certifications involves "the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information." [redacted]

[4] Unless otherwise stated, subsequent references to the "2016 Certifications" are to the Initial 2016 Certifications and accompanying procedures, as later amended by the 2017 Amendments and the accompanying revised procedures.

[redacted]

Each of the 2016 Certifications generally proposes to continue acquisitions of foreign intelligence information that are now being conducted under the corresponding certification made in 2015 ("the 2015 Certifications"). See September 26, 2016 Memorandum at 2. The 2015 Certifications, which are similarly differentiated by subject matter and [redacted] were approved by the FISC on November 6, 2015.[5] The 2015 Certifications, in turn, generally renewed authorizations to acquire foreign intelligence information under a series of certifications made by the AG and DNI pursuant to Section 702 that dates back to 2008.[6] The government also seeks approval of amendments to the certifications in the Prior 702 Dockets, such that the NSA, CIA, FBI and NCTC henceforward will apply the same minimization

[5] See Docket Nos. [redacted] Memorandum Opinion and Order entered on Nov. 6, 2015 ("November 6, 2015 Opinion"). The Court issued an order on November 9, 2015, approving amendments to prior Section 702 certifications and authorizing the use of revised minimization procedures in connection with those certifications.

[6] See Docket Nos. [redacted] These dockets, together with Docket Numbers [redacted] are collectively referred to as "the Prior 702 Dockets."

procedures to information obtained under prior certifications as they will to information to be obtained under the 2016 Certifications. See September 26, 2016 Memorandum at 2-3; [redacted] This practice, long approved by the FISC, has the advantage of applying a single set of updated procedures to Section 702-acquired information rather than requiring personnel to follow different rules for information acquired on different dates.

D. Review of Compliance Issues

The Court's review of targeting and minimization procedures under Section 702 is not confined to the procedures as written; rather, the Court also examines how the procedures have been and will be implemented. See, e.g., Docket No. [redacted], Memorandum Opinion entered on Apr. 7, 2009, at 22-24 ("April 7, 2009 Opinion"); Docket Nos. [redacted] Memorandum Opinion entered on Aug. 30, 2013, at 6-11 ("August 30, 2013 Opinion"). Accordingly, for purposes of its review of the 2016 Certifications, the Court has examined quarterly compliance reports submitted by the government since the most recent FISC review of Section 702 certifications and procedures was completed on November 6, 2015,[7] as well as individual notices of non-compliance relating to implementation of Section 702. The Court held a hearing on October 4, 2016, to address certain issues raised by the September 26,

[7] See Quarterly Reports to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on December 18, 2015, March 18, 2016, June 17, 2016, September 16, 2016, December 16, 2016 and March 17, 2017. These reports are cited herein in the form "[Date] Compliance Report."

2016 Submission, as well as certain compliance issues regarding the government's collection and handling of information under prior certifications ("October 4, 2016 Hearing").[8] The Court held a further hearing on October 26, 2016, to address matters raised in the October 26, 2016 Notice ("October 26, 2016 Hearing").[9]

II. REVIEW OF CERTIFICATIONS [redacted] AND OF THEIR PREDECESSOR CERTIFICATIONS AS AMENDED BY THE SEPTEMBER 26, 2016 AND MARCH 30, 2017 SUBMISSIONS

The Court must review a certification submitted pursuant to Section 702 "to determine whether [it] contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). The Court's examination of Certifications [redacted] as amended by the 2017 Amendments, confirms that:

> (1) the certifications have been made under oath by the AG and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see [redacted]
>
> (2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see [redacted]
>
> (3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures and minimization procedures;

---

[8] See generally Transcript of Proceedings Held Before the Honorable Rosemary M. Collyer on October 4, 2016 ("October 4, 2016 Transcript").

[9] See generally Transcript of Proceedings Held Before the Honorable Rosemary M. Collyer on October 26, 2016 ("October 26, 2016 Transcript").

(4) each of the certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);[10] and

(5) each of the certifications includes an effective date for the authorization in compliance with 50 U.S.C. § 1881a(g)(2)(D) – specifically, the certifications become effective on April 28, 2017, or on the date upon which this Court issues an order concerning the certifications under Section 1881a(i)(3), whichever is sooner, see [redacted].[11]

The Court therefore finds that [redacted] contain all the required statutory elements. See 50 U.S.C. § 1881a(i)(2)(A).

Similarly, the Court has reviewed the certifications in the Prior 702 Dockets, as amended by the 2016 Certifications, and finds that they also contain all the elements required by the statute. Id.[12]

---

[10] See Affidavits of Admiral Michael S. Rogers, United States Navy, Director, NSA; Affidavits of James B. Comey, Director, FBI; Affidavits of John O. Brennan, Director, CIA; and Affidavits of Nicholas Rasmussen, Director, NCTC, which are appended to each of Certifications [redacted]. Admiral Rogers filed amended affidavits in connection with the March 30, 2017 Submission.

[11] The statement described in 50 U.S.C. § 1881a(g)(2)(E) is not required in this case because there has been no "exigent circumstances" determination under Section 1881a(c)(2).

[12] The effective dates for the amendments to the certifications in the Prior 702 Dockets are the same as the effective dates for the 2016 Certifications. See [redacted]

III. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is also required, pursuant to 50 U.S.C. § 1881a(i)(2)(B) and (C), to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). Pursuant to 50 U.S.C. § 1881a(i)(3)(A), the Court further assesses whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

A. Statutory Standards for Targeting Procedures

Section 1881a(d)(1) requires targeting procedures that are "reasonably designed" to "ensure that any acquisition authorized under [the certification] 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." In addition to these statutory requirements, the government uses the targeting procedures as a means of complying with Section 1881a(b)(3), which provides that acquisitions "may not intentionally target a United States person reasonably believed to be located outside the United States." The FISC considers steps taken pursuant to these procedures to avoid targeting United States persons as relevant to its assessment of whether the procedures are consistent with the requirements of the Fourth Amendment. See Docket No. 702(i)-08-01, Memorandum Opinion entered on Sept. 4, 2008, at 14 ("September 4, 2008 Opinion").

Under the procedures adopted by the government, NSA is the lead agency in making targeting decisions under Section 702. Pursuant to its targeting procedures, NSA may target for

acquisition a particular "selector," which is typically a facility such as a telephone number or e-mail address. The FBI Targeting Procedures come into play in cases where [redacted] that has been tasked under the NSA Targeting Procedures. See FBI Targeting Procedures § I.1. "Thus, the FBI Targeting Procedures apply in addition to the NSA Targeting Procedures, whenever [redacted] acquired." September 4, 2008 Opinion at 20 (emphasis in original). Proposed changes to the existing NSA and FBI targeting procedures are discussed below.

B. Statutory Standards for Minimization Procedures

Section 1881a(e)(1), in turn, requires minimization procedures that "meet the definition of minimization procedures under [50 U.S.C. §] 1801(h) or 1821(4)]." Sections 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;[13]

---

[13] Section 1801(e) defines "foreign intelligence information" as

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> >
> > (B) sabotage, international terrorism, or the international proliferation of

(continued...)

> (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 law enforcement purposes[.]

50 U.S.C. § 1801(h); see also id. § 1821(4).[14] Each agency having access to "raw," or unminimized,[15] information obtained under Section 702 is governed by its own set of

---

[13](...continued)

> weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or a foreign territory that relates to, and if concerning a United States person is necessary to –
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

[14] 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"). For ease of reference, subsequent citations refer only to the definition set forth at Section 1801(h).

[15] This opinion uses the terms "raw" and "unminimized" interchangeably. The proposed NCTC Minimization Procedures define "raw" information as "section 702-acquired information that (i) is in the same or substantially the same format as when NSA or FBI acquired it, or (ii) has been processed only as necessary to render it into a form in which it can be evaluated to

(continued...)

minimization procedures in its handling of Section 702 information. Under Section 1881a(i)(2)(C), the Court must determine whether the agencies' respective minimization procedures meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) or 1821(4), as appropriate.

The most significant changes to the procedures proposed by the government in connection with the 2016 Certifications relate to: (i) the changes in the scope of NSA collection under Section 702, as reflected in the March 30, 2017 Amendments; and (ii) the government's proposal in the September 26, 2016 Submission to allow NCTC access to unminimized information acquired by NSA and FBI [redacted] relating to international terrorism [redacted]. Because those changes cut across several sets of procedures, each is discussed individually in a separate section. This opinion then examines several other changes to various sets of procedures proposed by the government in the September 26, 2016 Submission. The opinion then will assess whether, taken as a whole and including the proposed changes, the proposed targeting and minimization procedures satisfy applicable statutory and Fourth Amendment requirements.

C. Significant Changes to NSA Targeting and Minimization Procedures in the March 30, 2017 Submission

The October 26, 2016 Notice disclosed that an NSA Inspector General (IG) review and report and NSA Office of Compliance for Operations (OCO) verification activities indicated that,

---

[15](...continued)
determine whether it reasonably appears to be foreign intelligence information or to be necessary to understand foreign intelligence information or assess its importance." NCTC Minimization Procedures § A.3.d.

with greater frequency than previously disclosed to the Court, NSA analysts had used U.S.-person identifiers to query the results of Internet "upstream" collection, even though NSA's Section 702 minimization procedures prohibited such queries. To understand why such queries were prohibited, and why this disclosure gave the Court substantial concern, some historical background is necessary.

1. Upstream Collection and the Acquisition of MCTs

"Upstream" collection of Internet communications refers to NSA's interception of such communications as they transit the facilities of an Internet backbone carrier [redacted] as distinguished from acquiring communications from systems operated by Internet service providers [redacted].[16] Upstream Internet collection constitutes a small percentage of NSA's overall collection of Internet communications under Section 702, see, e.g., October 3, 2011 Memorandum Opinion at 23 n.21 (noting that, at that time, upstream Internet collection constituted only 9% of NSA's Internet collection), but it has represented more than its share of the challenges in implementing Section 702.

In 2011, the government disclosed that, as part of its upstream collection of Internet transactions, NSA acquired certain "Multiple Communication Transactions" or "MCTs."[17]

---

[16] See In re DNI/AG 702(g) Certifications [redacted] Memorandum Opinion, October 3, 2011 ("October 3, 2011 Memorandum Opinion"), at 5 n.3. For purposes of the discussion that follows, familiarity with that opinion is presumed. As discussed below, NSA does not share raw upstream collection (Internet or telephony) with any other agency.

[17] NSA's procedures define an Internet transaction as consisting of either a discrete communication (e.g., an individual e-mail) or multiple discrete communications obtained within (continued...)

MCTs might take the form of [redacted] containing multiple e-mail messages [redacted]. See March 30, 2017 Memorandum at 8 n.8. The term "active user" refers to the user of a communication service to or from whom the MCT is in transit when it is acquired (e.g., the user of an e-mail account [redacted] Eventually, as discussed below, a complicated set of minimization rules was adopted for handling different types of MCTs, based on whether the active user was the target[18] and, if not, the nationality and location (to the extent known) of the active user.

Moreover, NSA upstream collection acquired Internet communications that were to, from ***or about*** (i.e., containing a reference to) a selector tasked for acquisition under Section 702. As a result, upstream collection could acquire an entire MCT for which the active user was a non-target and that mostly pertained to non-targets, merely because a ***single*** discrete communication within the MCT was to, from ***or contained a reference to*** a tasked selector. Such acquisitions could take place even if the non-target active user was a U.S. person in the United States and the MCT contained a large number of domestic communications[19] that did not pertain to the foreign

---

[17](...continued)
an MCT. See NSA Targeting Procedures § I, at 2 n.1; NSA Minimization Procedures § 2(g).

[18] With a narrow exception for [redacted] all users of a selector tasked for acquisition under Section 702 are considered targets. See March 30, 2017 Memorandum at 6 n.7.

[19] In this opinion, "domestic communications" are communications in which the sender
(continued...)

intelligence target who used the tasked selector. Because of those types of acquisitions particularly, upstream Internet collection was "more likely than other forms of Section 702 collection to contain information of or concerning United States persons with no foreign intelligence value." November 6, 2015 Opinion at 25 n.21.

It should be noted, however, that not all MCTs in which the active user is a non-target are equally problematic; for example, some MCTs within that description may involve an active user who is a non-U.S. person outside the United States, and for that reason are less likely to contain a large volume of information about U.S. persons or domestic communications.

2. The 2011 Finding of Deficiency and Measures to Remedy the Deficiency

In its October 3, 2011 Memorandum Opinion, the Court found the NSA's minimization procedures, proffered in connection with Section 702 certifications then under consideration, statutorily and constitutionally deficient with respect to their protection of U.S. person information within certain types of MCTs. See October 3, 2011 Memorandum Opinion at 49-80. In response to the Court's deficiency finding, the government submitted amended minimization procedures that placed significant new restrictions on NSA's retention, use, and dissemination of MCTs. Those procedures included a sequestration regime for more problematic categories of MCTs.[20] A shorter retention period was also put into place, whereby an MCT of any type could not be retained longer than two years after the expiration of the certification pursuant to which it

---

[19](...continued)
and all intended recipients are in the United States.

[20] This sequestration regime is discussed in Section IV below in connection with an instance of NSA's not complying with that regime.

was acquired, unless applicable retention criteria were met. And, of greatest relevance to the present discussion, those procedures categorically prohibited NSA analysts from using known U.S.-person identifiers to query the results of upstream Internet collection. In substantial reliance on these and other changes, the Court approved the modified procedures for acquiring and handling MCTs. See In re DNI/AG 702(g) Certifications [redacted] Memorandum Opinion, November 30, 2011 ("November 30, 2011 Memorandum Opinion").

The Court also observed that one category of MCTs presented far fewer statutory and constitutional difficulties than the others:

> [I]f the target is the active user, then it is reasonable to presume that all of the discrete communications within an MCT will be to or from the target. Although United States persons and persons in the United States may be party to any of those communications, NSA' s acquisition of such communications is of less concern than the communications described in the [other] categories [of MCTs] because the communicants were in direct communication with a tasked facility, and the acquisition presumptively serves the foreign intelligence purpose of the collection.

October 3, 2011 Memorandum Opinion at 38. See also id. at 58 n.54 ("The government has also suggested that NSA may have limited capability, at the time of acquisition, to identify some MCTs as to which the "active user" is a tasked selector. To the extent that NSA is able to do so, such acquisitions ***would be consistent with FISA and the Fourth Amendment*** because all discrete communications within this class of MCTs would consist of communications to or from a tasked selector.") (internal citation omitted, emphasis added); id. at 80 (finding that the

proposed NSA procedures, although deficient as applied to other forms of MCTs, were consistent with the statute and the Fourth Amendment as applied to "MCTs as to which the 'active user' is known to be a tasked selector"). That point is significant to the current matters: as discussed below, the 2016 Certifications only authorize acquisition of MCTs when the active user is the target of acquisition.

3. The October 26, 2016 Notice and Hearing

Since 2011, NSA's minimization procedures have prohibited use of U.S.-person identifiers to query the results of upstream Internet collection under Section 702. The October 26, 2016 Notice informed the Court that NSA analysts had been conducting such queries in violation of that prohibition, with much greater frequency than had previously been disclosed to the Court. The Notice described the results of an NSA IG Report which analyzed queries using a set of known U.S.-person identifiers (those associated with targets under Sections 704 and 705(b) of the Act, 50 U.S.C. §§ 1881c and 1881d(b)), during the first three months of 2015, in a subset of particular NSA systems that contain the results of Internet upstream collection. That relatively narrow inquiry found that [redacted] analysts had made [redacted] separate queries using [redacted] U.S.-person identifiers that improperly ran against upstream Internet data. The government reported that the NSA IG and OCO were conducting other reviews covering different time periods, with preliminary results suggesting that the problem was widespread during all periods under review.

At the October 26, 2016 hearing, the Court ascribed the government's failure to disclose those IG and OCO reviews at the October 4, 2016 hearing to an institutional "lack of candor" on NSA's part and emphasized that "this is a very serious Fourth Amendment issue." October 26,

2016 Transcript at 5-6. The Court found that, in light of the recent revelations, it did not have sufficient information to assess whether the proposed minimization procedures accompanying the Initial 2016 Certifications would comply with statutory and Fourth Amendment requirements, as implemented. Based on the government's representation that an extension of time through January 31, 2017, would provide the government sufficient opportunity to assess and report on the scope of the problem and an appropriate remedial plan, and was consistent with the national security, the Court extended the time period for its consideration of the 2016 Certifications to that date.

4. The January 3, 2017 Supplemental Notice and January 27, 2017 Letter

In anticipation of the January 31 deadline, the government updated the Court on these querying issues in the January 3, 2017 Notice. That Notice indicated that the IG's follow-on study (covering the first quarter of 2016) was still ongoing. A separate OCO review, limited in many of the same ways as the IG studies, and covering the periods of April through December 2015 and April through July of 2016, found that some [redacted] improper queries were conducted by [redacted] analysts during those periods.[21] The January 3, 2017 Notice stated that "human error was the primary factor" in these incidents, but also suggested that system design issues contributed. For

[21] NSA further reported that OCO reviewed queries involving a number of identifiers for known U.S. persons who were not targets under Sections 704 or 705(b) of the Act, and which were associated with "certain terrorism-related events that had occurred in the United States." January 3, 2017 Notice at 6. NSA OCO found [redacted] such queries, [redacted] of which improperly ran against Section 702 upstream Internet data. [redacted] of the improper queries were run in a system called [redacted] which NSA analysts use to [redacted] of a current or prospective target of NSA collection, including under Section 702. Id. at 6-7.

example, some systems that are used to query multiple datasets simultaneously required analysts to "opt-out" of querying Section 702 upstream Internet data rather than requiring an affirmative "opt-in," which, in the Court's view, would have been more conducive to compliance. See January 3, 2017 Notice at 5-6. It also appeared that NSA had not yet fully assessed the scope of the problem: the IG and OCO reviews "did not include systems through which queries are conducted of upstream data but that do not interface with NSA's query audit system." Id. at 3 n.6. Although NSD and ODNI undertook to work with NSA to identify other tools and systems in which NSA analysts were able to query upstream data, id., and the government proposed training and technical measures, it was clear to the Court that the issue was not yet fully scoped out.

On January 27, 2017, the government provided further information on the technical and training measures NSA was taking and proposed to take to address this issue. NSA was implementing its technical measures only on systems with respect to the system thought to be used most frequently to query Section 702 data. The government still had not ascertained the full range of systems that might have been used to conduct improper U.S.-person queries. See, e.g., January 27, 2017 Letter at 5 ("NSA is progressing with its efforts to identify other tools or systems that analysts are using to query upstream data."). The government also reported that the NSA IG study for the first quarter of 2016 had found [redacted] improper queries, a substantial

improvement over the first quarter of 2015.[22] But NSA was still working to determine the scope of its U.S.-person query problem and to identify all relevant storage systems and querying tools.

The January 27, 2017 Letter concluded that, "[b]ased on the complexity of the issues, NSA will not be in a position to provide thorough responses [to the Court's questions] on or before January 31, 2017." January 27, 2017 Letter. The government represented that a further extension of the Court's time to consider the 2016 Certifications through May 26, 2017, would be consistent with the national security and would allow the government time to investigate and remedy the problem.

The Court granted an extension only through April 28, 2017.[23] January 27, 2017 Order at 6. In doing so, the Court noted its concern about the extent of non-compliance with "important safeguards for interests protected by the Fourth Amendment." Id. at 5. The Court also observed that, while recent remedial measures appeared promising, they were being implemented only on certain systems, while other systems remained to be assessed. Id. at 5-6.

On March 17, 2017, the government reported that NSA was still attempting to identify all systems that store upstream data and all tools used to query such data, though that effort was nearly complete. March 17, 2017 Compliance Report at 100. NSA had also redoubled training on querying requirements and made technical upgrades to certain commonly-used querying tools

---

[22] In addition to the findings of the IG and OCO reviews, the government identifies improper queries in the course of regular oversight efforts. The government reports those incidents to the Court through individual notices and quarterly reports.

[23] By operation of Section 1881a(i)(1)(B), the government's submission on March 30, 2017, of amendments to the 2016 Certifications and revised procedures started a new 30-day period for Court review, which ends on April 29, 2017.

that were designed to reduce the likelihood of non-compliant queries. Id. at 100-101. Meanwhile, the government continued to report further compliance issues regarding the handling and querying of upstream Internet collection[24] and to investigate potential root causes of non-compliant querying practices. April 7, 2017 Preliminary Notice (Queries) at 4 n.4.

5. The 2017 Amendments

As embodied in the March 30, 2017 Submission, the government has chosen a new course: [redacted]; sequestering and then destroying raw upstream Internet data previously collected; and substantially narrowing the scope of upstream collection [redacted]. Most significantly, the government will eliminate "abouts" collection altogether, which will have the effect of eliminating acquisition of the more problematic types of MCTs. These changes should substantially reduce the acquisition of non-pertinent information concerning U.S. persons pursuant to Section 702.

As of March 17, 2017, NSA had [redacted]. Revisions to the NSA Minimization Procedures now state that all Internet transactions acquired on or before that date and existing in NSA's institutionally managed

---

[24] See April 7, 2017, Preliminary Notice of Compliance Incidents Regarding the Labeling and Querying of Section 702-Acquired Data ("April 7, 2017 Preliminary Notice (Mislabeling)") (nearly [redacted] communications acquired through upstream Internet collection were "incorrectly labeled" as acquired from Internet service providers and, as a result, likely subject to prohibited queries using U.S.-person identifiers); April 7, 2017, Preliminary Notice of Potential Compliance Incidents Regarding Improper Queries ("April 7, 2017 Preliminary Notice (Queries)") (identifying another [redacted] potential violations of prohibition on using U.S.-person identifiers to query Internet upstream collection).

repositories[25] will be sequestered pending destruction such that "NSA personnel will not be able to access the[m] for analytical purposes." March 30, 2017 Memorandum at 4; see NSA Minimization Procedures §3(b)(4)a.

NSA will destroy such sequestered Internet transactions as soon as practicable through an accelerated age-off process. See NSA Minimization Procedures §3(b)(4)a. The government represents that the age-off may take up to one year to complete and verify (with quarterly reports to the Court), and that:

- Pending destruction, sequestered transactions (a) will not be subject to separate age-off or purge processes that otherwise would apply to them, see March 30, 2017 Memorandum at 15-16 & nn. 16-17; and (b) will be available only to NSA technical and compliance personnel for the limited purposes of ensuring the integrity of the systems used to store them and the controls that limit other employees' access to them, see id. at 14 n.13; NSA Minimization Procedures §3(b)(4)a.

- Copies of sequestered transactions will remain in backup and archive systems, not available for use by intelligence analysts, until they age off of those systems in the ordinary course. See March 30, 2017 Memorandum at 14 n.13;

- Sequestered transactions may be retained for litigation purposes as contemplated by Section 3(c)(3) of the NSA Minimization Procedures, subject to prompt notification to the Court. See id. at 16-17 & n.18.

- Certain records derived from upstream Internet communications (many of which have been evaluated and found to meet retention standards) will be retained by NSA, even though the underlying raw Internet transactions from which they are

[25] The March 30, 2017 Submission does not define what an "institutionally managed repository" is. If the government intends not to apply the above-described sequester-and-destroy process to any information acquired on or before March 17, 2017, by Internet upstream collection because the information is not contained in an "institutionally managed repository," it shall describe the relevant circumstances in a written submission to be made no later than June 2, 2017; however, the government need not submit such a description for circumstances referenced in this Opinion and Order as ones in which NSA may retain such information.

derived might be subject to destruction. These records include serialized intelligence reports and evaluated and minimized traffic disseminations; completed transcripts and transcriptions of Internet transactions; [redacted];[26] information used to support Section 702 taskings and FISA applications to this Court; and [redacted]."[27] See March 30, 2017 Memorandum at 20-24.

Finally, upstream collection of Internet transactions [redacted] for communications to or from a targeted person, but "abouts" communications may no longer be acquired. The NSA Targeting Procedures are amended to state that "[a]cquisitions conducted under these procedures will be limited to communications ***to or from*** persons targeted in accordance with these procedures," NSA Targeting Procedures § I, at 2 (emphasis added), and NSA's Minimization Procedures now state that Internet transactions acquired after March 17, 2017, "that are not to or from a person targeted in accordance with NSA's section 702 targeting procedures are unauthorized acquisitions and therefore will be destroyed upon recognition." NSA Minimization Procedures § 3(b)(4)b.[28] Because they are regarded as unauthorized, the government will report any acquisition of such communications to the Court as an incident of non-compliance. See March 30, 2017 Memorandum at 17-18.

---

[26] [redacted] See NSA Targeting Procedures § I at 6.

[27] [redacted] March 30, 2017 Memorandum at 23.

[28] The targeting procedures still require NSA either to use Internet Protocol (IP) filtering of upstream Internet collection to "limit such acquisitions to Internet transactions that originate and/or terminate outside the United States" or [redacted] Id.

Conforming changes are made throughout the NSA Minimization Procedures to remove references to "abouts" collection. Section 3(b)(4) of those procedures, in particular, is significantly revised and streamlined to reflect the narrower scope of authorized collection. For example, detailed procedures previously appearing in Section 3(b)(4) requiring sequestration and special handling of MCTs in especially problematic categories (e.g., those in which the "active user" is a non-target who is in the United States or whose location is unknown) are removed. Because NSA is no longer authorized to acquire those forms of MCTs, if it somehow acquires one, NSA must now destroy it upon recognition.[29]

NSA may continue to acquire MCTs under the amended procedures, but only when it can ensure that the target is a party to the entire MCT or, in other words, when the target is the active user. [redacted]

[29] Internet transactions properly acquired through NSA upstream collection after March 17, 2017, will continue to remain subject to a two-year retention limit, "unless the NSA specifically determines that at least one discrete communication within the Internet transaction meets the retention standards" in the NSA Minimization Procedures. See NSA Minimization Procedures § 3(c)(2). This reflects no change from the current procedures.

[redacted].[30] See March 30, 2017 Memorandum at 10.

It will still be possible, however, for NSA to acquire an MCT that contains a domestic communication. For example, [redacted] If NSA determines that the sender and all intended recipients of a discrete communication within an MCT were located in the United States at the time of that discrete communication, then the entire MCT must be promptly destroyed, see NSA Minimization Procedures § 5, unless the Director makes the required waiver determination for each and every domestic communication contained in the MCT. March 30, 2017 Memorandum at 9 n.9.[31]

U.S.-Person Queries. In light of the elimination of "abouts" communications from Section 702 upstream collection, the government proposes a change to Section 3(b)(5) of the NSA Minimization Procedures that would remove the prohibition on NSA analysts conducting

---

[30] This enumeration is without prejudice to NSA's ability to acquire other types of communications if it can limit acquisition to communications to or from a target as required by the new procedures.

[31] The NSA Minimization Procedures generally take an "all-or-nothing" approach to retention or destruction of MCTs. Thus, an MCT in which ***any*** discrete communication is not to or from a target is also subject to destruction in its entirety. See NSA Minimization Procedures § 3(b)(4)b; March 30, 2017 Memorandum at 13 n.12 ("[I]f for some reason NSA acquires an Internet transaction in which any discrete communication contained therein is not to or from a section 702 target, NSA must destroy such transactions upon recognition.").

queries of Internet upstream data using identifiers of known U.S. persons. Under this proposal, NSA analysts could query upstream data using known U.S. person identifiers, subject to the same requirements that apply to their queries of other Section 702-acquired data. Specifically, any query involving a U.S.-person identifier is subject to NSA internal approval requirements and "require[s] a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information." NSA is required to maintain records of all such determinations and those records are subject to review by NSD and ODNI. See NSA Minimization Procedures § 3(b)(5).[32]

The Court agrees that the removal of "abouts" communications eliminates the types of communications presenting the Court the greatest level of constitutional and statutory concern. As discussed above, the October 3, 2011 Memorandum Opinion (finding the then-proposed NSA Minimization Procedures deficient in their handling of some types of MCTs) noted that MCTs in which the target was the active user, and therefore a party to all of the discrete communications within the MCT, did not present the same statutory and constitutional concerns as other MCTs. The Court is therefore satisfied that queries using U.S.-person identifiers may now be permitted to run against information obtained by the above-described, more limited form of upstream Internet collection, subject to the same restrictions as apply to querying other forms of Section

[32] The Court understands that DOJ and ODNI review all U.S.-person identifiers approved for use in querying contents of Section 702-acquired communications as well as the written documentation of the foreign intelligence justifications for each such query during bi-monthly compliance reviews. See November 6, 2015 Opinion at 25 n.22.

702-acquired data.[33] See generally October 3, 2011 Memorandum Opinion at 22-24 (finding that addition of a provision allowing NSA to query non-upstream Internet transactions using U.S. person identifiers was consistent with the statute and the Fourth Amendment); November 6, 2015 Opinion at 24-26 (after inviting views of amicus curiae on this issue, finding that the CIA and NSA minimization procedures permitting such queries comported with the statute and the Fourth Amendment).

The Court concludes that, taken as a whole, these changes strengthen the basis for finding that the NSA Targeting Procedures meet the requirements of Section 1881a(d)(1) and that the NSA Minimization Procedures meet the definition of such procedures in Section 1801(h). The elimination of "abouts" collection and, consequently, the more problematic forms of MCTs, focuses Section 702 acquisitions more sharply on communications to or from Section 702 targets, who are reasonably believed to be non-U.S. persons outside the United States and expected to receive or communicate foreign intelligence information. That sharper focus should have the effect that U.S. person information acquired under Section 702 will come more

[33] Of course, NSA still needs to take all reasonable and necessary steps to investigate and close out the compliance incidents described in the October 26, 2016 Notice and subsequent submissions relating to the improper use of U.S.-person identifiers to query terms in NSA upstream data. The Court is approving on a going-forward basis, subject to the above-mentioned requirements, use of U.S.-person identifiers to query the results of a narrower form of Internet upstream collection. That approval, and the reasoning that supports it, by no means suggest that the Court approves or excuses violations that occurred under the prior procedures.

predominantly from non-domestic communications that are relevant to the foreign intelligence needs on which the pertinent targeting decisions were based.[34]

D. NCTC Raw Take Sharing

1. Sharing of Unminimized Information Acquired Under [redacted] with NCTC

The September 26, 2016 Submission proposes for the first time to allow NCTC access to unminimized information acquired by NSA and FBI pursuant to [redacted] Previously, NCTC only had access to minimized Section 702-acquired information residing in FBI's general indices and relating to certain categories of investigations concerning international terrorism. NCTC has not, and will not under the government's proposal, engage in FISA collection of its own. It does, however, have significant experience with handling FISA-acquired information, including unminimized information obtained pursuant to Titles I and III and Sections 704 and 705(b) of the Act, pursuant to AG- and FISC-approved minimization procedures.

Beginning in 2008, NCTC was authorized to receive certain FISA-derived information from terrorism cases that FBI had uploaded into its Automated Case Support ("ACS") system. FISA information residing in ACS has been minimized by FBI and appears in investigative

---

[34] When the Court approved the prior, broader form of upstream collection in 2011, it did so partly in reliance on the government's assertion that, due to [redacted] some communications of foreign intelligence interest could only be acquired by such means. See October 3, 2011 Memorandum Opinion at 31 & n. 27, 43, 57-58. This Opinion and Order does not question the propriety of acquiring "abouts" communications and MCTs as approved by the Court since 2011, subject to the rigorous safeguards imposed on such acquisitions. The concerns raised in the current matters stem from NSA's failure to adhere fully to those safeguards.

reports and other work product. The FISC in 2008 found that NCTC's access to such information in ACS was "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information" under 50 U.S.C. § 1801(h)(1). Docket No. [redacted], Memorandum Opinion and Order entered on Oct. 8, 2008, at 3-6. Later, in 2012, NCTC was granted access to raw information from terrorism cases obtained under Titles I and III and Sections 704 and 705(b) of the Act, subject to expanded minimization procedures. See Docket Nos. [redacted], Memorandum Opinion and Order entered on May 18, 2012 ("May 18, 2012 Opinion").

NCTC also has experience handling information obtained under Section 702 of the Act. Since 2012, NCTC has had access to minimized information obtained under Section 702 through its access to certain case categories in FBI's general indices (including ACS and another system known as Sentinel). See Docket Nos. [redacted], Memorandum Opinion entered on Sept. 20, 2012, at 22-25 ("September 20, 2012 Opinion").

In each instance in which the FISC has authorized expanded sharing of FISA-acquired information with NCTC, the FISC has recognized NCTC's role as the government's primary organization for analyzing and integrating all intelligence pertaining to international terrorism and counterterrorism. For example, in approving NCTC's access to minimized Section 702-acquired information in FBI general indices in 2012, the FISC observed that NCTC was statutorily charged with ensuring that intelligence agencies receive all-source intelligence support and that executive and legislative branch officials have access to international terrorism-related intelligence information and analysis to meet their constitutional responsibilities. See id. at 23

(citing then-applicable statutory provisions); see also Affidavits of Nicholas Rasmussen, Director, NCTC, appended at Tab 5 to each of the 2016 Certifications, at 1. The government further avers in support of the current proposal that: (1) NCTC is statutorily charged with providing "strategic operational plans for the civilian and military counterterrorism intelligence and operations across agency boundaries, both inside and outside the United States;" and (2) the NCTC Director "is assigned 'primary responsibility within the United States Government for conducting net assessments of terrorist threats.'" September 26, 2016 Memorandum at 12-13 (citing 50 U.S.C. § 3056(f)(1)(B) and (G)).

The Court is satisfied that NCTC's receipt of information acquired under [redacted] is consistent with its mission. As for the NCTC's need to have access to this information in raw form, the government asserts that NCTC's ability to obtain Section 702-acquired information more quickly and in a form closer to its original, and to examine that information in NCTC systems, using its own analytical tools in the context of potentially related information available in NCTC systems, will enhance NCTC's ability to produce counterterrorism foreign intelligence information. See September 26, 2016 Memorandum at 13-14. The government provides an example in which NCTC was able to use its access to raw FISA-acquired information from collection under other provisions of FISA to provide a timely and unique assessment that was shared with other elements of the Intelligence Community in support of their intelligence collection and analysis functions. See id. at 15. One would hope that this is one of many such examples.

In any event, as noted above, the government's proffered rationale for sharing raw information with NCTC was accepted by the FISC in the context of information obtained under other provisions of the Act, and the Court is persuaded that it applies with equal force in the context of collection under Section 702. Among other things, the volume of collection under Section 702 militates in favor of bringing all available analytical resources to bear on the careful analysis and exploitation of foreign intelligence information from such collection. The Court also credits the assertion that time can be of the essence in many rapidly-unfolding counterterrorism investigations. The Court is persuaded that timely access to raw Section 702-acquired information will enhance NCTC's ability to perform its distinct mission, to support the activities of other elements of the Intelligence Community, and to provide valuable input to senior decisionmakers in the Executive Branch and Congress.

Moreover, the information acquired under [redacted] though voluminous – is the result of targeting persons reasonably believed to be non-United States persons located outside the United States. For that reason, it is unlikely to contain as high a proportion of information concerning United States persons as information acquired by FISA electronic surveillance and physical search, which often involve targets who are United States persons and typically are directed at persons in the United States.

To be sure, information concerning unconsenting United States persons has been and will continue to be acquired under Section 702 and [redacted] particularly. The minimization procedures must carefully regulate the government's use and dissemination of such U.S. person information in order to satisfy the definition of "minimization

procedures" at Section 1801(h). The procedures NCTC will be required to follow with respect to its handling of such information are examined in detail below.

The Court also finds that the scope of the proposed sharing with NCTC is appropriate. Consistent with NCTC's mission, the proposed sharing of unminimized Section 702-acquired information is limited to [redacted] The government notes that the sharing will not include telephony data or the results of upstream Internet collection; in other words, it will be limited to Internet communications obtained with the assistance of the direct providers of the communication services involved. See September 26, 2016 Memorandum at 10-11. NCTC will receive raw information [redacted] and subject to the same limitations as CIA (no upstream Internet collection and no telephony). Id.

The government undertakes to notify the Court before altering these arrangements and providing raw telephony or upstream Internet data to NCTC, FBI or CIA. See id. at 11 n.7; accord March 30, 2017 Memorandum at 9-10 n.10. With regard to upstream Internet collection, the Court has determined that mere notification to the FISC would be insufficient, especially as NSA is in the process of transitioning to a narrower form of collection and segregating and destroying the results of the prior, broader collection. Accordingly, the Court is ordering that raw information obtained by NSA's upstream Internet collection under Section 702 shall not be provided to FBI, CIA or NCTC unless it is done pursuant to revised minimization procedures that are adopted by the AG and DNI and submitted to the FISC for review in conformance with Section 702.

With that limitation, the Court finds that NCTC's receipt of raw information acquired under [redacted] subject to appropriate minimization procedures as described below, will "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." 50 U.S.C. § 1801(h)(1).[35] The NCTC has followed AG- and FISC-approved minimization procedures in connection with its prior receipt of FISA-acquired information, including Section 702-acquired information, with relatively few documented instances of noncompliance. See generally Docket Nos. [redacted], Memorandum Opinion and Order entered on Aug. 26, 2014 Opinion ("August 26, 2014 Opinion") at 37 (noting that "no significant compliance issues have arisen under [NCTC's Section 702 minimization] procedures").

a. Changes to FBI and NSA Procedures Relating to Raw Information Sharing with NCTC

As noted above, the extension of raw information sharing to NCTC requires changes to several sets of procedures.[36] First, FBI's targeting procedures, and FBI and NSA's minimization procedures, are each amended to reflect the fact that those agencies may now provide to NCTC

[35] With regard to § 1801(h)(2)'s limitation on the dissemination of United States person identities, the Court adopts the analysis set out at pages 7-8 of the May 18, 2012 Opinion.

[36] Some technical, conforming edits to the certifications and procedures occasioned by the extension of raw information sharing to NCTC are not discussed herein because they raise no issues material to the Court's review. Certain other changes to the proposed certifications and procedures are not discussed for the same reason.

unminimized communications obtained under [redacted] See FBI Targeting Procedures § I.6; NSA Minimization Procedures § 6(c)(3); FBI Minimization Procedures § V.E. NCTC is required to identify to NSA those individual Section 702 selectors for which it wishes to receive unminimized information, and is required to apply its own approved minimization procedures to such information. See NSA Minimization Procedures § 6(c)(3); FBI Minimization Procedures § V.E.

b. Changes to NCTC Minimization Procedures Relating to Raw Information Sharing with NCTC

The NCTC Minimization Procedures have been enhanced significantly to account for its receiving raw information under Section 702. But they are not crafted out of whole cloth. They are modeled on the previously-approved minimization procedures that apply to NCTC's receipt of information under Titles I and III and Sections 704 and 705(b) of the Act.[37] Modifications are proposed to address issues that are unique to Section 702 collection and in some instances to harmonize the proposed NCTC procedures with those used by the FBI, NSA, and CIA in their handling of Section 702-acquired information. Several key elements of the NCTC Minimization Procedures are discussed below, focusing on instances in which they depart from the previously approved NCTC Title I Procedures.[38]

---

[37] For ease of reference, this opinion refers to these procedures (the "National Counterterrorism Center Standard Minimization Procedures for Information Acquired by the Federal Bureau of Investigation Pursuant to Title I, Title III, or Section 704 or 705(b) of the Foreign Intelligence Surveillance Act") as the "NCTC Title I Procedures."

[38] The government does not propose targeting procedures for NCTC, so NCTC will not be authorized to engage in any Section 702 collection.

The NCTC Minimization Procedures do not have a provision restricting NCTC's processing, retention, and dissemination of third-party information. In NCTC's Title I Procedures, third-party information is defined to include "communications of individuals who are not the targets of the collection," and to exclude "any information contained in a communication to which the target is a party." NCTC Title I Procedures § A.3.h. Third-party information thus defined is subject to stricter retention, processing, and dissemination limitations under NCTC's Title I Procedures than information directly involving the target. See id. § C.4. In 2012, the FBI removed similar third-party information provisions from its Section 702 minimization procedures. In approving that change, the Court explained that in the context of Section 702 collection such rules

> have no practical effect because the term "target" is defined as "the user(s) of a targeted selector." In light of that definition . . . there are no "third party" communications [in Section 702 collection] for the FBI to minimize. Because the deletion of the provisions regarding third party communications does not alter the manner in which the FBI acquires, retains, or disseminates Section 702 information, this change is not problematic under Section 1801(h).

September 20, 2012 Opinion at 17-18 (internal citations omitted). For the same reason, the omission of provisions present in NCTC's Title I Procedures governing the NCTC's retention, processing, and dissemination of third-party information from its Section 702 minimization procedures presents no impediment to their approval.

Exclusion and Departure Provisions. The NCTC Minimization Procedures contain certain exclusions and departure provisions that are consistent with the NCTC Title I Procedures with two notable exceptions:

(1) An exclusion is added for the performance of lawful oversight functions of NSD, ODNI, relevant Inspectors General, and NCTC itself, which is consistent with parallel provisions in other agencies' procedures. See NCTC Minimization Procedures § A.6.e; NSA Minimization Procedures § 1; FBI Minimization Procedures § I.G; CIA Minimization Procedures § 6(f); and

(2) A separate exclusion addresses compliance with congressional and judicial mandates. NCTC Minimization Procedures § A.6.d.

The latter provision was amended across all the agencies' minimization procedures in the September 26, 2016 Submission and is the subject of separate discussion below.

U.S. Person Presumptions. In general, the procedures provide a rebuttable presumption that persons known to be in the United States are United States persons, and those known or reasonably believed to be outside the United States are non-United States persons. Id. § A.4.a and b. The NCTC Minimization Procedures diverge slightly from their Title I counterpart with respect to individuals whose locations are not known. [redacted] NCTC Title I Procedures § A.4.a. That approach makes sense in those procedures, which apply to information predominantly obtained by electronic surveillance and physical search – [redacted] – directed at persons in the United States. [redacted] Id. §

A.4.c. [redacted] NCTC Minimization Procedures §A.4.e.

The Court assesses that Section 702 collection is more analogous to [redacted] than it is to other forms of collection that are regulated by the NCTC Title I Procedures and that the application of the [redacted] is appropriate in this context. Section 702 collection focuses exclusively on electronic data and communications collected with the assistance of electronic communication service providers, and its targets are reasonably believed to be non-U.S. persons located overseas. The presumption of non-U.S. person status for a communicant whose location is not known is also consistent with the presumptions allowed under the FBI and NSA's current and proposed Section 702 minimization procedures. See NSA Minimization Procedures § 2(k)(2); FBI Minimization Procedures § I.D. The Court finds the same framework reasonable as applied to NCTC's handling of Section 702 information and consistent with the requirements of Section 1801(h). See September 20, 2012 Opinion at 15-16 (approving parallel change to FBI Section 702 Minimization Procedures).[39]

Retention. The NCTC Minimization Procedures impose a retention schedule and framework that are consistent with those followed by FBI for Section 702-acquired information

[39] The NCTC Minimization Procedures also include provisions regarding unincorporated associations and aliens who have been admitted for lawful permanent residence (NCTC Minimization Procedures § A.4.c and d) that track current provisions in the NSA Minimization Procedures (§ 2(k)(3) and (4)). The Court sees no issue with these provisions.

and, with a few immaterial exceptions not warranting separate discussion, with corresponding provisions of the NCTC Title I Procedures. In brief, information that the NCTC retains on an electronic and data storage system, but has not reviewed, generally must be destroyed after five years from the expiration date of the certification authorizing the collection. NCTC Minimization Procedures § B.2.a. Information retained on such systems that has been reviewed, but not identified as information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime is generally subject to special access controls after ten years from such expiration date, and shall be destroyed after fifteen years from such date. Id. § B.2.b.[40]

In one respect, the proposed NCTC Minimization Procedures are more restrictive than the NCTC Title I Procedures: Unlike the NCTC Title I Procedures, the NCTC Minimization Procedures expressly provide that the prescribed time limits for retention apply to metadata repositories. NCTC Minimization Procedures § C.3; see October 4, 2016 Transcript at 7. They further require appropriate training and access controls for NCTC employees granted access to Section 702-acquired information. NCTC Minimization Procedures §§ B.1, F.1, F.2 and F.3. They also require that such information be maintained in secure systems that enable NCTC to mark or otherwise identify communications that meet the standards for retention. Id. Consistent with the procedures followed by other agencies, the NCTC Minimization Procedures require

[40] Generally speaking, information identified as meeting one of those criteria is not subject to the above-described temporal limitations on retention. Id. § B.3. See, however, the discussion on page 46 below regarding limitations on retention and use of evidence of a crime that is not foreign intelligence information.

destruction of information obtained under a reasonable, but mistaken, belief that the target was appropriate for Section 702 collection, subject to limited waiver provisions. Id. § B.4. Finally, they include provisions for retention of information reasonably believed to be necessary for, or potentially discoverable in, administrative, civil or criminal litigation. Id. § B.5. Analogous provisions already appear in NSA's and CIA's Minimization Procedures. See NSA Minimization Procedures § 3(c)(4); CIA Minimization Procedures § 11.

Processing. The NCTC Minimization Procedures set standards for queries of data obtained under Section 702, including requiring written justifications for queries using U.S. person identifiers that are subject to subsequent review and oversight by NSD and ODNI. NCTC Minimization Procedures § C.1; see also id. § C.3 (metadata queries "must be reasonably likely to return foreign intelligence information"). They apply heightened handling requirements to sensitive information and privileged communications. The provisions for sensitive information are essentially identical to those found in the NCTC Title I Procedures. Compare NCTC Minimization Procedures § C.4 with NCTC Title I Procedures § C.5.

The proposed procedures for NCTC's handling of privileged communications obtained under Section 702 closely track those found in NSA's and CIA's Section 702 minimization procedures. Compare NCTC Minimization Procedures § C.5 with NSA Minimization Procedures § 4; CIA Minimization Procedures § 7. The NCTC Minimization Procedures require, among other things, the destruction of attorney-client communications that are affirmatively determined not to contain foreign intelligence information or evidence of a crime. See NCTC Minimization Procedures § C.5.a. If an attorney-client communication appears to contain foreign

intelligence information or evidence of a crime, [redacted] See id. § C.5.b, c, and e. Communications containing privileged information will be segregated when such information pertains to a criminal charge in the United States, [redacted] See id. § C.5.c, d, e, and f. [redacted] See id. § C.5.i. [redacted] See id. § C.5.g and h.

The Court closely examined substantial revisions to the NSA and CIA procedures as they relate to privileged communications in 2015, and found that they "serve to enhance the protection of privileged information" and "present no concern under Section 1801(h)." See November 6, 2015 Opinion at 18. The Court now finds the same to be true with respect to the NCTC Minimization Procedures.

Dissemination. The dissemination provisions of the NCTC Minimization Procedures (§ D) provide for disseminations in a manner consistent with CIA's and NSA's handling of Section 702-acquired information. They also track in all material respects the NCTC Title I Procedures, which have been found to satisfy Section 1801(h).

Handling of Information in FBI General Indices. The NCTC Minimization Procedures, like the NCTC Title I Procedures, include a separate section that addresses NCTC's handling of minimized Section 702 information made available to it through FBI's general indices. This provision of the NCTC Minimization Procedures tracks the corresponding provision of the NCTC Title I Procedures. Compare NCTC Minimization Procedures § E with NCTC Title I Procedures § E. The government points out that the description of individuals who are expected to be allowed access to information in such systems ("NCTC personnel") is meant to be broader than the defined term "NCTC employees" that is used in all other instances throughout the proposed NCTC Minimization Procedures. The government explains that the broader term "NCTC personnel" is meant to encompass (in addition to the NCTC employees, detailees, and contractors who would qualify as "NCTC employees" as defined in the proposed procedures, see NCTC Minimization Procedures § A.3.b) NCTC assignees from other agencies. The government explains that, consistent with the current NCTC Section 702 minimization procedures, such assignees will continue to have access to minimized information in FBI general indices but will not be allowed to access raw Section 702-acquired information. September 26, 2016 Memorandum at 15 n.9. The Court assesses that is a sensible distinction.

Two Additional Issues. Two particular provisions in the agencies' proposed minimization procedures relating to NCTC represent departures from current practice under Section 702 and merit separate discussion. Those provisions pertain to NCTC's retention of evidence of a crime and receipt of information from FBI and NSA for collection avoidance purposes.

NCTC's Retention of Evidence of Crime. The predecessor procedures that regulated NCTC's retention, use, and dissemination of minimized Section 702 information obtained through FBI's general indices acknowledged that some of the information made available to NCTC might constitute evidence of a crime, but not foreign intelligence information or information necessary to understand such information or assess its importance. As a law enforcement agency, FBI would have a reason to maintain such information in its general indices, where NCTC employees might encounter it. NCTC, as a non-law-enforcement agency, was precluded under its previous Section 702 minimization procedures from retaining (in its own systems), using or disseminating such information. By contrast, under the new NCTC Minimization Procedures (and only with respect to information it receives in raw form),[41] NCTC may retain and disseminate evidence of a crime for law enforcement purposes. *See* NCTC Minimization Procedures §§ A.7, D.2. This proposed approach is consistent with Sections A.7 and D.2 of the NCTC Title I Procedures.

The government asserts that, under the proposed NCTC Minimization Procedures, NCTC might review raw information that has not been, and may never be, reviewed by any other agency. As such, the government posits, NCTC must disseminate evidence of a crime to meet its "crime reporting obligations" under Executive Order 12333 and other applicable law. See

---

[41] As noted above, the new NCTC Minimization Procedures incorporate (in Section E) the rules currently governing NCTC's retention, use, and dissemination of minimized information that it obtains through FBI's general indices. NCTC continues to be prohibited from retaining, using or disseminating information it obtains from those indices that constitutes evidence of a crime, but not foreign intelligence information, with anyone, including law enforcement, for reasons explained below. See NCTC Minimization Procedures § E.2

September 26, 2016 Memorandum at 16-17. Under NCTC's minimization procedures as now in effect, NCTC only has access to information from FBI indices that has already been reviewed and minimized by FBI, so it is presumed that FBI would have taken all necessary steps with respect to actionable law enforcement information. Under that construct, NCTC could, as required by its procedures, simply disregard and delete that information from its holdings (unless there was a foreign intelligence reason for NCTC to retain it). The government asserts that the same would not be true with respect to raw information passed to NCTC. See id.

It is less readily apparent, however, why NCTC would need to retain evidence of a crime after it has been passed to a law enforcement agency. The government asserts that NCTC needs to preserve original copies of the relevant information in order to be able to respond to potential follow-on requests for information or assistance from law enforcement. See October 4, 2016 Transcript at 4-6.[42] In other words, NCTC would have no reason to retain the information for its own purposes, but it would have a need for retention that derives from the needs of the law enforcement agency to which NCTC passed the information. The government further posits that NCTC may be the only agency that retains a copy of the relevant information and thus may be the only entity able to respond to follow-up requests from law enforcement. See October 4, 2016 Transcript at 5.

[42] The government correctly points out that in its opinion approving the NCTC's Title I Procedures, which contain identical provisions with respect to crime reporting and evidence of a crime, the Court found that those provisions met the statutory definition of minimization procedures in Section 1801(h)(3), which prescribes 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 law enforcement purposes." See September 26, 2016 Memorandum at 16 n.10.

The Court credits the government's explanation of NCTC's derivative need to retain such information for law enforcement purposes. It bears emphasis, however, that NCTC may retain and disseminate evidence of a crime that is not foreign intelligence information or necessary to understand foreign intelligence information or assess its importance and otherwise would be subject to destruction under the generally applicable age-off schedule, see NCTC Minimization Procedures § B.2, only in furtherance of those law enforcement purposes. See id. § D.2. The Court understands and expects that NCTC will only retain such information – including after it has been disseminated in compliance with crime reporting obligations, see id. § A.7 – for so long as is reasonably necessary to respond to law enforcement requests of the kind posited by the government. In the interim, NCTC shall make no independent use of such information. The Court directs the government to take steps to ensure that NCTC abides by these limitations and that any failures to do so are appropriately identified and reported to the FISC.

Collection Avoidance. The FBI and NSA would also be allowed, under proposed amendments to their respective procedures, to share with NCTC for "collection avoidance" purposes information about domestic communications obtained under Section 702 that indicate that a targeted person is in the United States or otherwise should no longer be targeted under Section 702. See NSA Minimization Procedures § 5; FBI Minimization Procedures § III.A. These provisions now allow sharing of such information among FBI, NSA, and CIA. At first it was not clear to the Court why this provision should be extended to include NCTC, given that NCTC engages in no independent collection under Section 702, or, so far as the Court is aware, under any other authorities. [redacted]

[redacted] Indeed, it seemed counterintuitive to the Court that an agency not engaged in collection would need to receive information, otherwise subject to destruction, for "collection avoidance purposes."

The government's response is that NCTC, upon receipt of such information, might be in a position to "connect the dots" and identify other individuals who might not be viable targets for Section 702 collection (or perhaps other facilities that might be used by the same individual and should not be targeted). See September 26, 2016 Memorandum at 17-18. Such information would also put NCTC on notice that the selector, or related selectors, might not be viable for nomination to be targeted for collection by other agencies. Id. The government adds that FBI and NSA typically only share the minimum information necessary for collection avoidance purposes, such as technical information from the relevant communication or a mere notification that the communication triggered a flag regarding the propriety of targeting someone. Id.

Because the government offers a plausible explanation of the need for sharing such information with NCTC, the Court is prepared to approve the provisions in question, with the understanding that NCTC may not use or disclose this information except as needed for collection avoidance purposes.[43]

Subject to the above-described understandings, the Court finds that the proposed minimization procedures for NCTC's handling of raw information acquired under [redacted]

[43] NSA's procedures, for example, require that a domestic communication retained for collection avoidance purposes be placed on the NSA's "Master Purge List" ("MPL"), which prevents further analytical use or dissemination of the communication for any other reason. See NSA Minimization Procedures § 5.

[redacted], and the modifications to the other agencies' procedures relating to NCTC's receipt of such information, are reasonable. The NCTC Minimization Procedures address retention, use, and dissemination of Section 702-acquired information in ways that are consistent with logical analogues. Indeed, the FISC has approved all the major elements of those procedures in the context of other FISA minimization procedures, and the Court finds that, taken as a whole and as applied to raw information acquired under [redacted], the NCTC Minimization Procedures conform to 50 U.S.C. § 1801(h).

E. Other Changes to Targeting and Minimization Procedures in the September 26, 2016 Submission

1. Changes to FBI Minimization Procedures Permitting the Retention of Section 702-Acquired Information Subject to Preservation Obligations Arising from Litigation

In 2014, the FISC approved provisions permitting FBI, NSA, and CIA to retain Section 702-acquired information subject to specific preservation obligations arising in litigation concerning the lawfulness of Section 702. See August 26, 2014 Opinion at 21-25. Under those provisions, information otherwise subject to destruction under the agencies' respective minimization procedures would nonetheless be retained to satisfy litigation preservation obligations. Access to information retained under those provisions is tightly restricted. See id. at 21, 23.

The NSA and CIA minimization procedures accompanying the 2015 Certifications included revisions to these "litigation hold" provisions. Among other things, those procedures included new provisions whereby NSA and CIA may retain for litigation purposes Section 702-

acquired information otherwise subject to destruction requirements that are not set forth in the minimization procedures, provided that access to such information is strictly controlled as prescribed in the procedures.[44] The government must promptly notify the Court and seek its approval whenever this provision is invoked. See NSA Minimization Procedures § 3(c)(4)b; CIA Minimization Procedures § 11.b.

The litigation hold provisions also require NSA and CIA to provide DOJ with a summary of all litigation matters requiring preservation of Section 702-acquired information, a description of the Section 702-acquired information being retained, and, if possible based on the information available to the agencies, the status of each litigation matter. See NSA Minimization Procedures § 3(c)(4)a and b; CIA Minimization Procedures § 11.a and b.[45] The FISC, in considering the 2015 Certifications, appointed amicus curiae to help it evaluate these litigation hold provisions. The FISC agreed with the amicus's assessment that the revised litigation hold provisions "comport with the requirements of Section 1801(h) and strike a reasonable and appropriate

[44] As stated in the November 6, 2015 Opinion, the Court understands this provision to apply to destruction requirements arising under a FISC order, a FISC rule, or other FISC-approved procedures – e.g., the requirement that NSA destroy any communication acquired through the intentional targeting of a person reasonably believed to be a United States person or to be located in the United States, see NSA Targeting Procedures § IV.

[45] The FISC has ordered the government to submit a report at the end of each year identifying matters in which FBI, NSA or CIA is retaining Section 702-acquired information that would otherwise be subject to destruction in order to satisfy a litigation preservation obligation. See August 26, 2014 Opinion at 42. The Court has reviewed the litigation hold reports filed by the government in December 2015 and December 2016. The Court is reaffirming that reporting obligation and extending it to NCTC.

balance between the retention limitations reflected in FISA and the government's need to comply with its litigation-related obligations." November 6, 2015 Opinion at 16.

The proposed NCTC Minimization Procedures, like NSA's and CIA's, include litigation hold provisions that address departures from destruction requirements arising under NCTC's minimization procedures and from other sources. See NCTC Minimization Procedures § B.5. The government proposes now to expand the FBI Minimization Procedures to address the latter situation and to bring FBI's litigation hold provisions more closely into line with those of the other agencies. [redacted] In 2015, with the concurrence of a FISC-appointed amicus curiae, the FISC found these procedures appropriate as applied to NSA and CIA. November 6, 2015 Opinion at 16. The Court sees no basis for a contrary conclusion now with regard to the NCTC and FBI.

The Court emphasizes, however, the need promptly to notify and seek leave of the Court to retain information pursuant to such provisions. [redacted]

[redacted]

~~at~~ 2-3. The Court will not look favorably on similarly lengthy delays in deciding whether to comply with an otherwise applicable destruction requirement or seek FISC approval to retain information in anticipation of bringing criminal charges.

2. Clarification of Age-off Requirements for Encrypted Information Under the FBI Minimization Procedures

In its 2015 Submission, the government added a new provision to the FBI Minimization Procedures permitting the FBI to retain Section 702-acquired information that is encrypted or believed to contain secret meaning for any period of time during which such material is subject to, or of use in, cryptanalysis or otherwise deciphering secret meaning. Access to such information is restricted to FBI personnel engaged in cryptanalysis or deciphering secret meaning. See FBI Minimization Procedures § III.G.5. Nonpublicly available information concerning unconsenting United States persons retained under the provision cannot be used for any other purpose unless such use is permitted under a different provision of the minimization procedures. See id. Once information retained under this provision is decrypted or its secret meaning is ascertained, the generally-applicable retention rules apply. The government stated that it would calculate the age-off date for such information from the later of the date of decryption or the date of expiration of the certification pursuant to which the information was

acquired. See Docket Nos. [redacted] July 15, 2015, Memorandum Regarding Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request For an Order Approving Such Certifications and Amended Certifications at 18. But the procedures themselves were silent on this point.

When it approved the 2015 Certifications, the FISC encouraged the government to make this calculation methodology explicit in future versions of the procedures. November 6, 2015 Opinion at 20 n.19. The government has done so. The FBI Minimization Procedures now [redacted]

3. Revisions to Minimization Provisions Permitting Compliance with Judicial or Legislative Mandates

The NSA and CIA minimization procedures approved in the November 6, 2015 Opinion each state that "[n]othing in these procedures shall prohibit the retention, processing, or dissemination of information reasonably necessary to comply with specific constitutional, judicial, or legislative mandates." See November 6, 2015 Opinion at 21 (citing relevant provisions of procedures). The FISC took issue with the facial breadth of these provisions,

observing that "[a] provision that would allow the NSA and CIA to deviate from any of the[] restrictions [in their respective minimization procedures] based upon unspecified 'mandates' could undermine the Court's ability to find that the procedures satisfy" statutory requirements. Id. at 22. The FISC addressed this issue in three ways. First, in order to avoid finding a deficiency in the procedures, it applied an interpretive gloss that the government had previously articulated with regard to similar language in another set of minimization procedures, to the effect that such provisions would be invoked sparingly and applied only to directives specifically calling for the information at issue, and not to Executive Branch orders or directives. Id. at 22. The FISC emphasized that it "must construe the phrase 'specific constitutional, judicial, or legislative mandates' to include only those mandates containing language that clearly and specifically requires action in contravention of an otherwise-applicable provision of the requirement of the minimization procedures." Id. at 23. Second, to ensure that these provisions were actually applied in a manner consistent with the FISC's understanding, the government was directed to report any action in reliance on this provision to the FISC promptly and in writing, along with a written justification for each such action. Id. at 23-24.[46] Finally, the government was encouraged to consider replacing these broadly-worded provisions with language more narrowly tailored to the above-described intent. Id. at 24 n.20.

The government proffered revisions to these provisions in the September 26, 2016 Submission. The provisions, as revised and incorporated in all of the agencies' minimization

[46] This reporting requirement is carried forward by this Opinion and Order. The Court understands that this provision has not yet been invoked.

procedures, now require that the departure be "necessary to comply with a specific congressional mandate or order of a court within the United States." NSA Minimization Procedures § 1; FBI Minimization Procedures § I.G; CIA Minimization Procedures § 6.g; NCTC Minimization Procedures § A.6.d. The Court finds the revised language acceptable, but again wishes to emphasize that it expects this provision to be interpreted narrowly.

As described in the September 26, 2016 Memorandum at 6-7, the government has received requests from members of Congress, including 14 members of the House Judiciary Committee, for estimates of the number of communications of U.S. persons that have been acquired under Section 702. Responding to such requests would require NSA, and possibly other agencies, to structure queries designed to elicit information concerning U.S. persons with no foreign intelligence purpose, facially in violation of applicable minimization procedures. Such requests, which have not taken the form of a subpoena or other legal process, would not constitute legal mandates for purposes of the departure provision discussed above. Instead, the government submits that, in order to respond to such requests, it may take actions that contravene otherwise applicable minimization requirements pursuant to provisions of the minimization procedures that allow for performance of lawful oversight functions. For example, the NSA Minimization Procedures state that nothing in them shall restrict "NSA's performance of lawful oversight functions of its personnel or systems, or lawful oversight functions" of NSD, ODNI, or relevant Inspectors General. NSA Minimization Procedures § 1; see also FBI Minimization Procedures § I.G (same); CIA Minimization Procedures § 6.f (same); NCTC Minimization Procedures § A.6.e (same). The government also undertook to notify the Court

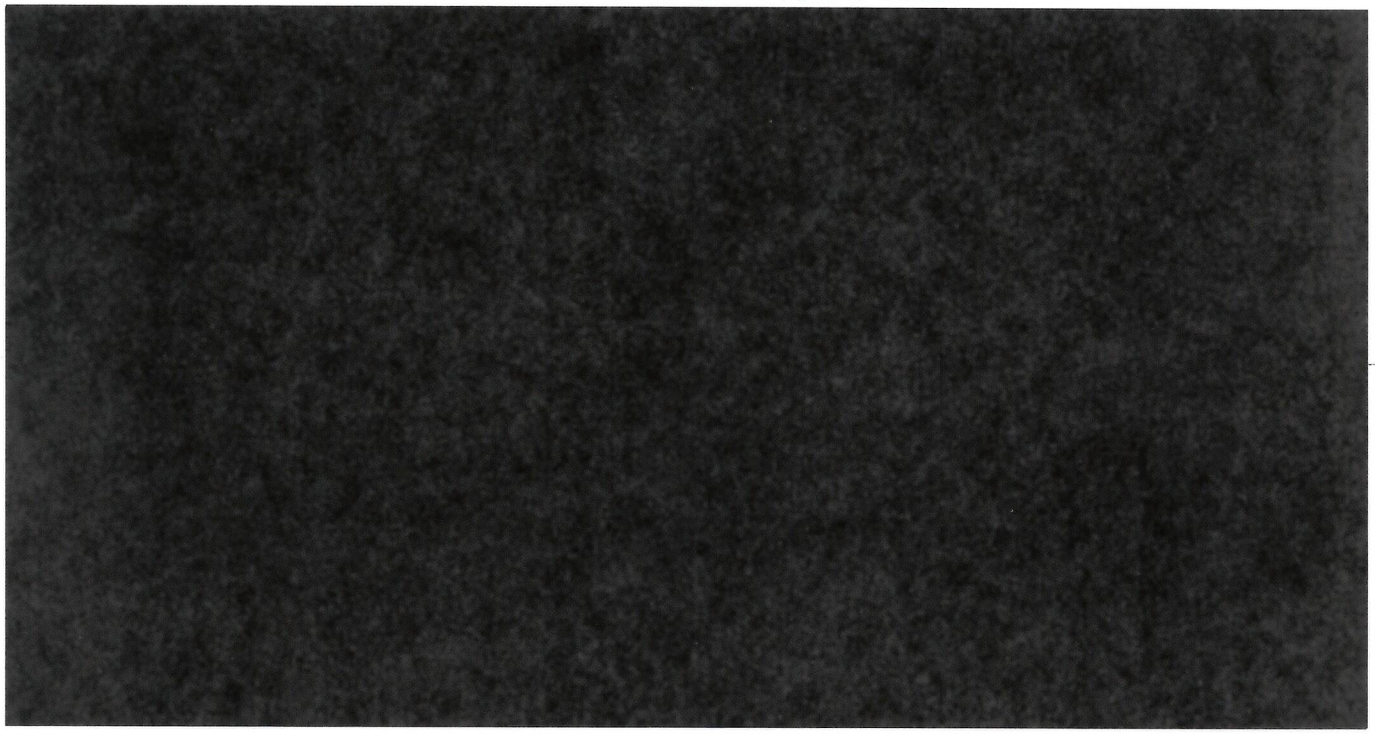
"promptly" if it "uses this provision to respond to such congressional oversight inquiries." September 26, 2016 Memorandum at 7.[47]

Although these provisions could more clearly address responses to requests from congressional overseers, the Court believes they can be fairly read to authorize actions necessary to respond to the requests described by the government. The Court directs the government to provide prompt written notification of any instance when an agency acts in contravention of otherwise applicable minimization requirements in order to respond to an oversight request from any outside entity other than those currently specified in its procedures. The Court expects the government to make such a submission regarding its response to the above-referenced congressional requests promptly upon completion of that response.

4. Amendment of FBI Targeting Procedures with Respect to [redacted]

[redacted]

[47] The government has since orally notified the Court that, in order to respond to these requests and in reliance on this provision of its minimization procedures, NSA has made some otherwise-noncompliant queries of data acquired under Section 702 by means other than upstream Internet collection.



The Court does not view this change, which deals with [redacted] agencies authorized to receive unminimized Section 702-acquired information, as problematic, provided that information is shared only with entities authorized to receive it (in the case of NCTC, information obtained pursuant to [redacted]). The legality of raw information sharing fundamentally rests on the foreign intelligence need to provide the information to the receiving agency and that agency's implementation of FISA-compliant minimization procedures. Accordingly, the Court concludes that this change does not preclude it from finding that the FBI Targeting Procedures meet the requirements of Section 1881a(d)(1).

F. Conclusions

1. The NSA and FBI Targeting Procedures Comply With Statutory Requirements and Are Reasonably Designed to Prevent the Targeting of United States Persons

To summarize, the proposed changes to NSA's targeting procedures now make clear that acquisitions thereunder will be limited to communications to or from persons targeted for acquisition under Section 702. FBI's revised targeting procedures allow it to [redacted] The Court has no difficulty finding that these changes, individually and taken together, do not detract from its earlier holdings with regard to the sufficiency and legality of the FBI and NSA targeting procedures.

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA Targeting Procedures and the FBI Targeting Procedures, as written, are reasonably designed, as required by Section 1881a(d)(1): (1) to ensure that any acquisition authorized under the 2016 Certifications is limited to targeting persons reasonably believed to be located outside the United States, and (2) 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. Moreover, for the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA and FBI Targeting Procedures, as written, are reasonably designed to prevent United States persons from

being targeted for acquisition – a finding that is relevant to the Court's analysis, which is set out below, of whether the procedures are consistent with the requirements of the Fourth Amendment.

2. The FBI, NSA, CIA, and NCTC Minimization Procedures Comply With Statutory Requirements

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court similarly concludes that the NSA, FBI, CIA, and NCTC Minimization Procedures satisfy the definition of minimization procedures at Section 1801(h). In the November 6, 2015 Opinion, the FISC found that the minimization procedures accompanying the 2015 Certifications met statutory and constitutional standards. The FISC recommended two changes to the procedures in future submissions. In both instances, the government has acted on those suggestions, proposing changes to narrow the "legal mandate" exception to each agency's minimization procedures and define more precisely the time limits placed on FBI's retention of information believed to be encrypted or contain secret meaning. Both changes further cabin the relevant agencies' discretion and enhance the protection of nonpublicly available information concerning unconsenting United States persons.[48]

Other changes to minimization procedures pertain to FBI's retention of information for "litigation hold" purposes and enable sharing [redacted] with NCTC. (As noted above, NCTC's revised procedures incorporate

[48] As discussed above, the NSA Minimization Procedures have been revised to eliminate acquisition of "abouts" communications and the most problematic forms of MCTs. As a result of that change, the Court no longer views the prohibition on U.S.-person queries in NSA upstream collection to be necessary to comport with the statute or, as discussed below, the Fourth Amendment.

elements from various other procedures, with appropriate adaptations to fit the context of Section 702.) The Court concludes that none of the proposed changes to the agencies' minimization procedures, individually or collectively, precludes the Court from finding that such procedures comport with Section 1801(h).

Accordingly, the Court finds that the agencies' proposed minimization procedures meet the requirements of 50 U.S.C. § 1801(h). That finding is made in reliance on (1) the above-stated limitations on (a) the types of information that will, and will not, be shared in raw form with the FBI, CIA, and NCTC, and (b) NCTC's retention, use or disclosure of evidence of a crime and information received from other agencies for collection avoidance purposes; and (2) the expectation that the government will faithfully comply with the reporting requirements set forth below, in the procedures themselves, and in Rule 13 of the FISC Rules of Procedure.

G. The Targeting and Minimization Procedures Are Consistent with the Fourth Amendment

The Court must also assess whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A). The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

Reasonableness is "'the ultimate touchstone of the Fourth Amendment.'" In re Certified Question of Law, Docket No. 16-01, Opinion at 31 (FISA Ct. Rev. Apr. 14, 2016) (per curiam) ("In re Certified Question")[49] (quoting Riley v. California, 134 S. Ct. 2473, 2482 (2014)).[50] In assessing the reasonableness of a governmental intrusion under the Fourth Amendment, a court must "balance the interests at stake" under the "totality of the circumstances." In re Directives at 20. Specifically, a court must "balance . . . the degree of the government's intrusion on individual privacy" against "the degree to which that intrusion furthers the government's legitimate interest." In re Certified Question at 31. "The more important the government's interest, the greater the intrusion that may be constitutionally tolerated." In re Directives at 19-20.

> If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in

---

[49] A declassified version of this opinion is available at: www.dni.gov/files/icotr/FISCR%Opinion%2016-01.pdf.

[50] Although "[t]he warrant requirement is generally a tolerable proxy for 'reasonableness' when the government is seeking to unearth evidence of criminal wrongdoing, . . . it fails properly to balance the interests at stake" when "the government is instead seeking to preserve the nation's security from foreign threats." In re Certified Question at 3. Accordingly, a warrant is not required to conduct surveillance "to obtain foreign intelligence for national security purposes . . . directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States." In re Directives Pursuant to Section 105B of FISA, Docket No. 08-01, Opinion at 18-19 (FISA Ct. Rev. Aug. 22, 2008) ("In re Directives"). (A declassified version of In re Directives is available at 551 F.3d 1004 (FISA Ct. Rev. 2008)). The FISC has repeatedly reached the same conclusion regarding Section 702 acquisitions. See, e.g., November 6, 2015 Opinion at 36-37; September 4, 2008 Opinion at 34-36; accord United States v. Hasbajrami, 2016 WL 1029500 at *7-*9 (E.D.N.Y. March 8, 2016); United States v. Mohamud, 2014 WL 2866749 at *15-*18 (D. Or. June 24, 2014).

> favor of upholding the government's actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Id. at 20.

"Collecting foreign intelligence with an eye toward safeguarding the nation's security serves . . . a particularly intense interest" that is "different from the government's interest in the workaday enforcement of the criminal law." In re Certified Question at 29 (internal quotation marks omitted); see also id. at 31 (noting "the paramount interest in investigating possible threats to national security"). For that reason, "the government's investigative interest in cases arising under FISA is at the highest level and weighs heavily in the constitutional balancing process." Id. at 32.

On the other side of the balance is the degree of intrusion on individual privacy interests protected by the Fourth Amendment. The degree of intrusion here is limited by restrictions on how the government targets acquisitions under Section 702 and how it handles information post-acquisition. For reasons explained above, the Court has found that the targeting procedures now before it are reasonably designed to limit acquisitions to targeted persons reasonably believed to be non-United States persons located outside the United States, whose privacy interests are not protected by the Fourth Amendment. See, e.g., November 6, 2015 Opinion at 38; September 4, 2008 Opinion at 37 (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990)). That is not to say, however, that targeting non-United States persons located outside the United States for acquisition under Section 702 never implicates interests protected by the Fourth Amendment. Under the revised procedures, the government may acquire communications to

which United States persons and persons within the United States are parties when such persons communicate with a Section 702 target.[51] Therefore it is necessary to consider how information from those communications will be handled.

Steps taken by the government to restrict the use or disclosure of information after it has been acquired can reduce the intrusiveness of the acquisition for purposes of assessing its reasonableness under the Fourth Amendment. See In re Certified Question at 35. In the Prior 702 Dockets, the FISC found that "earlier versions of the various agencies' targeting and minimization procedures adequately protected the substantial Fourth Amendment interests that are implicated by the acquisition of communications of such United States persons." November 6, 2015 Opinion at 38-39 (citing August 26, 2014 Opinion at 38-40; August 30, 2013 Opinion at 24-25). Specifically, "'the combined effect of these procedures'" was "'to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated' and to ensure that 'non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary.'" November 6, 2015 Opinion at 39 (quoting August 26, 2014 Opinion at 40).

The November 6, 2015 Opinion included a careful analysis of the rules for querying Section 702 information using United States person identifiers under the minimization procedures for the NSA, the CIA, and especially the FBI. See November 6, 2015 Opinion at 24-

[51] NSA's elimination of "abouts" collection should reduce the number of communications acquired under Section 702 to which a U.S. person or a person in the United States is a party.

36, 39-45. After receiving briefing and oral argument from an amicus curiae appointed under 50 U.S.C. § 1803(i)(2)(B), the FISC concluded that, although its review did not involve treating each query as a separate action subject to a test for Fourth Amendment reasonableness, the querying rules were relevant to its assessment of whether the procedures as a whole were reasonable under the Fourth Amendment. November 6, 2015 Opinion at 40-41. The FISC further determined that the querying rules did not preclude a finding that the procedures were consistent with the requirements of the Fourth Amendment. Id. at 44-45.

In the procedures now before the Court, the relevant provisions of the CIA and FBI minimization procedures remain unchanged, see CIA Minimization Procedures at § 4; FBI Minimization Procedures at §§ III.D, IV.D, and the NCTC procedures generally track the pertinent requirements of the CIA Minimization Procedures. See NCTC Minimization Procedures at § C.3.[52]

With regard to the querying rules in the CIA and NCTC procedures, the Court adopts the analysis of the November 6, 2015 Opinion.

As discussed above, NSA's procedures now limit all acquisitions – including upstream Internet acquisitions – to communications to or from an authorized Section 702 target. That limitation places upstream Internet collection in a posture similar to other forms of Section 702 collection for the purpose of assessing reasonableness under the Fourth Amendment. The revised procedures subject NSA's use of U.S. person identifiers to query the results of its newly-

[52] Unlike the CIA procedures, the NCTC procedures require that queries of Section 702 metadata, as well as contents, be reasonably designed to return foreign intelligence information. NCTC Minimization Procedures at § C.3.

limited upstream Internet collection to the same limitations and requirements that apply to its use of such identifiers to query information acquired by other forms of Section 702 collection. See NSA Minimization Procedures § 3(b)(5). For that reason, the analysis in the November 6, 2015 Opinion remains valid regarding why NSA's procedures comport with Fourth Amendment standards of reasonableness with regard to such U.S. person queries, even as applied to queries of upstream Internet collection.

As discussed in the November 6, 2015 Opinion, the FBI's minimization procedures contemplate queries conducted to elicit foreign intelligence information and queries conducted to elicit evidence of crimes. With respect to the latter type of query, the FISC's approval of the FBI minimization procedures in 2015 was bolstered by the government's assessment that "FBI queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results" from Section 702 information. See November 6, 2015 Opinion at 44. To confirm the continued accuracy of that assessment, the FISC ordered the government to report on "each instance after December 4, 2015, in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information." Id. at 78.

The government has reported one set of queries as responsive to this requirement. On [redacted], an FBI analyst reviewing Section 702 information found an email message in which a person in the United States gave detailed descriptions of violent, abusive acts [redacted] committed [redacted] children. [redacted] Notice regarding FBI queries of Section 702-

acquired information designed to return evidence of a crime unrelated to foreign intelligence ("[redacted] Notice"), at 2. In an effort to identify additional evidence of abuse, the FBI ran queries of Section 702 information using the names of the suspected abuser, the apparent victims, and other terms derived from that e-mail message. Those queries only retrieved the previously reviewed e-mail message from which the query terms were derived. Id. Pursuant to Section I.F of its minimization procedures, the FBI disseminated information about the child abuse to a local child protective services agency, [redacted] Id.

The undersigned judge finds persuasive the November 6, 2015 Opinion's analysis of the FBI's querying rules. The single reported instance of queries that returned U.S. person information unrelated to foreign intelligence information does not detract from that analysis, especially since those queries did not result in any further intrusion on privacy: they merely retrieved information already known to the analyst who ran the queries.[53]

For the reasons stated above, neither the NCTC's receipt of unminimized information acquired regarding counterterrorism targets, subject to its applying the NCTC Minimization Procedures, nor the other above-described modifications to the targeting and minimization procedures, causes the Court to deviate from prior assessments that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

---

[53] The Court notes, however, that the FBI did not identify those queries as responsive to the Court's reporting requirement until NSD asked whether any such queries had been made in the course of gathering information about the Section I.F dissemination. [redacted] Notice at 2. The Court is carrying forward this reporting requirement and expects the government to take further steps to ensure compliance with it.

IV. THE COMPLIANCE AND IMPLEMENTATION ISSUES REPORTED BY THE GOVERNMENT DO NOT WARRANT A FINDING THAT, AS IMPLEMENTED, THE TARGETING AND MINIMIZATION PROCEDURES ARE DEFICIENT.

The FISC has consistently understood its review of targeting and minimization procedures under Section 702 to include examining how the procedures have been and will be implemented. See, e.g., November 6, 2015 Opinion at 7; August 30, 2013 Opinion at 6-11, 19-22; April 7, 2009 Opinion at 22-25. As the Foreign Intelligence Surveillance Court of Review has noted, FISC "supervision of the execution of pen register orders further reduces the risk that such measures will be employed under circumstances, or in a manner, that unreasonably intrudes on individuals' privacy interests." In re Certified Question at 36-37. The same conclusion applies to FISC examination of how the government implements the Section 702 procedures.

For purposes of this examination, "the controlling norms are ones of reasonableness, not perfection," November 6, 2015 Opinion at 45, under both Section 702[54] and the Fourth Amendment.[55] The Court evaluates the reasonableness of "the program as a whole," not of individual actions in isolation. November 6, 2015 Opinion at 40-41. The assessment of

---

[54] See 50 U.S.C. § 1881a(d)(1) (requiring targeting procedures that are "reasonably designed to" limit targeting to "persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition" of communications to which all parties are known to be in the United States); § 1881a(e)(1) (requiring minimization procedures as defined in §§ 1801(h)(1) or 1821(4), i.e., procedures "reasonably designed" to minimize acquisition and retention, and to prohibit dissemination, of information concerning United States persons, consistent with foreign intelligence needs).

[55] See, e.g., United States v. Knights, 534 U.S. 112, 118 (2001) ("The touchstone of the Fourth Amendment is reasonableness . . . ."); In re Directives at 34 (surveillances found to be reasonable under the Fourth Amendment where "the risks of error and abuse are within acceptable limits and effective minimization procedures are in place").

reasonableness takes due account of the fact that implementing Section 702 is "a large and complex endeavor . . . effected through thousands of discrete targeting decisions for individual selectors,"[56] each of which implicates selector-specific pre-tasking and post-tasking requirements, November 6, 2015 Opinion at 45-46, and that for all information acquired under Section 702, minimization procedures impose "detailed rules concerning . . . retention, use, and dissemination . . . ." Id. at 46. As the FISC has previously observed:

> Given the number of decisions and volume of information involved, it should not be surprising that occasionally errors are made. Moreover, the government necessarily relies on [redacted] processes in performing post-tasking checks, see, e.g., August 30, 2013 Opinion at 7-9, and in acquiring, routing, storing, and when appropriate purging Section 702 information. See, e.g., April 7, 2009 Opinion at 17-22. Because of factors such as changes in communications technology or inadvertent error, these processes do not always function as intended.

Id.

Overall, the Court concludes that the targeting and minimization procedures satisfy applicable statutory requirements and are reasonable under the Fourth Amendment, despite the reported instances of non-compliance in prior implementation. The Court bases this conclusion in large measure on the extensive oversight conducted within the implementing agencies and by the DOJ and ODNI. Due to those efforts, it appears that compliance issues are generally

---

[56] For example, NSA "reports that, on average, approximately [redacted] facilities were under task at any given time between December 1, 2016 and February 28, 2017." March 17, 2016 Compliance Report at 1 (footnote omitted). Facilities tasked for acquisition include [redacted] Id. at 1 n.1. "Additionally, between December 1, 2016 and February 28, 2017, the [FBI] reports that it received and processed approximately [redacted] Id. at 1.

identified and remedied in a timely and appropriate fashion.[57] Nonetheless, the Court believes it beneficial to discuss certain ongoing or recent compliance issues and, in some cases, direct the government to provide additional information.

A. Resolution of Issues Addressed in the November 6, 2015 Opinion

The November 6, 2015 Opinion discussed several significant compliance problems that were then pending. See November 6, 2015 Opinion at 47-77. With the exception of non-compliance with minimization procedures related to attorney-client privileged communications, which are discussed separately, those compliance issues have been resolved as described below.

1. Failure of Access Controls in FBI's [redacted]

[redacted] while the 2015 Certifications were pending, the government filed a notice ("[redacted] Notice") indicating that a failure of access controls in an FBI database containing raw Section 702-acquired information resulted in [redacted] FBI employees improperly receiving access to such information. [redacted] Notice at 1. Specifically, [redacted]

[57] Too often, however, the government fails to meet its obligation to provide prompt notification to the FISC when non-compliance is discovered. See FISC Rule of Procedure 13(b). For example, it is unpersuasive to attribute – even "in part" – an eleven-month delay in submitting a preliminary notice to "NSA's efforts to develop remedial steps," see April 7, 2017 Preliminary Notice (Mislabeling) at 1 n.1, 2, when the purpose of a preliminary notice is to advise the Court while investigation or remediation is still ongoing. See also, e.g., February 28, 2017 Notice of a Compliance Incident Regarding Incomplete Purges of Information Obtained Pursuant to Multiple FISA Authorities ("February 28, 2017 Notice") at 1-2, n.3 (five-month delay attributed "to administrative issues surrounding the reorganization of NSA offices and personnel"). The Court intends to monitor closely the timeliness of the government's reporting of non-compliance regarding Section 702 implementation.

[redacted] allowed [redacted] users access to Section 702-acquired information, id., when only [redacted] were cleared for such access. Id. at 1, n.1. This resulted in violations of Sections III.A. and III.B of the FBI's minimization procedures.[58] The government provided testimony on this issue at a hearing on [redacted] filed a Supplemental Notice on [redacted] indicating that [redacted] FISA-acquired products were "exported" [redacted] users who were not authorized to access these products. [redacted] Notice at 2.

On [redacted], the government filed what was styled as a Final Notice on this issue [redacted] Notice"). That notice indicated that the FBI [redacted] had not disseminated the FISA-acquired products; and all [redacted] users had deleted from their systems the raw FISA-acquired information they had exported. [redacted]

[58] As then in effect and as now proposed, Section III.A of the FBI Minimization Procedures requires the FBI to "retain all FISA-acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with [the FBI Minimization Procedures] and other applicable FBI procedures." FBI Minimization Procedures § III.A. Section III.B of the FBI Minimization Procedures further requires the FBI to grant access to raw Section 702-acquired information in a manner that is "consistent with the FBI's foreign intelligence information-gathering and information-sharing responsibilities, . . . [p]ermitting access . . . only by individuals who require access in order to perform their job duties[.]" Id. § III.B. It also requires users with access to FISA-acquired information to receive training on minimization requirements. Id. § III.B.4.

[redacted] In the Court's assessment, the government has appropriately remedied this incident.

2. NSA Failures to Complete Required Purges

On July 13, 2015, the Government filed a notice regarding NSA's purge processes for FISA-acquired information in its mission management systems ("July 13, 2015 Notice"). That notice indicated that the NSA had not been removing records associated with Section 702 data subject to purge from its [redacted] database. July 13, 2015 Notice at 3.

On October 5, 2015, the government filed a Supplemental Notice regarding NSA's purge processes for FISA-acquired information ("October 5, 2015 Notice"). That notice indicated that NSA had now removed from [redacted] all Section 702-acquired records that were marked as subject to purge. October 5, 2015 Notice at 2. On October 28, 2015, however, the government filed another Supplemental Notice regarding NSA's purge processes ("October 28, 2015 Notice") in which it reported that a technical malfunction in [redacted] had rendered the aforementioned purges incomplete. October 28, 2015 Notice at 2.

On January 14, 2016, the government filed a Supplemental Notice ("January 14, 2016 Notice") indicating that as of October 30, 2015, [redacted] was properly configured to remove records subject to purge and corresponding to identifiers on the MPL. January 14, 2016

Notice at 2. At that time NSA had completed purging records that had been added to the MPL between 2011 and 2015. Id. On September 22, 2016, the government filed another Supplemental Notice ("September 22, 2016 Notice on [redacted] confirming that as of February 2016, the NSA had removed from [redacted] all historical Section 702-acquired records subject to purge.[59] September 22, 2016 Notice on [redacted] at 2.

The July 13, 2015 Notice also reported "a compliance incident regarding FISA-acquired information subject to purge or age off that [was] being retained in two of NSA's compliance mission management systems, [redacted] and [redacted] in a manner that is "potentially inconsistent with NSA's FISA-related minimization procedures." July 13, 2015 Notice at 2, 5. Subsequent communications between the government and FISC staff revealed that [redacted] and [redacted] may also have been retaining data, the use or disclosure of which could violate 50 U.S.C. § 1809(a)(2). The November 6, 2015 Opinion directed the government to provide additional information about NSA's retention of certain categories of information in [redacted] and [redacted] November 6, 2015 Opinion at 78.

On December 18, 2015, the government filed a detailed description of its plan and timeline for remedying improper retention in [redacted] and [redacted] See Prior 702 Dockets, Verified Response to the Court's Order Dated November 6, 2015, filed on Dec. 18,

[59] The government also disclosed in the January 14, 2016 Notice that [redacted] was not configured to age off all FISA-acquired information pursuant to relevant minimization procedures. January 14, 2016 Notice at 2. As of August 3, 2016, the NSA had removed from [redacted] all Section 702-acquired information identified as due for destruction under the retention periods set by the NSA Minimization Procedures, and prospectively, the NSA will remove Section 702-acquired information from [redacted] in compliance with those retention periods. September 22, 2016 Notice on [redacted] at 2.

2015. On September 22, 2016, the government provided a written update on the NSA's efforts to remove from [redacted] and [redacted] information that was subject to purge or age-off under the NSA Minimization Procedures ("September 22, 2016 Notice on [redacted] and [redacted] As of February 17, 2016, NSA had removed from [redacted] and [redacted] all Section 702-acquired information subject to age-off under the five- and two-year retention periods set by the NSA Minimization Procedures. September 22, 2016 Notice on [redacted] and [redacted] at 2. As of September 9, 2016, the NSA had deleted from [redacted] and [redacted] all historical Section 702-acquired data potentially subject to § 1809(a)(2), and it had developed a plan to deal prospectively with information potentially subject to § 1809(a)(2). Id. at 3. Finally, as of September 9, 2016, the NSA had removed from [redacted] and [redacted] other categories of information that the November 6, 2015 Opinion had identified as not permissible for retention in [redacted] and [redacted] (e.g., attorney-client communications that do not contain foreign intelligence information or evidence of a crime). Id. at 3-4.

B. Issues Arising Under the NSA Targeting Procedures

NSA's targeting procedures require that analysts, before tasking a selector for acquisition, make a reasonable assessment that the user of the selector is a non-U.S. person located outside the United States. See NSA Targeting Procedures § 1. Post-tasking, analysts are required to take reasonable steps to confirm that the selector continues to be used by a non-U.S. person located outside the United States. See NSA Targeting Procedures § 2. Those requirements directly bear on statutory limitations on Section 702 acquisitions. See 50 U.S.C. § 1881a(c)(1)(A), (d)(1)(A)

(targeting procedures must be reasonably designed to ensure that acquisitions are limited to targeting persons reasonably believed to be outside the United States); § 1881a(b)(3), (4) (government may not intentionally target a United States person reasonably believed to be outside the United States or intentionally acquire any communication as to which the sender and all intended recipients are known at time of acquisition to be in the United States).

Compliance and implementation issues have arisen regarding these pre-tasking assessments and post-tasking reviews. While those issues merit discussion, the Court does not believe they are sufficiently serious or pervasive to warrant finding that the targeting procedures do not meet the above-described statutory requirements or are inconsistent with the Fourth Amendment.

1. Scope of Pre-Tasking Review of [redacted]

One of the measures taken by NSA analysts to fulfill pre-tasking obligations is to check [redacted] for information that may be probative of [redacted] For example, [redacted].

According to a notice filed by the government on August 24, 2016, NSA analysts often relied on the above-referenced [redacted] tool to [redacted] as part of those pre-tasking checks. August 24, 2016 Update Regarding the Scope of Section 702 Pre-Tasking Review of [redacted] at 2 ("August 24, 2016 Update"). The data returned [redacted] was

limited, as [redacted] only [redacted]. Id. In certain circumstances, the results from [redacted] could have provided an incomplete and misleading impression of [redacted]. The government acknowledges that the sufficiency of running a [redacted] as the sole basis for a pre-tasking assessment "depends upon the information known about the target from other sources and the nature of the information returned by the [redacted] Id. Subsequent investigation revealed [redacted] instances of improper taskings. See August 24, 2016 Update at 2, n.2. NSA placed on its MPL information obtained as a result of these taskings. Id. at 2.[60]

NSA has developed a new tool for analysts to use for pre-tasking checks [redacted] August 24, 2016 Update at 4. "In addition to [redacted], NSA's new tool is also [redacted] that will greatly enhance analysts' pre-tasking reviews." Id.

[60] For discussion of the government's processes for purging Section 702 information, see March 17, 2017 Compliance Report at 2-5.

While the described functionality of the new tool improves on some of the limitations of [redacted] it should not be seen as a panacea. In the Court's view, the fundamental cause of these improper taskings was not the limitations of [redacted] or other [redacted] tools, but rather the failure of analysts in these particular cases to pursue reasonable lines of inquiry regarding [redacted] See, e.g., August 24, 2016 Update at 3 [redacted]. It remains the obligation of analysts to exercise due diligence in the particular circumstances of each pre-tasking review, rather than to presume that using a given [redacted] tool or protocol will suffice. The government acknowledges that sometimes, after deploying the new tool, "additional research will be necessary to satisfy the totality of the circumstances test [for pre-tasking reviews] contained in the NSA Targeting Procedures," id. at 5, and addresses in its training efforts how NSA analysts should understand and comply with this requirement. See October 4, 2016 Transcript at 19-20.

2. Frequency of Post-Tasking Review of Contents

While the government did not report the following information as involving non-compliance with the NSA's targeting procedures, the Court believes it bears significantly on how those procedures are implemented and therefore merits discussion.

The NSA's targeting procedures do not require analysts to review the contents of communications acquired from tasking a particular selector at fixed intervals. Instead, they provide that such content review "will be conducted according to analytic and intelligence

requirements and priorities." See, e.g., NSA Targeting Procedures § II at 6.[61] As previously described to the FISC, however, NSA follows a policy whereby such content review is performed no later than [redacted] days after the first acquisition and at intervals of no more than [redacted] days thereafter. See September 13, 2016, Update Regarding Post-Targeting Content Reviews ("September 13, 2016 Update") at 2; Docket No. [redacted], Memorandum Opinion at 9-10 (FISA Ct. Oct. 24, 2014).

NSA and FBI analysts with access to Section 702 data are trained on this policy, while CIA analysts receive training that "is consistent with" the policy and are instructed "to review content as it is acquired." September 13, 2016 Update at 3.[62] According to a supplemental letter filed on March 13, 2017 ("March 13, 2017 Supp. Letter"), the government monitors compliance with the policy with regard to Section 702 data in an NSA repository called [redacted] but otherwise does not comprehensively monitor or verify whether analysts in fact conduct content reviews in conformance with that policy. March 13, 2017 Supp. Letter at 2.[63] For that reason,

---

[61] This content review is in addition to other post-tasking steps to ascertain whether a tasked facility is being used inside the United States, such as [redacted] Id. § II at 6-7.

[62] [redacted] See NSA Targeting Procedures § 2 at 7 n. 2-3.

[63] NSA routes most forms of Internet communications acquired under Section 702 to a repository called [redacted] March 13, 2017 Supp. Letter at 2. For review of communications in [redacted] NSA has [redacted] that monitors whether content checks are performed, sends prompts to analysts to conduct [redacted] and [redacted] reviews, and sends overdue notices. Id. at 1-2. NSA does not have such an alert system for other repositories containing

(continued...)

deviations from the policy may not be detected unless and until the circumstances are examined for other purposes. See September 13, 2016 Update at 3.

To address this concern, the government undertakes "to notify the Court . . . when, in connection with compliance incidents, the government also learns that content was not reviewed in accordance with the applicable policy." Id. at 4. The government further undertakes to advise the FISC "of the total number of instances in which the government's investigation into a potential [non-compliance] incident revealed that content review was not timely conducted in accordance with [this policy]," even if the government determines that, strictly speaking, there was no violation of the targeting procedures themselves. See id. That figure will be included in each of the government's quarterly compliance reports. Id.

On March 13, 2017, the government reported the results of an examination of the performance of [redacted] and [redacted] content reviews for data in [redacted] during January-March 2016. March 13, 2017 Supp. Letter at 2. That examination revealed a compliance rate of approximately 79% for [redacted] reviews and 99% for [redacted] reviews. Id. NSA plans to issue an advisory to personnel reminding them of the policy. Id. at 3.

The Court intends to scrutinize the information submitted regarding future deviations from this policy. It also encourages the government to explore further measures, through

---

[63](...continued)
Section 702 information, though it has plans to develop systems for additional repositories by the end of 2017. Id. at 2-3. FBI and CIA do not have comparable systems. October 4, 2016 Transcript at 21, 24.

[redacted] processes or otherwise, to prompt analysts to conduct content reviews in accordance with this policy, and to monitor or verify adherence to it.

C. Issues Arising Under the NSA Minimization Procedures

In addition to the improper use of U.S.-person identifiers to query the results of upstream Internet data discussed above, noteworthy compliance issues have arisen with regard to NSA's upstream collection of Internet communications and querying of Section 702-acquired data.

1. NSA Upstream Collection of Internet Communications

Under the pre-2017 Amendments version of the NSA Minimization Procedures, NSA is required to "take reasonable steps post-acquisition to identify and segregate through technical means" those MCTs that are particularly likely to involve communicants in the United States; specifically, those for which "the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown." NSA Minimization Procedures § 3(b)(4)a. (prior to the 2017 Amendments). Those procedures permit only certain 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" to access MCTs that have been segregated in the manner described above. § 3(b)(4)a.2. Information in a segregated MCT "may not 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 communication as to which the

sender and all intended recipients are reasonably believed to be located in the United States." § 3(b)(4)a.2.(a).[64]

Starting in April 2015, a [redacted] error affected NSA's upstream collection [redacted] See September 30, 2016 Supplemental Notice of Compliance Incident Regarding Collection Pursuant to Section 702 ("September 30, 2016 Supp. Notice") at 1. The error was discovered on January 26, 2016, and corrected on a going-forward basis the next day. Id.

This [redacted] error led to two types of compliance problems. First, it resulted in the unauthorized acquisition of Internet "communications from facilities that only partially matched authorized Section 702 [selectors] (e.g., [redacted]" Id. at 1-2. It appears that the government has taken appropriate steps to identify and purge the improperly acquired information. Id. at 2-3. NSA has positively identified [redacted] "data objects" as having been subject to this over-collection. Id. In addition, based on the nature of the [redacted] error and the technical characteristics of information likely to have been improperly collected due to the error, NSA has identified in excess of [redacted] "data objects" that may have been over-collected. Id. at 3. Because it was not technically feasible for NSA to identify within that set any and all objects that actually had been over-collected, NSA has put [redacted]-plus objects, as well as the [redacted] objects positively identified as having been over-collected, on its MPL. Id.; see also March 17, 2017 Quarterly Report at 114-15.

[64] In practice, however, no analysts received the requisite training in order to work with the segregated MCTs. October 4, 2016 Transcript at 41-43.

Second, the [redacted] error resulted in failures in the technical processes whereby NSA identified MCTs that are subject to the segregation regime described above. Specifically, some MCTs may have been wrongly identified and labeled as ones in which the active user was the target, which would have resulted in those MCTs not being segregated. September 30, 2016 Supp. Notice at 3-4. To the extent wrongly-identified MCTs were actually ones for which the active user is reasonably believed to have been located in the United States or for whom the active user's location was unknown, they should have been segregated and subject to the above-described heightened access controls. Any large-scale failure to identify and segregate MCTs subject to those heightened access controls would have threatened to undermine one of the safeguards on which the FISC relied in 2011 when it approved the procedures adopted by the government in response to the FISC's prior finding of deficiency. See November 30, 2011 Opinion at 11-15.

The Court did not find entirely satisfactory the government's explanations of the scope of those segregation errors and the adequacy of its response to them and addressed some of its concerns at the October 4, 2016 Hearing. See, e.g., October 4, 2016 Transcript at 35-38.[65] Questions about the adequacy of steps previously taken to respond to the errors, however, are no longer material to the Court's review of the NSA Minimization Procedures. Under the revised

[65] The government later reported it had inadvertently misstated the percentage of NSA's overall upstream Internet collection during the relevant period that could have been affected by this [redacted] error (the government first reported the percentage as roughly 1.3%, when it was roughly 3.7%). April 11, 2017 Notice of Material Misstatement and Supplemental Notice of Compliance Incidents Regarding Collection Pursuant to Section 702 at 2.

NSA Minimization Procedures, the results of upstream Internet collection during the relevant timeframe must be segregated and destroyed.

2. Improper Querying [redacted] Communications

U.S. person identifiers may be used to query Section 702 data only if they are first "approved in accordance with [internal] NSA procedures, which must require a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information." NSA Minimization Procedures § 3(b)(5).[66] In performing such queries, NSA analysts sometimes use a tool called "[redacted] can be used to query data repositories, including one called [redacted] September 30, 2016 Final Notice of Compliance Incidents Regarding Improper Queries ("September 30, 2016 Final Notice") at 1. [redacted] communications acquired pursuant to Section 702, as well as other FISA authorities. Id.

In May and June 2016, NSA reported to oversight personnel in the ODNI and DOJ that, since approximately 2012, use of [redacted] to query communications in [redacted] had resulted in inadvertent violations of the above-described querying rules for Section 702 information. Id. The violations resulted from analysts not recognizing the need to avoid querying datasets for which querying requirements were not satisfied or not understanding how to formulate [redacted] queries to exclude such datasets. Id. at 1-2.

---

[66] As previously noted, NSA may not use U.S.-person identifiers to query the results of upstream Internet collection until the 2017 Amendments take effect, but will be able to run such queries of the narrower form of upstream Internet collection contemplated under the 2017 Amendments, subject to the approval process described above.

NSA examined all queries using identifiers for "U.S. persons targeted pursuant to Sections 704 and 705(b) of FISA using the [redacted] tool in [redacted] . . . from November 1, 2015 to May 1, 2016." Id. at 2-3 (footnote omitted). Based on that examination, "NSA estimates that approximately eighty-five percent of those queries, representing [redacted] queries conducted by approximately [redacted] targeted offices, were not compliant with the applicable minimization procedures." Id. at 3. Many of these non-compliant queries involved use of the same identifiers over different date ranges. Id. Even so, a non-compliance rate of 85% raises substantial questions about the propriety of using of [redacted] to query FISA data. While the government reports that it is unable to provide a reliable estimate of the number of non-compliant queries since 2012, id., there is no apparent reason to believe the November 2015-April 2016 period coincided with an unusually high error rate.

The government reports that NSA "is unable to identify any reporting or other disseminations that may have been based on information returned by [these] non-compliant queries" because "NSA's disseminations are sourced to specific objects," not to the queries that may have presented those objects to the analyst. Id. at 6. Moreover, [redacted] query results are generally retained for just [redacted] Id.[67]

The NSA has taken steps to educate analysts on the proper use of [redacted] it has provided a "reminder" to all analysts about the need "to limit queries across authorities in [redacted] with

[67] Information retrieved by an improper query might nonetheless satisfy the requirements for dissemination; indeed, absent a second violation of the minimization procedures, separate from the improper query, one would expect any disseminated information to have satisfied those requirements.

an explanation of how different types of queries operate; it issued a separate "Compliance Advisory," which further addressed querying practices using [redacted] to all NSA target offices; and it revised a "banner" presented to users of [redacted] to emphasize that U.S. person identifiers should never be used for a type of query (called a "selector query") that runs "against all data [that] an analyst is authorized to access." Id. at 1, 6.

At the October 4, 2016 Hearing, the government represented that, based on ongoing oversight efforts, those measures appear to have been effective in improving how analysts use [redacted] to query Section 702 data. October 4, 2016 Transcript at 47-49. On April 3, 2017, the government reported to the Court that it had reaffirmed that assessment, based on discussions with NSA analysts and the absence of additional non-compliant queries using [redacted] April 3, 2017, Supplemental Notice of Compliance Incidents Regarding Improper Queries, at 3. In view of these remedial steps, the Court believes that, notwithstanding the above-described non-compliance, the NSA Minimization Procedures meet the statutory definition of "minimization procedures" and are consistent with the requirements of the Fourth Amendment.

D. Issues Arising Under the FBI Minimization Procedures

The following violations of the FBI's minimization procedures merit discussion.

1. Improper Disclosures of Raw Information

On March 9, 2016, DOJ oversight personnel conducting a minimization review at the FBI's [redacted] learned that the FBI had disclosed raw FISA information, including but not limited to Section 702-acquired information, to a [redacted] Compliance Report at 92. [redacted] is part of the [redacted]

[redacted] and "is largely staffed by private contractors" [redacted] certain [redacted] contractors had access to raw FISA information on FBI storage systems [redacted] Id. The apparent purpose for the FBI's granting such access was to receive analytical assistance from [redacted] Nonetheless, the [redacted] contractors had access to raw FISA information that went well beyond what was necessary to respond to the FBI's requests; [redacted] The FBI discontinued the above-described access to raw FISA information as of April 18, 2016. [redacted]

The contractors in question received training on the FBI minimization procedures, stored the raw information only on FBI systems, and did not disseminate it further. Id. at 93. Nonetheless, the above-described practices violated the governing minimization procedures. Section III.A of the FBI's minimization procedures (as then in effect and as now proposed) provides: "The FBI must retain all FISA-acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with these and other applicable FBI procedures. These retention procedures apply to FISA-acquired information retained in any form." The FBI may disseminate Section 702-acquired information only in accordance with Section V of those procedures. FBI Minimization Procedures § III.C.1.

Under Section V.D of those procedures, personnel working for another federal agency such as [redacted] may receive raw information acquired under Section 702 in order to

provide technical or linguistic assistance to the FBI, but only if certain restrictions are followed. See id. § V.D. Those restrictions were not in place with regard to the [redacted] contractors: their access was not limited to raw information for which the FBI sought assistance and access continued even after they had completed work in response to an FBI request. See [redacted] Compliance Report at 93. At the October 4, 2016 Hearing, the government represented that it was investigating whether there have been similar cases in which the FBI improperly afforded non-FBI personnel access to raw FISA-acquired information on FBI systems. October 4, 2016 Transcript at 64.

In a separate violation of its minimization procedures, the FBI delivered raw Section 702-acquired information to a [redacted] contractor called [redacted] Compliance Report at 131. The information in question pertains to [redacted] accounts tasked under Section 702. Id. [redacted] as a federal agency, could receive raw Section 702-acquired information in order to provide technical assistance to the FBI, subject to the requirements of Section V.D of the FBI Minimization Procedures. See FBI Minimization Procedures § V.D ("FBI is authorized to

disclose FISA-acquired information to assisting federal agencies for further processing and analysis," subject to specified restrictions) (emphasis added). [redacted] however, is not a federal agency and the [redacted] personnel who worked with the information were "not directly supervised by or otherwise under the direction and control of [redacted] Compliance Report at 132. For these reasons, the government concluded that the FBI had given the information to the private entity [redacted], not to an assisting federal agency. See id.[68]

[redacted] The government has not explained why giving [redacted] personnel access to the raw information during installation of the tool would not involve a separate violation of the FBI Minimization Procedures. Accordingly, the Court is ordering the government to provide additional information regarding this second grant of access to raw Section 702 information.

These violations, when placed in the context of Section 702 acquisitions in their entirety, do not preclude a finding that the FBI Minimization Procedures meet the statutory definition of "minimization procedures" and are consistent with the requirements of the Fourth Amendment.

---

[68] In contrast, the above-described [redacted] contractors worked in a federal facility under the supervision of [redacted] Compliance Report at 93. It appears that the government views the above-described disclosures of information to the [redacted] contractors as disclosures to a federal agency, rather than to a private entity or private individuals. In any event, the government acknowledges that those disclosures were improper for other reasons, so the Court need not reach this question.

The improper access previously afforded the [redacted] contractors has been discontinued, while the information disclosed to [redacted] pertains to just [redacted] tasked selectors.

The Court is nonetheless concerned about the FBI's apparent disregard of minimization rules and whether the FBI may be engaging in similar disclosures of raw Section 702 information that have not been reported.[69] Accordingly, the Court is directing the government to provide additional as described below.

2. Potential Over-Retention of Section 702 Information

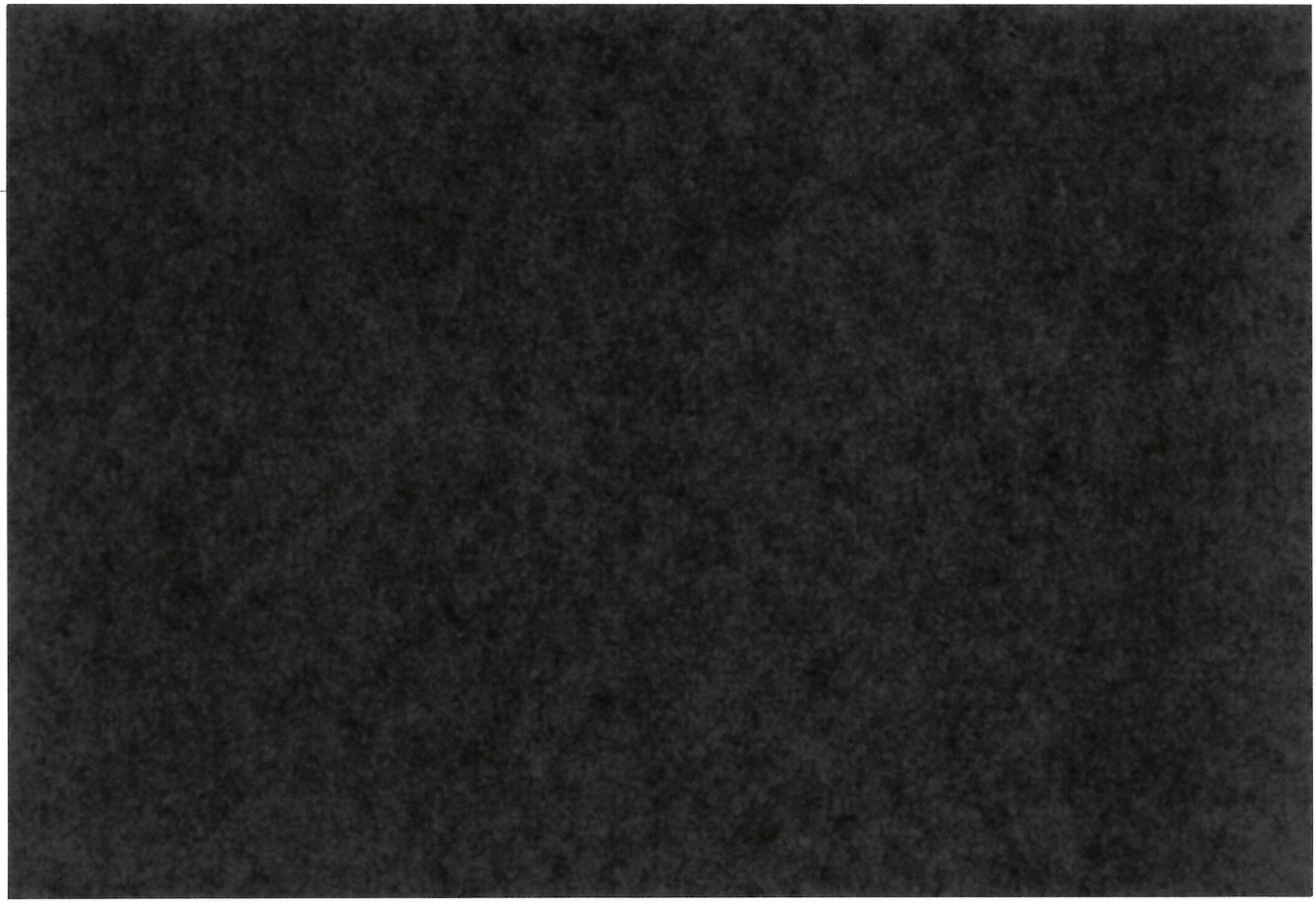
Last year, in the context of approving the standard minimization procedures employed by the FBI for electronic surveillance and physical search conducted under Titles I and III of FISA, a judge of the FISC observed:

> FBI personnel who develop storage systems for FISA-acquired information and decide under what circumstances FISA-acquired information is placed on those systems are bound by applicable minimization procedures and FISC orders, no less so than an agent conducting a FISC-authorized physical search or an analyst preparing a report for dissemination.

Docket No. [redacted], Opinion and Order at 45 (FISA Ct. May 17, 2016). Recent disclosures regarding [redacted] systems maintained by the FBI suggest that raw FISA

[69] The improper access granted to the [redacted] contractors was apparently in place [redacted] and seems to have been the result of deliberate decisionmaking. [redacted] Compliance Report at 92-93 ([redacted] access to FBI systems was the subject of an interagency memorandum of understanding entered into [redacted]). Despite the existence of an interagency memorandum of understanding (presumably prepared or reviewed by FBI lawyers), no notice of this practice was given to the FISC until 2016. Of course, such a memorandum of understanding could not override the restrictions of Section 702 minimization procedures.

information, including Section 702 information, may be retained on those systems in violation of applicable minimization requirements. [redacted][70]



The government has not identified the provisions of the FBI Minimization Procedures it believes are implicated by the above-described retention practices. Based on the information

[70] [redacted]

provided, however, those practices appear inconsistent with the provisions governing retention on electronic and data storage systems, see FBI Minimization Procedures § III.G.1, on ad hoc systems, id. § IV.A-B, and in connection with litigation, id. § III.G.4. Nearly four months ago, the government undertook to address this indefinite retention of information on the above-described systems in a subsequent filing, see December 29, 2016 Report at 10-11, but has not done so. Accordingly, the Court is directing the government to provide pertinent information, as described below.

3. Review Teams for Attorney-Client Communications

The Section 702 minimization procedures

> have specific rules for handling attorney-client communications. Because the FBI has law enforcement responsibilities and often works closely with prosecutors in criminal cases, its procedures have detailed requirements for cases in which a target is known to be charged with a federal crime. Unless otherwise authorized by the [National Security Division of DOJ], the FBI must establish a separate review team whose members have no role in the prosecution of the charged criminal matter to conduct the initial review of such a target's communications. When that review team identifies a privileged communication concerning the charged criminal matter, the original record or portion thereof containing that privileged communication is sequestered with the FISC and other copies are destroyed (save only any electronic version retained as an archival backup, access to which is restricted).

November 6, 2015 Opinion at 47-48 (citations and internal quotation marks omitted).

Failures of the FBI to comply with this "review team" requirement for particular targets have been a focus of the FISC's concern since 2014. See id. at 48-52; August 26, 2014 Opinion at 35-36. The government generally ascribed those failures to misunderstanding or confusion on the part of individuals – for example, when an agent is generally aware of the review team requirement but mistakenly believes that it does not apply when the charging instrument is under

seal. November 6, 2015 Opinion at 50. The government advised that it was emphasizing the review team requirement in ongoing training and oversight efforts, and that such emphasis had resulted in the identification and correction of additional cases in which review teams had not been properly established. Id. at 51.

[redacted] targets who have been subject to criminal charges [redacted] there was a delay of over two years in establishing review teams. See [redacted] Preliminary Notice of Compliance Incident Regarding [redacted] Section 702-Tasked Facilities ("[redacted] Preliminary Notice") at 2-3. The primary cause of this delay was that the responsible case agent was unaware of the review team requirement. That agent took the appropriate steps after reviewing an advisory that reminded FBI personnel about the requirement in [redacted] Id. at 3.[71] The government also reported a delay of approximately one month during [redacted] before establishing a review team after a target was charged in a sealed complaint. The delay appears to have been the result of lack of coordination among FBI field offices. According to the government, the review teams have completed examination of communications acquired prior to

[71] [redacted]

their creation for both incidents and did not discover any privileged communications. [redacted] [redacted] Compliance Report at 77, 105.

In addition, the government reported [redacted]

[redacted]

A separate source of under-inclusiveness is when personnel do not identify and segregate communications for [redacted]

[redacted] FBI examination of the erroneously-excluded communications is ongoing and, so far, has not identified any attorney-client privileged communications concerning a charged matter. [redacted] Compliance Report at 119.

A different [redacted] problem affected [redacted] accounts during November 28-30, 2016. That problem has been solved prospectively. Although some communications for

those tasked accounts were accessed before being segregated for the review team, none of them contained privileged information. Id. at 83 n.58.

In order to address some of the sources of such under-inclusiveness, the FBI has implemented a new [redacted] process for [redacted] In addition, the FBI and NSA have taken steps to address the difficulties encountered with regard to [redacted] Id. at 4.

It seems clear that the review team requirement should continue to be a point of emphasis in the government's training and oversight efforts. The measures taken to improve processes for identifying and routing information subject to the review team requirement appear well-suited to address the described under-inclusiveness problems. In view of those efforts, and the fact that lapses to date appear to have resulted in few, if any, privileged communications concerning charged matters being reviewed by investigators other than review team members, errors in implementing the review team requirements do not preclude a finding that the FBI Minimization Procedures meet the statutory definition of "minimization procedures" and are consistent with the requirements of the Fourth Amendment.

E. Issues Arising Under the CIA Minimization Procedures

In the course of investigating a separate compliance incident that occurred in December 2016,[72] the CIA discovered several problems with its purge practices. First, the software script used to identify communications subject to purge requirements within a storage system [redacted] had not been identifying all communications subject to purge that had been acquired by [redacted] December 28, 2016, Preliminary Notice of Compliance Incidents and Material Misstatements Regarding Collection Pursuant to Title I and Title III and Section 702 of FISA, at 4. As of March 29, 2017, CIA was in the process of remedying the incomplete purges. Supplemental Notice Regarding Incomplete Purges of Collection Acquired Pursuant to Section 702 of FISA, filed on March 29, 2017 ("March 29, 2017 Supp. Notice") at 2.

Further investigation of the December 2016 incident revealed similar problems with scripts used to purge metadata from [redacted] CIA repositories [redacted]. March 29, 2017 Supp. Notice at 2-3. The government reports CIA has corrected those script problems and completed the required purges, except for certain information relating [redacted] facilities, for which remedial efforts are ongoing. Id. at 3 & n.4.

[72] That incident appears to have been remedied, see id. at 3, and in and of itself does not merit discussion in this Opinion.

[73] [redacted]

In late March 2017, also in the course of investigating the December 2016 incident, CIA discovered another form of purging error affecting [redacted] March 24, 2017, Notice of Compliance Incident Regarding Incomplete Age Off of Data Acquired Pursuant to Section 702 of FISA at 2. The government is examining the scope of that error. Id.

The government has not advised the Court for how long these various purge-related problems persisted before CIA discovered them in the course of investigating the separate incident. It appears that, having recognized the problems, CIA is taking reasonable steps to address them. Nonetheless, the Court encourages the government to take proactive measures to verify that the automated processes upon which it relies to implement minimization requirements are functioning as intended.

V. CONCLUSION

For the foregoing reasons, the Court finds that: (1) the 2016 Certifications, as amended by the 2017 Amendments, as well as the certifications in the Prior 702 Dockets as amended by those documents, contain all the required statutory elements; (2) the targeting and minimization procedures to be implemented regarding acquisitions conducted pursuant to the 2016 Certifications, as amended by the 2017 Amendments, comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment; and (3) the minimization procedures to be implemented regarding information acquired under prior Section 702 certifications comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment. Orders approving the amended certifications and use of the accompanying procedures are being entered contemporaneously herewith.

For the reasons discussed above, it is HEREBY ORDERED as follows:

1. Raw information obtained by NSA's upstream Internet collection under Section 702 shall not be provided to FBI, CIA or NCTC unless it is done pursuant to revised minimization procedures that are adopted by the AG and DNI and submitted to the FISC for review in conformance with Section 702.

2. The government shall take steps to ensure that NCTC retains raw Section 702-acquired information that is determined to be evidence of a crime but not foreign intelligence information beyond the generally applicable age-off period specified in Section B.2 of the NCTC Minimization Procedures only as long as reasonably necessary to serve a law enforcement purpose and that NCTC does not use or disclose such information other than for a law enforcement purpose. The government shall report in writing on such steps when it seeks to renew or amend [redacted].

3. On or before December 31 of each calendar year, the government shall submit a written report to the FISC: (a) describing all administrative, civil or criminal litigation matters necessitating preservation by FBI, NSA, CIA or NCTC of Section 702-acquired information that would otherwise be subject to destruction, including the docket number and court or agency in which such litigation matter is pending; (b) describing the Section 702-acquired information preserved for each such litigation matter; and (c) describing the status of each such litigation matter.

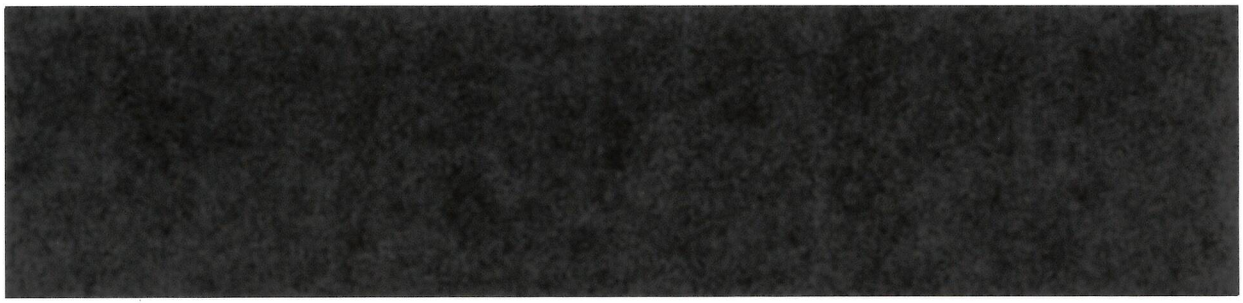
4. The government shall promptly submit a written report describing each instance in which FBI, NSA, CIA or NCTC invokes the provision of its minimization procedures stating that

nothing in those procedures shall prohibit the "retention, processing, analysis or dissemination of information necessary to comply with a specific congressional mandate or order of a court within the United States[.]" See NSA Minimization Procedures § 1; CIA Minimization Procedures § 6.g; FBI Minimization Procedures § I.G; NCTC Minimization Procedures § A.6.d. Each such report shall describe the circumstances of the deviation from the procedures and identify the specific mandate on which the deviation was based.

5. The government shall promptly submit a written report describing any instance in which an agency departs from any provision in its minimization procedures in reliance in whole or in part on the provision therein for lawful oversight when responding to an oversight request by an entity other than the oversight entities expressly referenced in the agency's procedures. See NSA Minimization Procedures § 1; CIA Minimization Procedures § 6.f; FBI Minimization Procedures § I.G; NCTC Minimization Procedures § A.6.e. Each such report shall describe the circumstances of the deviation from the procedures and identify the specific oversight activity on which the deviation was based.

6. No later than June 16, 2017, the government shall submit a written report:

(a) describing the extent to which raw FISA information, including Section 702 information, is retained:



(b) assessing whether such retention complies with applicable minimization requirements; and

(c) to the extent that noncompliance is found, describing the steps the government is taking or plans to take to discontinue the above-described forms of retention or bring them into compliance with applicable minimization requirements.

7. No later than June 16, 2017, the government shall submit one or more written reports that provide the following:

(a) the results of the government's investigation of whether there have been additional cases in which the FBI improperly afforded non-FBI personnel access to raw FISA-acquired information on FBI systems; and

(b) a description of the installation of the [redacted] by [redacted] personnel on an FBI system, including:

[redacted]

8. At 90-day intervals, the government shall submit written updates on NSA's implementation of the above-described sequester-and-destroy process to information acquired on or before March 17, 2017, by upstream Internet collection under Section 702.

9. If the government intends not to apply the above-described sequester-and-destroy process to information acquired on or before March 17, 2017, by upstream Internet collection

under Section 702 because the information is not contained in an "institutionally managed repository," it shall describe the relevant circumstances in a written submission to be made no later than June 2, 2017; however, the government need not submit such a description for circumstances referenced in this Opinion and Order as ones in which NSA could retain such information.

10. The government shall promptly submit in writing a report concerning each instance in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information. The report should include a detailed description of the information at issue and the manner in which it has been or will be used for analytical, investigative or evidentiary purposes. It shall also identify the query terms used to elicit the information and provide the FBI's basis for concluding that the query was consistent with applicable minimization procedures.

ENTERED this 26 day of April, 2017, in Docket Nos. [redacted].

ROSEMARY M. COLLYER
Judge, United States Foreign
Intelligence Surveillance Court

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

[redacted]