Approved for public release by the ODNI 20160415

Filed
United States Foreign
Intelligence Surveillance Court

NOV 0 6 2015

LeeAnn Flynn Hall, Clerk of Court

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

MEMORANDUM OPINION AND ORDER

This matter is 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 July 15, 2015 ("July 15, 2015 Submission"). For the reasons explained below, the government's request for approval is granted, subject to certain reporting requirements. The Court's approval of the certifications, amended certifications, and accompanying targeting procedures and minimization procedures is set out in a separate order that is being entered contemporaneously herewith.

Approved for public release by the ODNI 20160415

I. BACKGROUND

A. The 2015 Certifications

The July 15, 2015 Submission includes [redacted] certifications that have been executed by the Attorney General ("AG") and the Acting Director of National Intelligence ("DNI") pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which is codified at 50 U.S.C. § 1881a: [redacted] Each of the [redacted] certifications (collectively referred to as "the 2015 Certifications") is accompanied by the supporting affidavits of the Director of the National Security Agency ("NSA"), the Director of the Federal Bureau of Investigation ("FBI"), and the Director of the Central Intelligence Agency ("CIA"); two sets of targeting procedures, for use by the NSA and FBI respectively;[1] and four sets of minimization procedures, for use by the NSA, FBI, CIA, and the National Counterterrorism Center ("NCTC"), respectively.[2] The July 15, 2015 Submission also includes an explanatory memorandum prepared by the Department of Justice

[1] The targeting procedures for each of the 2015 Certifications are identical. The targeting procedures for the NSA ("NSA Targeting Procedures") appear as Exhibit A to each of the 2015 Certifications. The targeting procedures for the FBI ("FBI Targeting Procedures") appear as Exhibit C to each of the 2015 Certifications.

[2] The minimization procedures for each of the 2015 Certifications are identical. The minimization procedures for the NSA ("NSA Minimization Procedures") appear as Exhibit B to each of the 2015 Certifications. The minimization procedures for the FBI ("FBI Minimization Procedures") appear as Exhibit D to each of the 2015 Certifications. The minimization procedures for the CIA ("CIA Minimization Procedures") appear as Exhibit E to each of the 2015 Certifications. The minimization procedures for the NCTC ("NCTC Minimization Procedures") appear as Exhibit G to each of the 2015 Certifications.

Approved for public release by the ODNI 20160415

("DOJ") ("July 15, 2015 Memorandum"). Finally, it includes an unclassified summary of DOJ and DNI oversight of Section 702 implementation, and a summary of "notable Section 702 requirements," which have been submitted to the Court in accordance with the recommendation of the Privacy and Civil Liberties Oversight Board ("PCLOB"). See July 15, 2015 Memorandum at Tabs 1 and 2; see also PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act at 142-43 (July 2, 2014) ("PCLOB Report") (Recommendation 5).

Each of the 2015 Certifications involves "the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information."

Approved for public release by the ODNI 20160415

[redacted]

Each of the 2015 Certifications generally proposes to continue acquisitions of foreign intelligence information that are now being conducted under certifications that were made in 2014 ("the 2014 Certifications"). See July 15, 2015 Memorandum at 2. The 2014 Certifications, [redacted] were approved by the FISC on August 26, 2014.[3] The 2014 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.[4] In its July 15, 2015 Submission, the government also seeks approval of amendments to the certifications in all of the Prior 702 Dockets, such that the NSA, CIA, and FBI henceforward will apply the same minimization procedures to information obtained under prior certifications as they will to information to be obtained under the 2015 Certifications. See July 15 Memorandum at 2-3; [redacted][5]

[3] See [redacted] Memorandum Opinion and Order entered on August 26, 2014 ("August 26, 2014 Opinion").

[4] See [redacted] These dockets, [redacted] are collectively referred to as "the Prior 702 Dockets").

[5] The July 15, 2015 Submission does not propose any changes to the FBI Targeting Procedures or NCTC Minimization Procedures. See July 15, 2015 Memorandum at 3.

Approved for public release by the ODNI 20160415

B. The Extension of Time and the Appointment of Amicus Curiae

Before making the July 15, 2015 Submission, the government filed draft versions of the 2015 Certifications on June 15, 2015. After reviewing those drafts, the Court concluded "that this matter is likely to present one or more novel or significant interpretations of the law, which would require the Court to consider appointment of an amicus curiae" under 50 U.S.C. § 1803(i)(2). See Order issued on July 7, 2015 ("July 7, 2015 Order"), at 3. The Court further noted that the 30-day review period specified by 50 U.S.C. § 1881a(i)(1)(B) would, as a practical matter, foreclose amicus participation. Id. The Court may, however, extend that 30-day review period "as necessary for good cause in a manner consistent with national security." 50 U.S.C. § 1881a(j)(2).

To help the Court decide "whether to extend the time it would have to act on the 2015 Certifications and revised procedures in order to allow for meaningful amicus assistance in reviewing them," the Court ordered the government to "explain in writing whether – and if so, how long – an extension of the time for the Court to review the 2015 Certifications and revised procedures would be consistent with national security." July 7, 2015 Order at 4. On July 14, 2015, the Government timely filed its Response to the July 7, 2015 Order, advising that "the government assesses that an extension of 60 to 90 days . . . would be consistent with national security." See Government's Response to the Court's Order of July 7, 2015, filed on July 14, 2015, at 7.

On July 23, 2015, the Court found that "the need for an extension to allow for [amicus] participation constitutes 'good cause'" for an extension under Section 1881a(j)(2). See Order

Approved for public release by the ODNI 20160415

issued on July 23, 2015, at 3. Accordingly, it extended "the period for Court review under [Section 1881a(i)(1)(B)] for 90 days, such that this review must be completed no later than November 12, 2015." Id.

On August 13, 2015, the Court issued an order appointing Amy Jeffress to serve as amicus curiae in this matter pursuant to 50 U.S.C. § 1803(i)(2)(B).[6] The Court directed Ms. Jeffress to address whether the minimization procedures accompanying the 2015 Certifications meet the requirements of 50 U.S.C. § 1881a(e) and are consistent with the Fourth Amendment, see id. § 1881a(i)(3)(A), in view of the provisions of the procedures that apply to:

> (i) queries of information obtained under section 702, particularly insofar as queries may be designed to return information concerning United States persons, see NSA Minimization Procedures at 7, FBI Minimization Procedures at 11-12, and CIA Minimization Procedures at 3-4; and
>
> (ii) preservation for litigation purposes of information otherwise required to be destroyed under the minimization procedures, see NSA Minimization Procedures at 8-9, FBI Minimization Procedures at 24-25, and CIA Minimization Procedures at 10-11.

Thereafter, the Court issued an order directing Ms. Jeffress and the government to submit briefs on these issues no later than October 16, 2015. See Briefing Order issued on September 16, 2015, at 4. After both briefs were timely filed, the Court received oral argument from the

[6] The Court wishes to thank Ms. Jeffress for her exemplary work in this matter. Her written and oral presentations were of the highest quality and extremely informative to the Court's consideration of this matter. The Court is grateful for her willingness to serve in this capacity.

Approved for public release by the ODNI 20160415

amicus and counsel for the government on October 20, 2015.[7]

C. Review of Compliance Issues

FISC 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., [redacted], Memorandum Opinion entered on April 7, 2009, at 22-24 ("April 7, 2009 Opinion"); [redacted], and [redacted], Memorandum Opinion entered on Aug. 30, 2013, at 6-11 ("August 30, 2013 Opinion"). Accordingly, for purposes of its review of the July 15, 2015 Submission, the Court has examined quarterly compliance reports submitted by the government[8] since the most recent FISC review of Section 702 certifications and procedures was completed on August 26, 2014, as well as individual notices of non-compliance relating to implementation of Section 702. Based on its review of these submissions, the Court, through its staff, orally conveyed a number of compliance-related questions to the government. On October 8, 2015, the Court conducted a hearing to address some of the same compliance-related questions ("October 8 Hearing").

II. REVIEW OF CERTIFICATIONS [redacted] AND OF THEIR PREDECESSOR CERTIFICATIONS AS AMENDED BY THE JULY 15, 2015 SUBMISSION.

The Court must review a certification submitted pursuant to Section 702 "to determine

---

[7] See generally Transcript of Proceedings Held Before the Honorable Thomas F. Hogan on October 20, 2015 ("October 20 Transcript").

[8] See Quarterly Reports to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on December 19, 2014, March 20, 2015, June 19, 2015, and September 19, 2015.

Approved for public release by the ODNI 20160415

whether [it] contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). The Court's examination of Certifications [redacted] confirms that:

(1) the certifications have been made under oath by the AG and the Acting DNI,[9] 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;

(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 August 14, 2015, or on the date upon which this Court issues an order concerning the certification under Section 1881a(i)(3), whichever is later, see [redacted]

---

[9] The 2015 Certifications were made by the Attorney General and Michael P. Dempsey, the Deputy DNI for Intelligence Integration. At the time, Mr. Dempsey was serving as Acting DNI pursuant to a Presidential Memorandum dated September 20, 2013. That Memorandum, which was issued pursuant to the Federal Vacancies Reform Act of 1998, as amended, 5 U.S.C. § 3345, et seq., provides that the Deputy DNI for Intelligence Integration "shall act as and perform the functions and duties of the [DNI] during any period in which the DNI and the Principal Deputy Director of National Intelligence have died, resigned, or otherwise become unable to perform the functions and duties of the DNI." See Presidential Memorandum, "Designation of Officers of the Office of the Director of National Intelligence [("ODNI")] to Act as Director of National Intelligence," 78 Fed. Reg. 59,159 (Sept. 20, 2013).

[10] See Affidavits of Admiral Michael S. Rogers, United States Navy, Director, NSA ([redacted]); Affidavits of James B. Comey, Director, FBI ([redacted]); and Affidavits of John O. Brennan, Director, CIA ([redacted]).

Approved for public release by the ODNI 20160415

[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 2015 Certifications, and finds that they also contain all the elements required by the statute. Id.[12]

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.

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

---

[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 2015 Certifications. See [redacted].

Approved for public release by the ODNI 20160415

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." See NSA Targeting Procedures at 1, 3-4, 7; FBI Targeting Procedures at 1-4. 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").

Section 1881a(e)(1) requires minimization procedures that "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4)]." The applicable statutory definition is fully set out at pages 12-14 below.

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

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 email address. The FBI Targeting Procedures come into play in cases where the government [redacted] that has been tasked under the NSA Targeting Procedures. See FBI Targeting Procedures at 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).

Approved for public release by the ODNI 20160415

The NSA Targeting Procedures included as part of the July 15, 2015 Submission contain two revisions, neither of which raises any concern. Both changes concern the requirement that, before tasking a selector for collection under Section 702, NSA first assess that the target is expected to possess or receive, or is likely to communicate, foreign intelligence information concerning a foreign power or a foreign territory. See NSA Targeting Procedures at 4. The first change consists of new language clarifying that such assessments must be "particularized and fact-based" and must consider the "totality of the circumstances." See id. The new language, which was added following a recommendation of the PCLOB, see PCLOB Report at 134-35 (Recommendation 1), results in no change in practice, as NSA has interpreted prior versions of the procedures to require the same particularized, fact-based assessments of the totality of the circumstances. See July 15, 2015 Memorandum at 5-6.

The second change, made in response to the same PCLOB recommendation, is the addition of language requiring NSA analysts to document each such foreign intelligence assessment. New language requires NSA analysts to "provide a written explanation of the basis for their assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning [the] foreign power or foreign territory" about which they expect to obtain foreign intelligence information pursuant to a particular targeting determination. See NSA Targeting Procedures at 8. This change, which will facilitate review and oversight of NSA targeting decisions, presents no issue under Section 1881a(d)(1).

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the

Approved for public release by the ODNI 20160415

Court concludes that the NSA Targeting Procedures and the FBI Targeting Procedures,[13] as written, are reasonably designed, as required by Section 1881a(d)(1): (1) to ensure that any acquisition authorized under the 2015 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 of whether those procedures are consistent with the requirements of the Fourth Amendment. See pages 36-45 below.

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

The FBI, NSA, and CIA all have access to "raw," or unminimized, information obtained under Section 702. Each agency is governed by its own set of 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 included as part of the July 15, 2015 Submission meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) or 1821(4), as appropriate. Sections 1801(h) and 1821(4) define "minimization

[13] The Court has already concluded that procedures identical to the FBI Targeting Procedures included as part of the July 15, 2015 Submission comply with the applicable statutory requirements. See August 26, 2014 Opinion at 12-14. There is no basis for the Court to deviate from that conclusion here.

Approved for public release by the ODNI 20160415

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;[14]
>
> (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[.]

---

[14] 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 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.

Approved for public release by the ODNI 20160415

50 U.S.C. § 1801(h); see also id. § 1821(4).[15]

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

In 2014, the Court 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. Access to information retained under these provisions is tightly restricted. See id. at 21, 23. The revised NSA and CIA Minimization Procedures accompanying the 2015 Certifications contain revisions to these "litigation hold" provisions.

The litigation hold provisions currently in effect allow NSA and CIA to retain specific Section 702-acquired information that is otherwise subject to age-off[16] if DOJ has advised either agency in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. See id. at 22-23. Those provisions also recognize that litigation preservation obligations can also apply to Section 702-acquired information that is subject to destruction for reasons other than the age-off requirements of the procedures – e.g., domestic communications subject to destruction under Section 5 of the NSA

[15] The definitions of "minimization procedures" set forth in these provisions are substantively identical (although Section 1821(4)(A) refers to "the purposes . . . of the particular physical search") (emphasis added). For ease of reference, subsequent citations refer only to the definition set forth at Section 1801(h).

[16] For example, the NSA generally may not retain telephony and certain forms of Internet communications for "longer than five years from the expiration date of the certification authorizing the collection" unless the NSA determines that certain specified retention criteria are met. See NSA Minimization Procedures at 7. The CIA Minimization Procedures contain a similar requirement. See CIA Minimization Procedures at 2.

Approved for public release by the ODNI 20160415

Minimization Procedures. See id. at 23-24. When such circumstances arise, the provisions currently in effect state that "'the Government will notify the [FISC] and seek permission to retain the material as appropriate [and] consistent with the law.'" See id. (quoting 2014 procedures). The Court encouraged the government to consider further revision of the procedures to address such circumstances with generally applicable rules rather than on a piecemeal basis. See id. at 24.

In response to this suggestion, the government has modified the language in the NSA and CIA Minimization Procedures [redacted]

[redacted]

[redacted]

Approved for public release by the ODNI 20160415

[redacted]

The Court agrees with amicus curiae Amy Jeffress that the revised litigation hold provisions comport with the requirements of Section 1801(h) and strike a reasonable and appropriate balance between the retention limitations reflected in FISA and the government's need to comply with its litigation-related obligations. See Brief of Amicus Curiae submitted on October 16, 2015, at 28-34 ("Amicus Brief").

2. Provisions Restricting the Retention and Use of Section 702-Acquired Information Subject to the Attorney-Client Privilege

The revised FBI, NSA and CIA Minimization Procedures all include modifications to the provisions restricting the use and dissemination of attorney-client communications that are acquired pursuant to Section 702. The FBI Minimization Procedures include three such changes. The procedures currently in effect include a provision permitting the FBI, after providing the

[redacted]

Approved for public release by the ODNI 20160415

original copy of an attorney-client communication to DOJ for sequestration with this Court and destroying other copies, to maintain a back-up copy that is subject to strict access controls. See August 26, 2014 Opinion at 35. The first change to the FBI procedures clarifies that system administrators and technical personnel may have access to such backup copies, but not for analytical or operational purposes. See FBI Minimization Procedures at 14. The second change consists of the addition of language requiring the FBI's Office of General Counsel to approve all disseminations that include attorney-client privileged communications. See id. at 17. The new language requires that before any such dissemination be made, reasonable efforts be undertaken to instead use other, non-privileged sources of information, and to tailor each dissemination to minimize or eliminate the disclosure of attorney-client privileged information. See id. at 17-18. The third change is the addition of a requirement that all disseminations of attorney-client privileged communications include language to advise recipients that the dissemination contains information subject to the attorney-client privilege, that the information is being disseminated "solely for intelligence or lead purposes," and that it may not be further disseminated or used in any trial, hearing, or other proceeding without approval of the AG or the Assistant AG for National Security. See id. at 18.

The provisions of the NSA and CIA Minimization Procedures concerning attorney-client communications also have been modified. The revised language requires, 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 NSA Minimization Procedures at 10; CIA Minimization Procedures at 5. [redacted]

Approved for public release by the ODNI 20160415



Moreover, dissemination of privileged information must contain an appropriate caveat to protect the information from being used in a legal proceeding in the United States. See NSA Minimization Procedures at 11; CIA Minimization Procedures at 7.

The revisions to the provisions of the FBI, NSA, and CIA Minimization Procedures concerning attorney-client communications serve to enhance the protection of privileged information. The Court is satisfied that the changes present no concern under Section 1801(h).

3. Provisions of the FBI Minimization Procedures Permitting the Retention of Back-up Copies and Encrypted Information

The government has added new language to the FBI Minimization Procedures to permit the retention of Section 702-acquired information in "backup and original evidence systems."

Approved for public release by the ODNI 20160415

See FBI Minimization Procedures at 24. Only systems administrators and technical personnel may have access to such systems and data in them may not be viewed or used for the purpose of intelligence analysis. See id. Backup and original evidence systems are used to preserve copies of Section 702-acquired data in the form it was originally acquired. See July 15, 2015 Memorandum at 16. Such unaltered copies are unreadable without additional processing but can be used in case of emergency "to restore lost, destroyed, or inaccessible data," or to create an "original evidence copy" for evidentiary uses (e.g., to establish chain of custody in connection with a criminal prosecution or to fulfill the government's criminal discovery obligations, see id. at 16-17). See FBI Minimization Procedures at 24. In the event backup and original evidence systems are used to restore lost, destroyed, or inaccessible data, the FBI must apply its minimization procedures, including any applicable time limits on retention, to the restored data. See id.

The government has also 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. See id. at 25. Access to such information is restricted to FBI personnel engaged in cryptanalysis or deciphering secret meaning. See id. 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-

Approved for public release by the ODNI 20160415

applicable retention restrictions of the procedures apply, though the government has stated that it will calculate the age-off date from the later of the date of decryption or the date of expiration of the certification pursuant to which the information was acquired. See July 15, 2015 Memorandum at 18.[19]

Neither of these new provisions precludes the Court from finding that the FBI Minimization Procedures comport with Section 1801(h). Both are narrowly tailored to serve legitimate government interests in a manner that appropriately protects nonpublicly available information concerning unconsenting United States persons.

4. Reporting Requirement for Disseminations to Private Entities or Individuals

The version of the FBI Minimization Procedures that was approved by the Court in 2014 provides that "'information that reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime'" may be disseminated to "'a private individual or entity in situations where the FBI determines that said private individual or entity is capable of providing assistance in mitigating serious economic harm or serious harm to life or property.'" See August 26, 2014 Opinion at 19 (quoting 2014 FBI Minimization Procedures at 33). Whenever reasonably practicable, such disseminations must not include information identifying a United States person "'unless the FBI reasonably believes it is necessary to enable the recipient to assist in the mitigation or prevention of the harm.'" See id. (quoting 2014 FBI Minimization Procedures at 33). Such disseminations

[19] To avoid confusion regarding the applicable age-off requirements, the government is encouraged to make this calculation methodology explicit in future versions of the procedures.

Approved for public release by the ODNI 20160415

must be reported to DOJ within ten business days. See id. The government has retained the foregoing language but added language requiring that disseminations pursuant to this provision also promptly be reported to the FISC. See FBI Minimization Procedures at 37. This modification does not alter the Court's conclusion that this provision of the procedures is consistent with the requirements of Section 1801(h). See August 26, 2014 Opinion at 20.

5. Provisions Permitting Compliance with Specific Constitutional, Judicial or Legislative Mandates

The NSA and CIA Minimization Procedures included as part of the July 15, 2015 Submission each contain new language stating 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 NSA Minimization Procedures at 1; CIA Minimization Procedures at 4-5. These provisions were not included in the draft procedures that were submitted to the Court in June 2015, but appear to have been added by the government thereafter. They are not discussed in the July 15, 2015 Memorandum.

The apparent breadth of these new provisions gives the Court pause. As discussed above, the applicable definition of "minimization procedures" requires, inter alia, "specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1) (emphasis added). In light of this requirement, the NSA

Approved for public release by the ODNI 20160415

and CIA Minimization Procedures contain page after page of detailed restrictions on the acquisition, retention, and dissemination, of Section 702-acquired information concerning United States persons. A provision that would allow the NSA and CIA to deviate from any of these restrictions based upon unspecified "mandates" could undermine the Court's ability to find that the procedures satisfy the above-described statutory requirement.

It appears, however, that the government does not intend to apply these provisions as broadly as their language would arguably permit. In 2012, the government proposed a similar provision as part of minimization procedures to be applied by NCTC in handling certain unminimized terrorism-related information acquired by FBI pursuant to other provisions of FISA. In requesting approval of a provision that would allow NCTC personnel to deviate from other requirements of its minimization procedures when "reasonably necessary to comply with specific constitutional, judicial, or legislative mandates," the government asserted that "Executive Branch orders or directives will not trigger this provision, nor will general Congressional directives that are not specific to information NCTC receives pursuant to this motion." See [redacted], Government's Submission of Amendments to Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under FISA and Submission of Revised Minimization Procedures for the NCTC, submitted on April 23, 2012, at 31-32. The Court approved the NCTC minimization procedures with the understanding that this provision would be applied sparingly. The Court described the provision as permitting NCTC personnel to "retain, process or disseminate information when reasonably necessary to fulfill specific legal requirements" and compared it to

Approved for public release by the ODNI 20160415

a more narrowly-drafted provision of separate procedures that permits CIA to retain or disseminate information that is "required by law to be retained or disseminated." [redacted]. Memorandum Opinion and Order issued on May 18, 2012, at 11 (emphasis added).

The Court understands based on informal communications between the Court staff and attorneys for the government that NSA and CIA intend to apply the similar provisions at issue here in the same narrow manner. In any case, to avoid a deficiency under the above-described definition of "minimization procedures," the Court 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. Such clear and specific language, for instance, might be found in a court order requiring the government to preserve a particular target's communications beyond the date when they would otherwise be subject to age-off under the minimization procedures. On the other hand, these provisions should not be interpreted as permitting an otherwise prohibited retention or use of information simply because that retention or use could assist the government in complying with a general statutory requirement, such as those stated at 50 U.S.C. § 1881a(b). To ensure that these provisions are being applied in a manner consistent with the Court's understanding, the government will be directed to promptly report any use thereof to the Court in writing, along with a written justification for each such

Approved for public release by the ODNI 20160415

action. See page 78 below.[20]

6. Provisions Concerning Queries of Information Acquired Through Collection Under Section 702

Finally, the NSA, CIA, and FBI Minimization Procedures included as part of the July 15, 2015 Submission all include revised provisions concerning queries of unminimized data acquired pursuant to Section 702. The previously-approved minimization procedures for all three agencies permit appropriately-trained personnel with access to Section 702-acquired information to query repositories containing such information, subject to certain restrictions. See PCLOB Report at 55. The terms used to conduct such queries may in some circumstances include information concerning United States persons or otherwise be expected to return information about a United States person. See id. at 55-60.

a. *NSA and CIA querying provisions*

The NSA and CIA Minimization Procedures accompanying the 2015 Certifications contain several important restrictions that have been carried forward from prior versions of the procedures. Most notably, all terms used to query the contents of communications acquired through Section 702, such as phone numbers or key words, must be terms "reasonably likely to return foreign intelligence information." See NSA Minimization Procedures at 7; CIA Minimization Procedures at 3. This requirement applies to all queries of Section 702-acquired

[20] The Court understands that the government may have added these new provisions to clarify that information acquired under Section 702 may be shared with Members of Congress or Congressional committees in connection with Congressional oversight of the program. If so, the Court would urge the government to consider replacing these broadly-worded provisions with language that is narrowly tailored to that purpose.

Approved for public release by the ODNI 20160415

contents, not just queries containing United States-person identifiers. See NSA Minimization Procedures at 7; CIA Minimization Procedures at 3. Further, the NSA and CIA Minimization Procedures continue to require that both agencies maintain records of all United States-person identifiers that are used to query Section 702 data and that such records be made available for mandatory review by DOJ and ODNI. See NSA Minimization Procedures at 7; CIA Minimization Procedures at 3.[21]

In addition, the NSA and CIA Minimization Procedures accompanying the 2015 Certifications now also mandate that NSA and CIA prepare "a statement of facts establishing that the use of any [United States-person] identifier as a selection term is reasonably designed to return foreign intelligence information as defined in FISA," see NSA Minimization Procedures at 7; CIA Minimization Procedures at 3. Like the records referred to above, these written justifications are provided to DOJ and ODNI to facilitate their oversight of NSA and CIA queries. See July 15, 2015 Memorandum at 20-21.[22]

---

[21] The NSA Minimization Procedures also continue to preclude United States-person queries of its "upstream collection." See NSA Minimization Procedures at 7. Such collection includes Internet communications acquired through the assistance of providers that control the "backbone" over which Internet communications are carried and is more likely than other forms of Section 702 collection to contain information of or concerning United States persons with no foreign intelligence value. See [redacted] Memorandum Opinion entered on October 3, 2011, at 5 n.3, 33-41 ("October 3, 2011 Opinion"). Because only NSA receives "upstream collection," see id. at 18 n.17, CIA and FBI are unable to query information so acquired.

[22] Representatives of DOJ and ODNI conduct bi-monthly reviews at NSA and CIA to assess the agencies' compliance with the Section 702 targeting and minimization procedures. July 15, 2015 Memorandum, Tab 1 at 2, 4. As part of those reviews, those DOJ and ODNI representatives review all United States-person identifiers approved for use in querying the (continued...)

Approved for public release by the ODNI 20160415

These additional requirements will result in no change in practice, as NSA and CIA already prepare and record foreign intelligence justifications for each query, which are subsequently provided to DOJ and ODNI oversight personnel. Nevertheless, adding these documentation requirements to the NSA and CIA Minimization Procedures serves to further reduce the risk that Section 702-acquired information concerning United States persons will be used, or even accessed, for improper purposes. The Court agrees with the government and Ms. Jeffress[23] that the revised querying provisions of the NSA and CIA Minimization Procedures are consistent with the requirements of Section 1801(h).

b. *FBI querying provisions*

i. *Description of the FBI querying provisions*

The FBI Minimization Procedures also permit appropriately-trained personnel to conduct queries of systems containing Section 702 data. See FBI Minimization Procedures at 11 (queries of electronic and data storage systems); see id. at 28-29 (queries of ad hoc systems). In one respect, the queries permitted under the FBI's procedures are broader than those allowed by the NSA and CIA Minimization Procedures. Queries by FBI personnel of Section 702-acquired data

---

[22](...continued)
contents of Section 702-acquired communications as well as the written documentation of the foreign intelligence justifications for each such query. See id. at 3, 4. When necessary to assess compliance, additional information is requested by the oversight personnel and provided by NSA, and any compliance issues are promptly reported to the FISC. See id. at 3, 4.

[23] See Amicus Brief at 14 ("I conclude that the NSA and CIA minimization procedures are sufficient to ensure that the use of U.S. person identifiers for th[e] purpose of [querying Section 702-acquired information] complies with the statutory requirements of Section 702 and with the Fourth Amendment.").

Approved for public release by the ODNI 20160415

may be reasonably designed to "find and extract" either "foreign intelligence information" or "evidence of a crime." See id. at 11, 28-29. Both types of queries have been explicitly permitted by the FBI Minimization Procedures since 2009.[24] Unlike NSA and CIA, the FBI applies this standard to all queries of Section 702-acquired information, regardless of whether the querying term includes information concerning a United States person. See id.; see also Oct. 20 Transcript at 19-20.[25] The FBI also applies this standard regardless of whether the dataset being queried

[24] In [redacted], the Court approved FBI Minimization Procedures that incorporated by reference, as modified in a number of respects not relevant here, the "Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act" which were approved by the Attorney General on October 22, 2008 and submitted to this Court in [redacted] ("October 2008 SMPs"). See [redacted], Memorandum Opinion issued on April 7, 2009, at 14-17 ("April 7, 2009 Opinion"). Section III.D of the October 2008 SMPs permitted FBI personnel to use queries that were reasonably designed "to find and extract foreign intelligence information or evidence of a crime and to minimize the extraction of third-party information." See Oct. 2008 SMPs at 16.

[redacted]

[25] The FBI Minimization Procedures contain a general statement that, except for certain listed provisions, "these procedures do not apply to information concerning non-United States persons." FBI Minimization Procedures at 2. The querying provisions discussed in the text above are not among the listed exceptions. See id. Nevertheless, there are substantial quantities of information concerning United States persons within the Section 702 data subject to querying by the FBI, and it is impossible for FBI personnel to know beforehand whether or not United States-person information will be responsive to a given query of that data. Accordingly, the Court does not understand the above-described exception for "information concerning non-United States persons" to qualify the requirement that each query be reasonably designed to find and extract foreign intelligence information or evidence of a crime. In light of the FBI's practice

(continued...)

Approved for public release by the ODNI 20160415

includes the contents of communications or only metadata. See FBI Minimization Procedures at 11-12, 28-29. The FBI Minimization Procedures require that records be maintained of all queries of the Section 702 acquired data, and that such records include the term used in making each query. See id. at 11, 29. Unlike CIA and NSA, however, the FBI does not require its personnel to record their justifications for any queries. See id.

The government has added language to the querying provisions of the FBI Minimization Procedures to clarify that a search of an FBI storage system containing raw-FISA acquired information does not constitute a "query" within the meaning of the procedures if the user conducting the search does not receive access to unminimized Section 702-acquired information in response to the search. See id. at 11-12, 29.[26] In such cases, the query results include a notification that the queried dataset contains Section 702-acquired information responsive to the query. See id. at 12 n.4.

The new language also clarifies what actions an agent or analyst without appropriate training and access to Section 702 information may take upon receiving a positive "hit" indicating the existence of (but not access to) responsive information. See FBI Minimization Procedures at 12 n.4. Such a user may request that FBI personnel with Section 702 access rerun

---

[25](...continued)
of applying this standard to all queries of datasets including Section 702-acquired information, see October 20 Transcript at 20, the FBI also does not appear to consider the exception to apply in this regard.

[26] This can occur either because the user running the query has not been granted access to raw FISA-acquired information, or because a user who has been granted such access has chosen to limit the query such that it will not return raw FISA-acquired information. See FBI Minimization Procedures at 11-12, 29.

Approved for public release by the ODNI 20160415

the query if it otherwise would be authorized by the FBI Minimization Procedures and if the request is approved by both the user's supervisor and by a national security supervisor. See id. Generally speaking, the user without access to FISA-acquired information can be provided with access to information contained in the query results only if such information reasonably appears (based on the review of FBI personnel with authorized access to Section 702-acquired information) to be foreign intelligence information, to be necessary to understand foreign intelligence information, or to be evidence of a crime. See id. If it is "unclear," however, whether one of these standards is met, "the user, who does not otherwise have authorized access may review the query result solely in order to assist in the determination of whether information contained within the results meets those standards." Id. According to the government, such situations are "very rare." See October 20 Transcript at 45.

In addition, on the PCLOB's recommendation, see PCLOB Report at 137-38 (Recommendation 2), the government has added language to the querying provisions of the FBI Minimization Procedures to more fully describe the FBI's querying practices.[27] This language is

---

[27] Specifically, the procedures state:

> It is a routine and encouraged practice for the FBI to query databases containing lawfully acquired information, including FISA-acquired information, in furtherance of the FBI's authorized intelligence and law enforcement activities, such as assessments, investigations and intelligence collection. Section III.D governs the conduct of such queries. Examples of such queries include, but are not limited to, queries reasonably designed to identify foreign intelligence information or evidence of a crime related to an ongoing authorized investigation or reasonably designed queries conducted by FBI personnel in making an initial decision to open an assessment concerning a threat to the national security, the prevention or protection against a Federal crime, or the collection of foreign intelligence, as authorized by the Attorney General Guidelines. These examples

(continued...)

Approved for public release by the ODNI 20160415

descriptive and works no change to the applicable querying requirements or to the FBI's querying practices.[28]

ii. *Analysis of the FBI querying provisions*

Amicus curiae Amy Jeffress has raised concerns regarding the querying provisions of the FBI Minimization Procedures. See Amicus Brief at 18-28. Ms. Jeffress does not specifically assert that the querying provisions render the procedures inconsistent with the applicable statutory definition of minimization procedures. Nevertheless, she contends that the FBI Minimization Procedures "go far beyond the purpose for which the Section 702-acquired information is collected in permitting queries that are unrelated to national security." See id. at

---

[27](...continued)
are illustrative and neither expand nor restrict the scope of the queries authorized in the language above.

FBI Minimization Procedures at 11 n.4; see also id. at 28 n.8 (similar language).

[28] The FBI has adopted one policy change that is not reflected in its minimization procedures. The government has imposed additional limitations on the FBI's use of Section 702-acquired information in connection with non-foreign intelligence criminal matters. These limitations, which are reflected in the ODNI's Signals Intelligence Reform 2015 Anniversary Report, are described in the report as follows:

> [C]onsistent with the recommendation of the [PCLOB], information acquired under Section 702 about a U.S. person will not be introduced as evidence against that person in any criminal proceeding except (1) with the approval of the Attorney General, and (2) in criminal cases with national security implications or certain other serious crimes. This change will ensure that, if [DOJ] decides to use information acquired under Section 702 about a U.S. person in a criminal case, it will do so only for national security purposes or in prosecuting the most serious crimes.

Amicus Brief at 17 (quoting http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#section-702); see also id. at 18 (further describing policy).

Approved for public release by the ODNI 20160415

19. The Court respectfully disagrees.

There is no statutory requirement that all activities involving Section 702 data serve solely a foreign intelligence national security purpose. To be sure, Section 702 was enacted to permit "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a) (emphasis added). But even at the time of acquisition, the statute does not require the government to have as its sole purpose obtaining foreign intelligence information. Rather, the AG and DNI need certify only that obtaining foreign intelligence information is "a significant purpose" of the acquisition. See id. § 1881a(g)(2)(v) (emphasis added).[29] Under the "significant purpose" standard, an acquisition under Section 702 is permissible "even if 'foreign intelligence' is only a significant – not a primary – purpose" of the targeting decision. See In re Sealed Case, 310 F.3d 717, 734 (FISA Ct. Rev. 2002) (discussing 2001 amendment to Title I of FISA permitting government to conduct electronic surveillance based upon certification that obtaining foreign intelligence information is a "significant purpose of the surveillance").[30]

Nor does FISA foreclose any examination or use of information acquired pursuant to Section 702 that lacks a purpose relating to foreign intelligence. It is true that the government's

---

[29] As discussed above, each of the 2015 Certifications includes such an attestation of purpose. See [redacted]

[30] 50 U.S.C. § 1804 (a)(6)(b) – the substance of which appeared in subsection 1804(a)(7)(B) at the time of In re Sealed Case – requires that each application for an order approving electronic surveillance under FISA contain a certification by a high-level Executive Branch official that, among other things, "a significant purpose of the surveillance is to obtain foreign intelligence information."

Approved for public release by the ODNI 20160415

minimization procedures must be "reasonably designed in light of the purpose and technique of the [collection], to minimize the . . . retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information," 50 U.S.C. § 1801(h)(1) (emphasis added), and must limit the dissemination of nonpublicly available information identifying unconsenting United States persons to certain circumstances, see id. § 1801(h)(2). Notwithstanding these requirements, however, FISA states that the minimization procedures must also "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." Id. § 1801(h)(3). Hence, FISA does not merely contemplate, but expressly requires, that the government's procedures provide for the retention and dissemination of Section 702-acquired information that is evidence of crime for law enforcement purposes. This requirement applies whether or not the crime in question relates to foreign intelligence or national security. See In re Sealed Case, 310 F.3d at 731 (notwithstanding restrictions in subsections 1801(h)(1)-(2), subsection 1801(h)(3) permits "the retention and dissemination of non-foreign intelligence information which is evidence of *ordinary crimes* for preventative or prosecutorial purposes") (italics in original).

Ms. Jeffress acknowledges this statutory framework permits the retention and dissemination for law enforcement purposes of evidence of crimes that is discovered by queries of the Section 702-acquired data that are designed to find and extract foreign intelligence information. See October 20 Transcript at 10. She suggests, however, that it restricts queries of

Approved for public release by the ODNI 20160415

the unminimized data – in particular those that are predicated on United States-person information – that are designed to elicit information about crimes unrelated to foreign intelligence. See id. But this distinction finds no support in the statutory text. Nothing in the statute precludes the examination of information that has otherwise been properly acquired through application of the targeting procedures and retained under the minimization procedures for the purpose of finding evidence of crimes, whether or not those crimes relate to foreign intelligence.

It would be a strained reading of the definition of minimization procedures to permit FBI personnel to retain and disseminate Section 702 information constituting evidence of a crime implicating a United States person for law enforcement purposes, but to prohibit them from querying Section 702 data in a manner designed to identify such evidence. And such an interpretation would lead to anomalous results: FBI personnel who came across one communication acquired under Section 702 that incriminates a United States person – perhaps because it was responsive to a query for foreign intelligence information – would be prohibited from running queries tailored to identify additional communications obtained under Section 702 pertaining to the same criminal activity, even though Section 1801(h)(3) explicitly authorizes the retention and dissemination of such information for law enforcement purposes.

Finally, the Court respectfully disagrees with Ms. Jeffress' assertion that the FBI's querying practices run afoul of the Foreign Intelligence Surveillance Court of Review's admonition that "'the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.'" See Amicus Brief at 18 (quoting In re Sealed Case, 310 F.3d at 736)). The

Approved for public release by the ODNI 20160415

Court of Review made that statement in rejecting the government's contention that "even prosecutions of *non*–foreign intelligence crimes are consistent with a purpose of gaining foreign intelligence information so long as the government's objective is to stop espionage or terrorism by putting an agent of a foreign power in prison." See In re Sealed Case, 310 F.3d at 735-736 (italics in original). The Court of Review concluded that it would be an "anomalous reading" of the "significant purpose" language of 50 U.S.C. § 1804(a)(6)(B) to allow the use of electronic surveillance in such a case. See id. at 736. The Court nevertheless stressed, however, that "[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test." Id. at 735.

The FBI's use of queries designed to elicit evidence of crimes unrelated to foreign intelligence does not convert Section 702 acquisitions into "a device to investigate wholly unrelated ordinary crimes." The FBI's querying provisions apply only to information that has been acquired following application of the NSA Targeting Procedures. As discussed above, those targeting procedures require that before tasking a selector for collection, NSA first make a particularized assessment, based on the totality of the circumstances, that the user of the selector is expected to possesses or receive, or is likely to communicate, foreign intelligence information concerning a foreign power or a foreign territory. See NSA Targeting Procedures at 4. This requirement ensures that at least a significant purpose of each targeting decision under Section 702 is the acquisition of foreign intelligence information. Queries of the data acquired through application of this targeting process that are designed to elicit evidence of crimes unrelated to foreign intelligence are therefore consistent with the "significant purpose" language of Section

Approved for public release by the ODNI 20160415

1881a(g)(2)(A)(v).

Finally, it must be noted that the FBI Minimization Procedures impose substantial restrictions on the use and dissemination of information derived from queries that, taken together, ensure that the requirements of Section 1801(h) are satisfied. In the event that a query produces a positive hit on Section 702-acquired information, the query results can only be viewed by FBI personnel who are appropriately trained and approved to handle such information and "only for the purpose of determining whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime." See FBI Minimization Procedures at 8. Generally, other FBI personnel who have not been trained for and granted access to FISA-acquired information are not allowed to view the query results unless the information has first been determined by appropriately cleared personnel to meet one of those standards. See FBI Minimization Procedures at 12 n.4.[31] Information that is determined to meet one of those criteria can be retained for further investigation and analysis and may be disseminated only in accordance with additional restrictions. See id.; see also id. at 30-37. Before using FISA-acquired information for further investigation, analysis, or dissemination, the FBI must strike, or substitute a characterization for, information of or concerning a United States person, including that person's identity, if it does not reasonably appear to be foreign intelligence information, to

[31] In "very rare" circumstances, see October 20 Transcript at 45, FBI personnel who are not trained for and do not have access to Section 702-acquired information may view the results of a query solely to aid in the determination of whether the information constitutes foreign intelligence information or evidence of a crime. See FBI Minimization Procedures at 12 n.4.

Approved for public release by the ODNI 20160415

be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. See id. at 9.

Based on the foregoing, the Court concludes that the revised querying provisions of the FBI Minimization Procedures comport with the requirements of Section 1801(h). Ms. Jeffress' constitutional concerns about these provisions are addressed below.

7. Conclusion

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA, FBI, and CIA Minimization Procedures satisfy the definition of minimization procedures at Section 1801(h).

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

The Court next considers whether the targeting and minimization procedures included in the July 15, 2015 Submission are consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A).

1. The Applicable Analytical Framework

The Fourth Amendment does not require the government to obtain a warrant to conduct surveillance "to obtain foreign intelligence for national security purposes [that] is 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").[32] This exception to the Fourth

[32] A declassified version of the opinion in In re Directives is available at 551 F.3d 1004 (continued...)

Approved for public release by the ODNI 20160415

Amendment's warrant requirement applies even when a United States person is the target of such a surveillance. See id. at 25-26 (discussing internal Executive Branch criteria for targeting United States persons). The FISC has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within this "foreign intelligence exception" to the warrant requirement of the Fourth Amendment. See September 4, 2008 Opinion at 34-36; accord United States v. Mohamud, 2014 WL 2866749 at *15-18 (D. Or. June 24, 2014).

It follows that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment if those procedures, as implemented, are reasonable. In assessing the reasonableness of a governmental intrusion under the Fourth Amendment, the court must "balance the interests at stake" under the "totality of the circumstances." Id. at 20. The court must consider "the nature of the government intrusion and how the government intrusion is implemented. The more important the government's interest, the greater the intrusion that may be constitutionally tolerated." In re Directives at 19-20 (citations omitted).

> 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 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.

The government's national security interest in conducting acquisitions pursuant to Section 702 "'is of the highest order of magnitude.'" September 4, 2008 Opinion at 37 (quoting

---

[32](...continued)
(FISA Ct. Rev. 2008).

Approved for public release by the ODNI 20160415

In re Directives at 20). With regard to the individual privacy interests involved, the Court has concluded, as discussed above, that the targeting procedures now before it are reasonably designed to target non-United States persons who are located outside the United States. Such persons fall outside the ambit of Fourth Amendment protection. See September 4, 2008 Opinion at 37 (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990)).

Nevertheless, because the government acquires under Section 702 communications to which United States persons and persons within the United States are parties, that is not the end of the matter. Such acquisitions can occur when those non-targeted persons are parties to a communication that is to or from, or that contains a reference to, a tasked selector. See September 4, 2008 Opinion at 15-20. Such communications may also be acquired when they constitute part of a larger "Internet transaction" (e.g., [redacted]) that also contains one or more communications that are to or from, or that contain a reference to, a tasked selector. In the latter case, the entire transaction may be unavoidably acquired by the NSA's "upstream" collection. See October 3, 2011 Opinion at 5, 30-31.[33]

In the Prior 702 Dockets, the FISC concluded that earlier versions of the various agencies' targeting and minimization procedures adequately protected the substantial Fourth

[33] FISA minimization protects the privacy interests of United States persons in communications in which they are discussed, regardless of whether they were parties to such communications. See Section 1801(h)(1) (protecting "nonpublicly available information concerning unconsenting United States persons") (emphasis added). In contrast, non-targets generally do not have a Fourth Amendment-protected interest in communications in which they are discussed, unless they are also parties to the communication. See Alderman v. United States, 394 U.S. 165, 174-76 (1969).

Approved for public release by the ODNI 20160415

Amendment interests that are implicated by the acquisition of communications of such United States persons. See, e.g., August 26, 2014 Opinion at 38-40; August 30, 2013 Opinion at 24-25. In the FISC's assessment, the combined effect of these procedures has been "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." August 26, 2014 Opinion at 40 (internal quotation marks omitted).

2. The FBI's Querying Practices Do Not Render the Targeting and Minimization Procedures Inconsistent with the Fourth Amendment

Amicus curiae Amy Jeffress urges the Court to reconsider its prior Fourth Amendment assessments and to reach "a different conclusion" in light of the provisions of the FBI Minimization Procedures, discussed above, permitting agents and analysts to query the Section 702-acquired information in the FBI's possession using United States-person information for the purpose of finding evidence of crimes unrelated to foreign intelligence. See Amicus Brief at 22. Ms. Jeffress asserts that without additional safeguards, such querying is inconsistent with the requirements of the Fourth Amendment:

> The FBI's querying procedures effectively treat Section 702-acquired data like any other database that can be queried for any legitimate law enforcement purpose. The minimization procedures do not place any restrictions on querying the data using U.S. person identifiers . . . . As a result, the FBI may query the data using U.S. person identifiers for purposes of any criminal investigation or even an assessment. There is no requirement that the matter be a serious one, nor that it have any relation to national security. . . . [T]hese practices do not comply with . . . . the Fourth Amendment.

Id. at 19. According to Ms. Jeffress, the querying provisions of the FBI Minimization Procedures should be revised to "require a written justification for each U.S. person query of the database

Approved for public release by the ODNI 20160415

that explains why the query is relevant to foreign intelligence information or is otherwise justified," or in some other manner that provides additional protection for the United States-person information in the FBI's possession. See id. at 27.

Although the FBI's minimization procedures have for several years expressly permitted the FBI to query unminimized Section 702-acquired data using query terms that are reasonably designed to find and extract not only foreign intelligence information but also evidence of a crime, Ms. Jeffress raises concerns that the Court has not expressly addressed in its prior Section 702 Opinions. The Court agrees with Ms. Jeffress, see id. at 21-24, that it is not bound by its prior approvals of procedures permitting such querying. Indeed, Section 702 requires the Court to assess anew whether the procedures accompanying each certification submitted to it for review are both consistent with both the applicable statutory requirements and with the Fourth Amendment. See 50 U.S.C. § 1881a(i)(2)(B)-(C), (i)(3)(A). After conducting the required reassessment, the Court concludes that the FBI's querying practices do not render the government's implementation of Section 702 inconsistent with the Fourth Amendment.

Ms. Jeffress contends that each query by FBI personnel of Section 702-acquired information is a "separate action subject to the Fourth Amendment reasonableness test." See October 20 Transcript at 6; see also Amicus Brief at 24-25. The government agrees that the FBI's querying process is relevant to the Court's reasonableness analysis, but asserts that each query is not a "separate Fourth Amendment event" that should be independently assessed. See October 20 Transcript at 19. Rather, in the government's view, it is "the program as a whole [that] must . . . be reasonable under the Fourth Amendment." See id. The Court agrees with the

Approved for public release by the ODNI 20160415

government and declines to depart from the analytical framework described above.

As discussed above, FISA requires the Court to assess whether "the targeting and minimization procedures adopted in accordance with [50 U.S.C. § 1881a(d) and (e)] are consistent . . . with the fourth amendment to the Constitution." 50 U.S.C. § 1881a(i)(3)(A). This language directs the Court to assess the constitutionality of the framework created by the targeting and minimization procedures. Moreover, as also discussed above, the Court of Review made clear in In re Directives that the proper analytical approach to Fourth Amendment reasonableness involves "balanc[ing] the interests at stake" under the "totality of the circumstances" presented. In re Directives at 20. That approach requires the Court to weigh the degree to which the government's implementation of the applicable targeting and minimization procedures, viewed as whole, serves its important national security interests against the degree of intrusion on Fourth Amendment-protected interests that results from that implementation. See id. at 19-20.

After assessing the FBI's querying practices under the totality of circumstances, the Court declines to deviate from its prior decisions. As discussed above, the querying provisions of the FBI Minimization Procedures are applied only to information that has been acquired following application of the NSA Targeting Procedures. Those procedures require that before tasking a selector for collection, NSA first take steps to determine that the user of the selector is a non-United States person who is reasonably believed to be located outside the United States and that he or she is expected to possess, receive, or communicate foreign intelligence information. See NSA Targeting Procedures at 4. These requirements direct the government's acquisitions toward

Approved for public release by the ODNI 20160415

communications that are likely to yield foreign intelligence information.

Moreover, the purpose of permitting queries designed to elicit evidence of ordinary crimes is not entirely unconnected to foreign intelligence. Such queries are permitted in part to ensure that the FBI does not fail to identify the foreign-intelligence significance of information in its possession. One of the main criticisms of the government following the attacks of September 11, 2001, was its failure to identify and appropriately distribute information in its possession that could have been used to disrupt the plot. Although the queries at issue here are designed to find and extract evidence of crimes believed to be unrelated to foreign intelligence, such queries may nonetheless elicit foreign intelligence information, particularly since the Section 702 collection is targeted against persons believed to possess, receive, or communicate such information. See NSA Targeting Procedures at 4. A query designed to find and extract data regarding a [redacted] plot, for example, might reveal a previously unknown connection to persons believed to be funding terrorist operations on behalf of [redacted]. See October 20 Transcript at 20-21. Such unexpected connections may arise only rarely, but when they do arise, the foreign intelligence value of the information obtained could be substantial.

With respect to the intrusiveness of the querying process, the FBI Minimization Procedures impose substantial restrictions on the use and dissemination of information derived from queries. In the event that a query produces a positive hit on Section 702-acquired information, the query results can only be viewed by FBI personnel who are appropriately trained and approved to handle such information and "only for the purpose of determining whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign

Approved for public release by the ODNI 20160415

intelligence information or to assess its importance, or to be evidence of a crime." See FBI Minimization Procedures at 8, 12 n.4. Generally, other FBI personnel who have not been trained for and granted access to FISA-acquired information are not allowed to view the query results unless the information has first been determined to meet one of these standards. See FBI Minimization Procedures at 12 n.4. Information that is determined to meet one of those criteria can be retained for further investigation and analysis and may be disseminated only in accordance with additional restrictions. See id.; see also id. at 30-37. Before using FISA-acquired information for further investigation, analysis, or dissemination, the FBI must strike, or substitute a characterization for, information of or concerning a United States person, including that person's identity, if it does not reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. See id. at 9.

Furthermore, it must be noted that only a subset of the information acquired by the government pursuant to Section 702 is subject to queries by the FBI. The FBI acquires only a "small portion" of the unminimized Section 702 collection. See October 20 Transcript at 29-30; PCLOB Report at 161 n.571 (Separate Statement By Board Members Rachel Brand and Elisebeth Collins Cook) (citing Letter from Deirdre M. Walsh, Director of Legislative Affairs, to Hon. Ron Wyden, United States Senate (June 27, 2014)). The FBI only receives collection on tasked facilities that are deemed to be relevant to an open [redacted] FBI investigation. See October 20 Transcript at 30. Moreover, the FBI does not receive any unminimized information acquired through NSA's "upstream collection" under Section 702, a form of collection that is, on

Approved for public release by the ODNI 20160415

balance, more likely than others to include non-target communications of United States persons and persons located in the United States that have no foreign intelligence value. See [redacted], Memorandum Opinion issued on November 30, 2011, at 6.

Finally, according to the government, FBI queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results from the Section 702-acquired data. See PCLOB Report at 59-60; id. at 162 (Separate Statement of Board Members Brand and Cook). Hence, the risk that the results of such a query will be viewed or otherwise used in connection with an investigation that is unrelated to national security appears to be remote, if not entirely theoretical. The Court is not prepared to find a constitutional deficiency based upon a hypothetical problem. Nevertheless, to reassure itself that this risk assessment is valid, the Court will require the government to report any 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. See page 78 below.

In light of the foregoing, the Court concludes that the querying provisions of the FBI Minimization Procedures strike a reasonable balance between the privacy interests of United States persons and persons in the United States, on the one hand, and the government's national security interests, on the other. The FBI's use of those provisions to conduct queries designed to return evidence of crimes unrelated to foreign intelligence does not preclude the Court from concluding that taken together, the targeting and minimization procedures submitted with the

Approved for public release by the ODNI 20160415

2015 Certifications are consistent with the requirements of the Fourth Amendment.

E. The Compliance and Implementation Issues Reported by the Government Do Not Preclude a Finding that the Targeting and Minimization Procedures Comply With Statutory Requirements and the Fourth Amendment

As noted above at pages 6-7, the FISC examines the government's implementation of, and compliance with, the targeting and minimization procedures as part of assessing whether those procedures comply with the applicable statutory (and Fourth Amendment) requirements.

In conducting this assessment, the Court is mindful that the controlling norms are ones of reasonableness, not perfection.[34] This distinction is particularly important in the context of a large and complex endeavor such as the government's implementation of Section 702. While in absolute terms, the scope of acquisitions under Section 702 is substantial, the acquisitions are not conducted in a bulk or indiscriminate manner. Rather, they are effected through [redacted] discrete targeting decisions for individual selectors.[35] Each targeting decision requires

---

[34] See Section 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); Section 1801(h)(1) (requiring minimization procedures that are "reasonably designed" to minimize acquisition and retention, and to prohibit dissemination, of information concerning United States persons, consistent with foreign intelligence needs); United States v. Knights, 534 U.S. 112, 118 (2001) ("The touchstone of the Fourth Amendment is reasonableness . . . .").

[35] For example, the NSA reports that, "on average, approximately [redacted] individual facilities" were tasked for acquisition "at any given time between June 1 and August 31, 2015." Quarterly Report to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on September 18, 2015, at 1 (footnote omitted) ("September 18, 2015 Compliance Report"). Facilities tasked for acquisition include "[redacted]" Id. at 1 n.1. "Additionally, between June 1 and August 31, 2015, the [FBI] reports that it received and processed approximately [redacted]

(continued...)

Approved for public release by the ODNI 20160415

application of the pre-tasking provisions of the applicable targeting procedures. See NSA Targeting Procedures at 1-6; FBI Targeting Procedures at 1-3. For each selector while it is subject to tasking, there are post-tasking requirements designed to ascertain, for example, whether its targeted user has entered the United States. See NSA Targeting Procedures at 6-8. And pursuant to the minimization procedures, there are detailed rules concerning the retention, use, and dissemination of information obtained pursuant to Section 702. See NSA Minimization Procedures at 3-16; FBI Minimization Procedures at 5-33; CIA Minimization Procedures at 1-9.

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.

It is apparent to the Court that the implementing agencies, as well as ODNI and the National Security Division ("NSD") of DOJ devote substantial resources to their compliance and oversight responsibilities under Section 702.[36] With relatively few exceptions – one of which is

---

[35](...continued)
[redacted]." Id. at 1.

[36] Indeed, during the past year, NSD has provided the Court with a very detailed overview of its and ODNI's oversight efforts with respect to the Intelligence Community's implementation of Section 702. In July 2014, PCLOB recommended that the government provide the Court with random samples of tasking sheets and (NSA's and CIA's) United States person query terms to assist the Court's consideration of Section 702 certifications. PCLOB (continued...)

Approved for public release by the ODNI 20160415

discussed in detail below – instances of non-compliance are identified promptly and appropriate remedial actions are taken, to include purging information that was improperly obtained or otherwise subject to destruction requirements. Accordingly, the Court's overall assessment of the implementation of, and compliance with, the targeting and minimization procedures permits a finding that the these procedures, as implemented, satisfy the applicable statutory requirements. Nonetheless, the Court believes it is useful to discuss the following aspects of implementation and, in some respects, to direct the government to provide additional information.

1. The FBI's Non-compliance With Attorney-Client Minimization Procedures

FISA's definition of minimization procedures at Section 1801(h) does not, by its terms, afford any special protection to communications subject to the attorney-client privilege.[37] Nevertheless, as discussed above, the minimization procedures under review have specific rules for handling attorney-client communications. See NSA Minimization Procedures at 10; FBI Minimization Procedures at 12-17, 29-30; CIA Minimization Procedures at 5-7. Because the FBI

---

[36](...continued)
Report at 141 (Recommendation 4). The government adopted this recommendation, and in January 2015 it provided the Court's legal staff with an extensive briefing on its oversight activities, as well as sample tasking sheets and query terms. The government offered to make additional tasking sheets and query terms available to the Court. At the Court's request, the government provided an overview of its Section 702 oversight efforts to all of the Court's judges in May 2015, which included a review of sample tasking sheets. These briefings confirmed the Court's earlier understanding that the government's oversight efforts with respect to Section 702 collection are robust.

[37] FISA does provide that "[n]o otherwise privileged communication obtained in accordance with, or in violation of, the provisions of [FISA] shall lose its privileged character." 50 U.S.C. § 1806(a).

Approved for public release by the ODNI 20160415

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 NSD, 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. FBI Minimization Procedures at 13. 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). Id. As discussed above, the FBI Minimization Procedures contain new provisions designed to further enhance the protection of attorney-client privileged communications. See FBI Minimization Procedures at 17-18.

At the time the Court was considering the 2014 Certifications, the government had identified [redacted] instances, discovered in the preceding six months, in which FBI case agents knew that persons targeted under Section 702 faced federal criminal charges, but had not established the required review teams. See August 26, 2014 Opinion at 35-36. The government generally attributed those instances to individual failures or confusion, rather than a "systematic issue." Id. The Court's Memorandum Opinion and Order issued in connection with the 2014 Certifications noted that one would expect the number of Section 702 targets charged with federal crimes to be fairly small, given that these targets are reasonably believed to be non-United States persons located outside of the United States Id. at 36. Accordingly, the Court noted that [redacted] then-recent

Approved for public release by the ODNI 20160415

cases in which the FBI had not established the required review teams seemed to represent a potentially significant rate of non-compliance. Id. In light of this, the Court required, among other things, that the government make a subsequent written submission providing an assessment of the adequacy of the government's training, guidance and oversight efforts with regard to the requirements for attorney-client privileged communications in the FBI Minimization Procedures. Id. at 42-43.

Since the Court approved the prior certifications in August 2014, the government has identified an additional [redacted] instances in which FBI case agents knew that persons targeted under Section 702 faced federal criminal charges, but did not establish the required review teams.[38] In notifying the Court of [redacted] these instances, the government wrote that "[w]hile there have been isolated instances in which FBI personnel have not established review teams, the Government continues to believe that these were the result of individual failures or confusion and

[38] See Quarterly Report to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on December 19, 2014 ("December 19, 2014 Compliance Report"), at 83-86; Quarterly Report to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on March 20, 2015 ("March 20, 2015 Compliance Report"), at 71-73; Quarterly Report to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on June 19, 2015 ("June 19, 2015 Compliance Report"), at 110-113; September 18, 2015 Compliance Report at 134-135; September 9, 2015, Preliminary Notice of Compliance Incident Regarding [redacted] ("September 9 Preliminary Notice"); October 5, 2015, Preliminary Notice of Compliance Incident Regarding [redacted] ("October 5 Preliminary Notice"); and October 8, 2015, Preliminary Notice of Compliance Incidents Regarding [redacted] and [redacted] ("October 8 Preliminary Notice").

Approved for public release by the ODNI 20160415

not a systematic issue."[39] Review of the individual instances indeed suggests that at least some FBI case agents are generally aware of the requirement for a review team when a Section 702 target is charged with a federal crime, but they are confused about the specific requirements of the FBI Minimization Procedures. In [redacted] instances, for example, the relevant FBI case agents set up ad hoc or informal review teams wherein a case agent or a professional support employee not involved with the investigation was assigned to review communications for attorney-client privileged material prior to the case agent and team members reviewing the communications.[40] In [redacted] other instances, the relevant FBI case agents were generally aware of the requirement for a review team, but mistakenly believed that a review team is not required if the pertinent charging document is under seal or if the target is located outside of the United States.[41]

The Court was extremely concerned about these additional instances of non-compliance, and at the October 8 Hearing on compliance matters, the Court asked the government to explain why there had been an additional [redacted] instances of non-compliance in the past year.[42] The government indicated that it had taken a two-pronged approach to improving compliance with these provisions of the minimization procedures during the preceding year. Id. at 3.

---

[39] See December 19, 2015 Compliance Report at 83, 86; June 19, 2015 Compliance Report at 113; September 18, 2015 Compliance Report at 135; September 9 Preliminary Notice at 2; October 5 Preliminary Notice at 2; and October 8 Preliminary Notice at 2-3.

[40] See December 19, 2014 Compliance Report at 83, 85-86; and June 19, 2015 Compliance Report at 112.

[41] See October 8, 2015 Preliminary Compliance Notice at 2.

[42] Transcript of Proceedings Held Before the Honorable Thomas F. Hogan at 3, [redacted] (October 8, 2015), ("October 8 Transcript").

Approved for public release by the ODNI 20160415

First, the government indicated that at each of the approximately [redacted] oversight reviews that NSD conducted at FBI field offices in the preceding year, NSD reminded individual case agents that a review team is required when a target is charged with a crime pursuant to the United States Code, both in individual meetings and general training sessions. Id. at 3-4. The government represented at the hearing that it was through some of these oversight reviews that it identified some of the instances of non-compliance reported to the Court during the past year. Id. at 4. In response to a question from the Court, the government also indicated that every FBI case agent is required to receive electronic training prior to receiving access to Section 702 collection, which includes training on the review team requirement. Id. at 6.

Second, the government reported that in August 2015, the FBI modified its [redacted] system through which a case agent nominates a selector for collection [redacted] – of the Section 702 collection. Id. at 4-5. As a result of this modification, the [redacted] system now asks the case agent whether the user of the relevant selector is charged with a federal crime. Id. at 4. If the agent indicates that the user is not currently charged, the system asks whether the agent expects the user to be charged in the future, and if so, when. Id. If the agent indicates that the user of a facility is currently charged or likely to be charged in the future, FBI Headquarters receives notice, and the Headquarters unit that manages Section 702 collection will reach out to the agent to ensure that a review team is established. Id. This [redacted] tool also requires agents to update information about their Section 702 targets every 90 days. Id. The government represented that as a result of the modification to this system in August, [redacted]

Approved for public release by the ODNI 20160415

additional instances of non-compliance with the review team requirement were discovered by the time of the October 8 Hearing. Id. at 5.

Based on the measures described at the October 8 Hearing, the Court is satisfied that the government is taking appropriate measures to prevent further instances of non-compliance with the review team requirement. The Court understands that as a result of these modifications to the [redacted] system – especially the requirement that case agents update information about their Section 702 targets every 90 days – remaining instances of non-compliance for currently-tasked selectors should be identified and remedied in the immediate future. The Court understands from post-hearing communications with the government that for de-tasked facilities, identifying remaining instances of non-compliance with the review team requirement will likely happen through NSD oversight reviews.

The Court does not believe that the recent instances of non-compliance with the review team requirement prevent a finding that the minimization procedures under review comply with the requirements of Section 1801(h) and the Fourth Amendment. However, the Court strongly encourages the government to try to identify any remaining instances of non-compliance as quickly as possible. The Court anticipates holding a follow-up hearing on Section 702 compliance matters in early 2016, at which time the Court will expect to receive an update on compliance with the review team requirements of the FBI Minimization Procedures. See page79 below.

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

Section III.A. of the FBI Minimization Procedures requires the FBI to "retain all FISA-

Approved for public release by the ODNI 20160415

acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with" the minimization and other applicable FBI procedures. FBI Minimization Procedures at 5. 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[.]" FBI Minimization Procedures at 7. It also requires users with access to raw FISA-acquired information to receive training on the minimization procedures. Id.

[redacted]

Approved for public release by the ODNI 20160415

[redacted]

[redacted]

Approved for public release by the ODNI 20160415

[redacted]

3. [redacted]

On July 13, 2015, the Government filed an Update and Notice Regarding the National Security Agency's (NSA) purge process for FISA-acquired information in Mission Management Systems ("July 13, 2015 Notice"). That notice indicated that the NSA had not been purging from its [redacted] database records associated with purged Section 702 collection. July 13, 2015 Notice at 3. The [redacted] database, and the question of whether the NSA had to purge the fruits of unlawful surveillance from this "mission management system," were the subject of several opinions issued by the Court in 2010 and 2011. Because the analyses and

Approved for public release by the ODNI 20160415

holdings of those opinions are relevant to the issue presented by the July 13, 2015 Notice, the Court will briefly review them.

Between June and August of 2010, the government filed several compliance notices indicating that the NSA had, under an authorization to conduct electronic surveillance [redacted] Opinion and Order Regarding Fruits of Unauthorized Electronic Surveillance issued on December 10, 2010, at 1-2 ("December 2010 [redacted]"). The government proposed to retain the fruits of this unlawful surveillance insofar as they resided in the [redacted] database. Id. at 3. In making this proposal, the government argued that the Standard Minimization Procedures For Electronic Surveillance Conducted by the NSA ("NSA Electronic Surveillance SMPs") only applied to interceptions authorized by the Court and did not apply to the fruits of unlawful surveillance. Id. at 3-4. The government also argued that the criminal prohibition in 50 U.S.C. §1809(a)(2) only prohibits use or disclosure of unlawfully obtained information for investigative or analytic purposes.[44] Id. at 6.

The Court issued an opinion in December 2010 rejecting the government's argument that the NSA Electronic Surveillance SMPs do not apply to over-collected information, noting instead that they appeared to require the destruction of at least some of the over-collected

[44] Section 1809(a)(2) provides that "a person is guilty of an offense if he intentionally . . . discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. 50 U.S.C. § 1809(a)(2).

Approved for public release by the ODNI 20160415

information. Id. at 4-5. The Court also rejected the government's argument that §1809(a)(2) only applies to use or disclosure of information for investigative or analytic purposes, but recognized a narrower implicit exception from this prohibition for use or disclosure of "the results of unauthorized surveillance [that] are needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future." Id. at 6-8. In recognizing this exception, the Court noted that:

> Congress may be presumed not to have prohibited actions that are necessary to mitigate or prevent the harms at which Section 1809(a)(2) is addressed. But the application of this principle must be carefully circumscribed, so that it does not lead to an unjustified departure from the terms of the statute. "[W]hen Congress has spoken clearly, a court assessing the reach of the criminal statute must heed Congress's intent as reflected in the statutory text." Docket No. PR/TT [redacted], Memorandum Opinion issued on [redacted], [redacted], at 113 (citing Huddleston v. United States, 415 U.S. 814, 831 (1974) ("[redacted] Opinion").

Id. at 8 (emphasis in original). Because the Court could not ascertain whether or to what extent the over-collected information [redacted] case might fall within this implicit exception for § 1809(a)(2), the Court ordered the government to make a subsequent submission explaining why the particular information at issue in that case was needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future. Id. at 8-9. After review of this submission and a hearing, the Court issued an opinion in May 2011 in which it found that the unauthorized collection in this case did not fall within the implicit narrow exception to § 1809(a)(2), and that the NSA's Electronic Surveillance SMPs required the destruction of the unauthorized collection in this case. Opinion and Order Requiring Destruction of Information Obtained by Unauthorized Electronic Surveillance issued on May 13, 2011, at 8-9 ("May 2011 [redacted]"). In discussing the narrow exception to § 1809(a)(2) in this opinion, the Court

Approved for public release by the ODNI 20160415

noted the following:

> [C]ourts should not attempt "to restrict the unqualified language of a [criminal] statute to the particular evil that Congress was trying to remedy – even assuming that it is possible to identify that evil from something other than the text of the statute itself." Brogan v. United States, 522 U.S. 398, 403 (1998). . . . The exception recognized in the December 10, 2010 Opinion stands on narrower but firmer ground: that in limited circumstances, prohibiting use or disclosure of the results of unauthorized electronic surveillance would be "so 'absurd or glaringly unjust' . . . as to [call into] question whether Congress actually intended what the plain language of Section 1809(a)(2) "so clearly imports."

May 2011 [redacted] at 5 (citations omitted).

In light of the May 2011 [redacted], the Court was very surprised to learn from the July 13, 2015 Notice that the NSA had not been deleting from [redacted] Section 702 records placed on the NSA's Master Purge List ("MPL").[45] While that opinion dealt exclusively with Title I collection in a particular case, it would be difficult to conclude from its analysis and holding that Section 702 collection subject to purge should not also be deleted from [redacted]. Perhaps more disturbing and disappointing than the NSA's failure to purge this information for more than four years, was the government's failure to convey to the Court explicitly during that time that the NSA was continuing to retain this information in [redacted]. At the October 8, 2015 Hearing, the government acknowledged that it should have "more prominently and more fulsomely" explained the continued retention of this information in [redacted] to the Court, and that it should not have taken four years for the government to explain its proposed resolution of this issue to the Court. October 8 Transcript

[45] The July 13, 2015 Notice did indicate that the NSA had reconfigured [redacted] to delete prospectively records placed on the MPL, and that it would soon start purging from [redacted] historical records that had been placed on the MPL. July 13, 2015 Notice at 4.

Approved for public release by the ODNI 20160415

at 26-27. As the Court explained to the government at the October 8 Hearing, it expects the government to comply with its heightened duty of candor in ex parte proceedings at all times. Candor is fundamental to this Court's effective operation in considering ex parte submissions from the government, particularly in matters involving large and complex operations such as the implementation of Section 702.

On October 5, 2015, the government filed a supplemental notice regarding the National Security Agency's purge process for FISA-acquired information ("October 5, 2015 Notice"). That notice indicated that since the filing of the July 13, 2015 Notice, NSA had removed from [redacted] Section 702-acquired records that were marked as subject to purge. October 5, 2015 Notice at 2. However, on October 28, 2015, the government filed another supplemental notice regarding NSA's purge processes ("October 28, 2015 Notice") in which it indicated that a technical malfunction in [redacted] had rendered the aforementioned purges incomplete.[46] October 28, 2015 Notice at 2. The October 28, 2015 Notice indicated that the NSA was "working to develop a technical solution to fix this system error in how [redacted] effects purges and . . . investigating the amount of time it will take to develop and implement that fix." Id. Given the government's representation that the NSA is working to correct this error in [redacted] purging process, the Court does not believe the incomplete purges in this system prevent it from finding that the NSA Minimization Procedures comply with the requirements of Section 1801(h) and the Fourth Amendment. Nevertheless, the

---

[46] More specifically, in effecting the purges, [redacted] computer program had been searching for records using only [redacted] of the [redacted] identifiers on the MPL relevant to the information held in [redacted] Id.

Approved for public release by the ODNI 20160415

Court expects the government to resolve this issue expeditiously, and it anticipates receiving an update on this issue at a follow-up hearing on Section 702 compliance matters in early 2016. See page 79 below.

4. [redacted] & [redacted]

a. *Introduction*

As noted above, on July 13, 2015, the government filed a letter regarding the NSA's purge processes for FISA-acquired information in NSA "mission management systems." In addition to discussing [redacted], this letter also "serve[d] as notice pursuant to Rule 13(b) [of the FISC's Rules of Procedure] of a compliance incident regarding FISA-acquired information subject to purge or age off that is being retained in two of NSA's compliance mission management systems, [redacted] and [redacted]." July 13, 2015 Notice at 2. More specifically, the letter noted that the government had "concluded that these two systems have been retaining data subject to purge and age-off in a manner that is potentially inconsistent with NSA's FISA-related minimization procedures." July 13, 2015 Notice at 5. Subsequent communications between the government and Court 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).

b. *Relevant Legal Authorities*

Analysis of the issues presented by the [redacted] and [redacted] disclosures requires consideration of the following legal authorities:

Approved for public release by the ODNI 20160415

i. *50 U.S.C. § 1881a*

As discussed above, Section 702, codified at 50 U.S.C. § 1881a, permits the Attorney General and the Director of National Intelligence to target non-United States persons reasonably believed to be located outside of the United States to acquire foreign intelligence information. 50 U.S.C. §1881a(a). Acquisitions under Section 702 must comply with a number of limitations, the first of which is that the government may not intentionally target any person known at the time of acquisition to be located in the United States 50 U.S.C. §1881a(b)(1). To effect this prohibition, the statute requires the adoption and use of targeting procedures that are reasonably designed to ensure that Section 702 acquisitions are limited to targeting persons reasonably believed to be located outside of the United States. 50 U.S.C. §1881a(c)(1)(A), (d)(1)(A). Section 702 also prohibits the government from intentionally targeting a United States person reasonably believed to be outside of the United States, or acquiring any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States. 50 U.S.C. §1881a(b)(3),(4).

ii. *NSA Targeting Procedures*

The NSA Targeting Procedures contain a number of provisions designed to enable its compliance with the requirements and prohibitions of Section 702. Among the most important are Sections I and II. Section I of the procedures, which relates to the determination of whether a given target is a non-United States person reasonably believed to be located outside of the United States, provides that the NSA may [redacted] NSA Targeting Procedures at 1.

Approved for public release by the ODNI 20160415

With respect to electronic communications [redacted], the procedures provide that the NSA may [redacted] Section II of the NSA Targeting Procedures also provides that "[a]fter a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis." Id. at 6. For electronic communications [redacted], this analysis may include "[r]outinely checking all electronic communications [redacted] tasked pursuant to these procedures [redacted] to determine if an electronic communications [redacted] was accessed from inside the U.S." Id.

iii. *NSA Minimization Procedures*

Section 2(e) of the NSA Minimization Procedures defines a foreign communication as one that has at least one communicant outside of the United States, and all other communications are considered domestic communications. NSA Minimization Procedures at 2. Section 3(d)(2) of the NSA Minimization Procedures also provides that "[a]ny communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired . . . will be treated as domestic communications . . . [.]" NSA

Approved for public release by the ODNI 20160415

Minimization Procedures at 9. Section 5 of the NSA Minimization Procedures provides that a domestic communication will be promptly destroyed upon recognition, unless the Director of NSA specifically determines that the sender or intended recipient had been properly targeted, and the communication satisfies one or more additional requirements (e.g., the communication is reasonably believed to contain significant foreign intelligence information). NSA Minimization Procedures at 12. Notwithstanding this destruction requirement, Section 5 also provides that "NSA may . . . use information derived from domestic communications for collection avoidance purposes, and . . . NSA may retain the communication from which such information is derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL)." Id. at 13.

With respect to the length of time that NSA is permitted to retain Section 702 collection, Section 3(c) of the procedures provides, in relevant part, that 1) telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers may not be retained longer than five years from the expiration date of the certification authorizing the collection, unless the NSA specifically determines that each such communication meets retention standards in the procedures; 2) Internet transactions acquired through NSA's upstream collection techniques may not be retained longer than two years from the expiration date of the certification authorizing the collection (unless NSA makes particular findings about the transaction); and 3) any Internet transactions acquired through NSA's upstream collection techniques prior to to October 31, 2011, will be destroyed upon recognition. Id. at 7-8.

Approved for public release by the ODNI 20160415

iv. *50 U.S.C. § 1809(a)(2)*

As noted above, 50 U.S.C. § 1809(a)(2) provides that "a person is guilty of an offense if he intentionally . . . discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. 50 U.S.C. § 1809(a)(2)

c. *Background on* [redacted] *&* [redacted] *and their compliance with legal requirements*

In the July 13, 2015 Notice, the government provided the following background information about [redacted] and [redacted] [redacted] is a system analysts use to [redacted] July 13, 2015 Notice at 6. Analysts most commonly use [redacted] as part of a determination of whether the facility can be properly tasked under Section 702. Id. This system provides information regarding [redacted]

[redacted]

Approved for public release by the ODNI 20160415

[redacted] is a tool used to perform post-tasking [redacted] checks to identify indications that a Section 702 target may be located in the United States. Id. at 5. This tool [redacted]

The July 13, 2015 Notice indicated that [redacted] and [redacted] were not compliant with several provisions of the NSA Minimization Procedures. With respect to [redacted], the notice indicated that it does not age off analyst query results within the time periods required by the NSA Minimization Procedures (i.e., within two years for upstream

---

[47] As discussed in greater detail below, on October 21, 2015, the government – in response to an Order issued by this Court -- filed the "Government's Verified Response to the Court's Order Dated October 14, 2015" ("Government's October 21, 2015 Response"), in which it provided more information about [redacted] and [redacted]. This filing indicated that [redacted] Government's October 21, 2015 Response at 3.

[48] According to the July 13, 2015 Notice, [redacted]

Approved for public release by the ODNI 20160415

collection, and within five years for Internet communications acquired by or with the assistance of the FBI from Internet Service Providers), though it has aged-off all Section 702 upstream data acquired before October 31, 2011. July 13, 2015 Notice at 7. [redacted]

[redacted] Id. The July 13, 2015 Notice indicated that the NSA does not age off records in [redacted] in compliance with the NSA Minimization Procedures "because of the utility of these records for compliance and collection avoidance purposes." Id. The notice further indicated that NSA compliance personnel use historical information – which presumably includes both information required to be aged-off and information associated with objects on the NSA's MPL – to support the resolution of alerts (i.e., when a Section-702 tasked facility appears to have been accessed in the United States) and to respond to questions posed by NSD and ODNI in the course of those offices' oversight of the Section 702 program. Id.

With respect to [redacted], the July 13, 2015 Notice indicated that [redacted] does not comply with the requirement in the NSA Minimization Procedures to age off telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers within five years of the expiration date of the certification authorizing

Approved for public release by the ODNI 20160415

the collection. Id. at 6.[49] Additionally, [redacted] is retained within [redacted] records even after the [redacted] have been purged from other NSA systems that directly support intelligence analysis pursuant to minimization requirements. Id. at 5. The notice indicated that instead of purging [redacted], certain fields within the records are made inaccessible to analysts and are visible only to a small number of personnel who have responsibility for system administration and compliance issues.[50] Id. The notice indicated that the NSA has not been purging historical data or data associated with objects placed on the MPL from [redacted] "because compliance personnel use historical information [redacted] to resolve alerts." Id. By way of example, the notice described that if an [redacted] record, in combination with other analysis, indicates [redacted], that record can be used to resolve an alert (and detask the relevant selector) more quickly in the event that the same target or a different target enters the United States and begins using a tasked selector [redacted]. Id. Additionally, [redacted]

---

[49] The notice indicated that [redacted] is in compliance with the requirement to remove Section 702 information acquired from upstream collection within two years of the expiration date of the certification authorizing the collection. Id. Additionally, all Section 702 upstream Internet collection acquired prior to October 31, 2011, has been purged from [redacted]. Id.

[50] The Government's October 21, 2015 Response indicated that after a communication has been placed on the MPL, the following Section 702-acquired data is retained in [redacted] to permit more effective resolutions of future alerts: [redacted] Government's October 21, 2015 Response at 7.

Approved for public release by the ODNI 20160415

[redacted] Finally, the notice indicated that the resolution of prior alerts can provide context surrounding new alerts. [redacted] If this information was purged from [redacted], NSA would not have information about the prior [redacted], which might result in an unnecessary delay in detasking selectors that [redacted]. Id.

The Court was extremely concerned about the NSA's failure to comply with its minimization procedures – and potentially 50 U.S.C. § 1809(a)(2) – and questioned the government about these issues at the October 8 Hearing. Additionally, the Court issued an Order on October 14, 2015 ("October 14, 2015 Order"), requiring the government to make a written submission within a week describing how it justified under the NSA Minimization Procedures and § 1809(a)(2) the retention and use in [redacted] and [redacted] of information otherwise subject to purge. On October 21, 2015, the government filed a timely response.

---

[51] The Government's October 21, 2015 Response indicated that "since October 2013, NSA identified approximately [redacted] instances in which prior alert information resulted in alerts being prioritized as 'urgent' and subject to priority review." Government's October 21, 2015 Response at 10.

Approved for public release by the ODNI 20160415

d. *Government's Proposed Resolution of Identified Issues*

The Government's October 21, 2015 Response provided more detailed information about [redacted] and [redacted], some of which is noted above. It also indicated that the NSA will begin complying with some elements of its minimization procedures which it is currently violating. Finally, the submission included the government's justifications under the NSA Minimization Procedures and 50 U.S.C. § 1809(a)(2) for the retention and use in [redacted] and [redacted] of other information otherwise subject to purge.

With respect to the NSA's non-compliance with the age-off requirements in its minimization procedures, the Government's October 21, 2015 Response indicated that the NSA will begin implementing the age-off time periods required by the procedures. Government's October 21, 2015 Response at 13-14. With respect to the NSA's retention in [redacted] and [redacted] of data associated with objects on the MPL, the government noted that despite the general destruction requirement for domestic communications, Section 5 of the NSA Minimization Procedures permits the NSA to use information derived from such communications for collection avoidance purposes.[52] Id. at 19. The government noted that the NSA has been retaining information in [redacted] and [redacted] that has been placed on the MPL for the very purpose of collection avoidance. Id. The Government's October 21, 2015

[52] Again, as noted above, Section 5 of the NSA Minimization Procedures states that "[n]otwithstanding the [general destruction requirement] above, . . . NSA may . . . use information derived from domestic communications for collection avoidance purposes, and may provide such information to the FBI and CIA for collection avoidance purposes. NSA may retain the communication from which such information is derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List[.]" NSA Minimization Procedures at 13.

Approved for public release by the ODNI 20160415

Response also argued that keeping information in these systems that has been placed on the MPL supports the NSA's obligations under Sections I and II of the NSA Targeting Procedures. Id. at 5, n.3, and 8, n.9. As described above, those provisions require the NSA to conduct pre- and post-tasking checks on Section 702 selectors by checking its data repositories to determine a target's location. Id. The government noted that "foreignness determinations, both pre-tasking and post-tasking, are a fundamental element of Section 702's statutory scheme" and "contribute significantly to the Fourth Amendment reasonableness of Section 702 collection." Id. at 17.

Notwithstanding the government's argument that retention of information on the MPL in [redacted] and [redacted] is consistent with the NSA's procedures, the government indicated that it plans to modify its treatment of information collected under FISA and placed on the MPL to better ensure that such information is only used for collection avoidance. Id. at 14. Specifically, the government indicates that for [redacted], if the underlying data is subject to purge, NSA will delete the underlying data from [redacted] and analysts will only be able to access FISA-acquired or derived information in the following specific fields: [redacted] Id. As part of the query response, analysts will also receive notice that the evidence supporting the foreignness determination has been purged from [redacted]. Id. at Attachment A.

With respect to [redacted], the government indicated that going forward, if the underlying data is subject to purge, NSA will limit access to FISA-acquired or derived

Approved for public release by the ODNI 20160415

information in [redacted] to the following specific fields: [redacted] The government's submission noted that access to this information will be restricted to compliance and technical personnel, and intelligence analysts will only see a notice indicating that the information has been purged. Id. Again, the government noted that altering the way in which it treats information collected under FISA and placed on the MPL will further ensure that this information is only used for collection avoidance. Id.

The Court is persuaded by the government's argument that Section 5 of the NSA Minimization Procedures does not prohibit the NSA from keeping data in [redacted] and [redacted] that is derived from domestic communications placed on the MPL for the purpose of collection avoidance. The Court also appreciates the NSA's plan to modify its treatment of Section 702-acquired information in [redacted] and [redacted] that has been placed on the MPL, to further ensure that it is only used for collection avoidance. Accordingly, the information that remains of concern to the Court – at least insofar as the NSA's compliance with its targeting and minimization procedures is concerned – is what the Court assesses to be the much smaller categories of Section 702-acquired information in [redacted] and [redacted] that have been placed on the MPL because of other destruction requirements under the NSA Targeting and Minimization Procedures. Examples would be incidentally acquired communications of or concerning United States persons that are clearly not relevant to the authorized purpose of the

Approved for public release by the ODNI 20160415

acquisition or that do not contain evidence of a crime which may be disseminated under the minimization procedures (see Section 3(b)(1) of NSA Minimization Procedures); attorney-client communications that do not contain foreign intelligence information or evidence of a crime (see Section 4(a) of NSA Minimization Procedures); and any instances in which the NSA discovers that a United States person or a person not reasonably believed to be outside the United States at the time of targeting has been intentionally targeted under Section 702 (see Section IV of the NSA Targeting Procedures). The Court is directing the government to report on 1) how the NSA plans to comply with its targeting and minimization procedures with respect to these other categories of information in [redacted] and [redacted], or alternatively, 2) how the retention and use of these other categories of information in [redacted] and [redacted] comports with the NSA's targeting and minimization procedures. See page 78 below. The Court also expects to hear from the government on this issue at the aforementioned follow-up hearing on Section 702 compliance matters in early 2016.

The other issue the Court directed the government to report on in its October 14, 2015 Order was how the government justified under 50 U.S.C. § 1809(a)(2) the retention and use in [redacted] and [redacted] of information otherwise subject to purge. As noted above, § 1809(a)(2) states that "a person is guilty of an offense if he intentionally . . . discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. 50 U.S.C. § 1809(a)(2). Accordingly, a violation of § 1809(a)(2) must involve the intentional disclosure or use of information that is obtained through activity that meets the

Approved for public release by the ODNI 20160415

definition of "electronic surveillance;"[53] that activity must have been unauthorized; and the use or disclosure must be made with at least reason to know it was unauthorized.[54]

The plain language of § 1809(a)(2) does not require the NSA to search for and identify information in [redacted] and [redacted] that may be subject to the criminal prohibition. It similarly does not require the NSA to destroy information in these systems that is subject to § 1809(a)(2). It does, however, prohibit the NSA from intentionally disclosing or using information under the circumstances described above. Therefore, when the NSA knows or has reason to know that a piece of information was acquired through an unauthorized electronic surveillance, it has an affirmative statutory obligation to refrain from disclosing or using it.

Notably, this Court has previously stated that the collection of "roamer communications" does not generally violate Section 702. Specifically, in the September 4, 2008 Opinion referenced above, the Court stated the following:

---

[53] It is worth noting that 50 U.S.C. § 1827 contains analogous criminal prohibitions related to physical search, which could include the acquisition of stored data under Section 702.

[54] With respect to this knowledge element, the Court has previously stated the following:

> When it is not known, and there is no reason to know, that a piece of information was acquired through electronic surveillance that was not authorized by the Court's prior orders, the information is not subject to the criminal prohibition in Section 1809(a)(2). Of course, government officials may not avoid the strictures of Section 1809(a)(2) by cultivating a state of deliberate ignorance when reasonable inquiry would establish that information was indeed obtained through unauthorized electronic surveillance. See e.g., United States v. Whitehall, 532 F.3d 746, 751 (8th Cir.) (where "failure to investigate is equivalent to 'burying one's head in the sand,'" willful blindness may constitute knowledge), cert. denied, 129 S. Ct. 610 (2008).

[redacted] Opinion at 115.

Approved for public release by the ODNI 20160415

> There may be cases where, after properly applying the targeting procedures, the government reasonably believes at the time it acquires a communication that a target is a non-U.S. person outside the United States, when in fact the target is a U.S. person and/or is in the United States. The acquisition of such communications is properly authorized under Section 1881a notwithstanding the fact that the government is prohibited from intentionally targeting U.S. persons or persons inside the United States, or intentionally acquiring a communication when it is known that all parties thereto are inside the United States.

September 4, 2008 Opinion at 26 (emphasis in original). Accordingly, the domestic communications that the NSA acquires when non-United States person targets who are reasonably believed to be outside of the United States are in fact in the United States are not subject to § 1809(a)(2), as their acquisition was authorized under Section 702.[55]

As noted above, the Court recognized a narrow, implicit exception to § 1809(a)(2) in the December 2010 [redacted] December 2010 [redacted] at 8. Specifically, the Court recognized an exception for use or disclosure of the "results of unauthorized surveillance [that] are needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future." Id. The Court made clear that this exception applied to "actions that are necessary to mitigate or prevent the very harms at which Section 1809(a)(2) is addressed." Id. (emphasis in original).

The government made clear at the October 8 Hearing that it has not parsed through the data in [redacted] and [redacted] to determine what portion of it is subject to § 1809(a)(2).

---

[55] A different situation would be presented if the NSA failed to detask a Section-702 tasked selector after it knew the user entered the United States. In this case, the ongoing collection of "roamer communications" would exceed the authorization to acquire communications under Section 702. See 50 U.S.C. § 1881a(a) (providing for authorization of "the targeting of persons reasonably believed to be located outside the United States").

Approved for public release by the ODNI 20160415

October 8 Transcript at 30. The government made a general argument in its written submission, however, that the retention and use in [redacted] and [redacted] of information that is otherwise subject to purge falls within the narrow, implicit exception to § 1809(a)(2) recognized in the December 2010 [redacted] discussed above. Government's October 21, 2015 Response at 21, 25. The Government's October 21, 2015 Response repeatedly emphasized that the retention of information in [redacted] and [redacted] that has been placed on the MPL plays a significant role in preventing unauthorized surveillance in the future. See e.g., Government's October 21, 2015 Response at 22-23, 25-27. While the Court finds it plausible that some information in [redacted] and [redacted] that is otherwise subject to purge may fall within the Court's recognized exception to § 1809(a)(2), the Court is simply not in a position to ascertain what portion of that information meets the standard for the narrow exception. As described in the May 2011 [redacted], the determination of whether the use or disclosure of unauthorized electronic surveillance falls within the exception to § 1809(a)(2) is a fact-driven assessment and involves an analysis of whether the use or disclosure of that specific information is "necessary to avoid similar instances of over-collection (e.g., by identifying and remedying a technical malfunction) or to remedy a prior over-collection (e.g., by aiding the identification of over-collected information in various storage systems)." May 2011 [redacted] at 4-5. The Government's October 21, 2015 Response argued that a more programmatic or categorical approach to the exception is warranted in the context of Section 702 collection. Government's October 21, 2015 Response at 23-24, 27. That may be correct, but on the current record, the government has not made a persuasive case that all of the information that it wants to retain in

Approved for public release by the ODNI 20160415

[redacted] and [redacted] falls within this exception. In these circumstances, the Court simply cannot conclude whether or not the government's proposed course of action is wholly consistent with § 1809(a)(2). Nor does the Court have the authority to permit violations of § 1809(a)(2), even when they are de minimis.[56]

In summary, it is likely that most Section 702 information in [redacted] and [redacted] that is otherwise subject to purge pertains to roamer communications, and therefore may be retained under the NSA Minimization Procedures for collection avoidance purposes and generally does not implicate § 1809(a)(2). Other Section 702 information that the government proposes to retain in [redacted] and [redacted], notwithstanding generally

---

[56] As the Court explained in the [redacted] Opinion,

> To be sure, this Court, like all other Article III courts, was vested upon its creation with certain inherent powers. See In re Motion for Release of Court Records, 526 F. Supp. 2d 484, 486 (FISA Ct. 2007); see also Chambers v. NASCO, Inc., 501 U.S. 32, 43 (1991) ("It has long been understood that [c]ertain implied powers must necessarily result to our Courts of justice from the nature of the their institution. . . . "). It is well settled, however, that the exercise of such authority "is invalid if it conflicts with constitutional or statutory provisions." Thomas v. Arn, 474 U.S. 140, 148 (1985). And defining crimes is not among the inherent powers of the federal courts; rather, federal crimes are defined by Congress and are solely creatures of statute. Bousley v. United States, 523 U.S. 614, 620-21 (1998); United States v. Hudson, 11 U.S. (7 Cranch) 32, 34 (1812). Accordingly, when Congress has spoken clearly, a court assessing the reach of a criminal statute must heed Congress's intent as reflected in the statutory text. See, e.g., Huddleston v. United States, 415 U.S. 814, 831 (1974). The plain language of Section 1809(a)(2) makes it a crime for any person, acting under color of law, intentionally to use or disclose information with knowledge or reason to know that the information was obtained through unauthorized electronic surveillance. The Court simply lacks the power, inherent or otherwise, to authorize the government to engage in conduct that Congress has unambiguously prohibited.

[redacted] Opinion at 113 (footnote omitted).

applicable purge requirements, is limited in nature and also would be used for collection avoidance and other compliance-related purposes. For these reasons, the Court does not believe that the aforementioned issues related to [redacted] and [redacted] preclude a finding that the NSA Targeting Procedures and Minimization Procedures, taken as a whole, comply with the applicable statutory and Fourth Amendment requirements. The Court does expect, however, to hear more from the government about how it is applying the destruction requirements of those procedures to Section 702 information in [redacted] and [redacted] at the compliance hearing to be held in early 2016. Finally, the Court cannot find, at least on the current record, that the information the government proposes to retain in [redacted] and [redacted] falls entirely within the implicit exception to § 1809(a)(2)'s prohibition on disclosure and use.

IV. CONCLUSION

For the foregoing reasons, the Court finds that: (1) the 2015 Certifications, as well as the certifications in the Prior 702 Dockets as amended by the 2015 Certifications, contain all the required statutory elements; (2) the targeting and minimization procedures to be implemented regarding acquisitions conducted pursuant to the 2015 Certifications 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 certifications, 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. The government shall submit a report to the Court by December 18, 2015, describing a) how the NSA plans to comply with its targeting and minimization procedures with respect to the categories of information in [redacted] and [redacted] that are identified on pages 71-72 of this opinion, or alternatively, b) how the retention and use of the aforementioned categories of information in [redacted] and [redacted] comports with the NSA's targeting and minimization procedures.

2. The government shall promptly submit in writing a report describing each instance in which NSA or CIA invokes the provision of its minimization procedures stating 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 NSA Minimization Procedures at 1; CIA Minimization Procedures at 4-5. Each such report should describe the circumstances of the deviation from the procedures and identify the specific mandate on which the deviation was based.

3. The government shall promptly submit in writing a report concerning 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. 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 is consistent with the applicable minimization procedures.

4. The government shall provide substantive updates on each of the four compliance issues discussed herein at a hearing to be held on January 27, 2016, at 11 A.M.

ENTERED this 6th day of November, in [redacted].

Thomas F. Hogan

THOMAS F. HOGAN
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]

~~SECRET~~

Filed
United States Foreign
Intelligence Surveillance Court

NOV 0 6 2015

LeeAnn Flynn Hall, Clerk of Court

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

ORDER

For the reasons stated in the Memorandum Opinion and Order issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications referenced above contain all the required statutory elements and that the targeting procedures and minimization procedures approved for use in connection with those certifications are consistent with the requirements of 50 U.S.C. §1881a(d)-(e) and with the Fourth Amendment.

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications and the use of such procedures are approved.

ENTERED this 6th day of November 2015, in [redacted].

Thomas F. Hogan

THOMAS F. HOGAN
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]

~~SECRET~~