

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

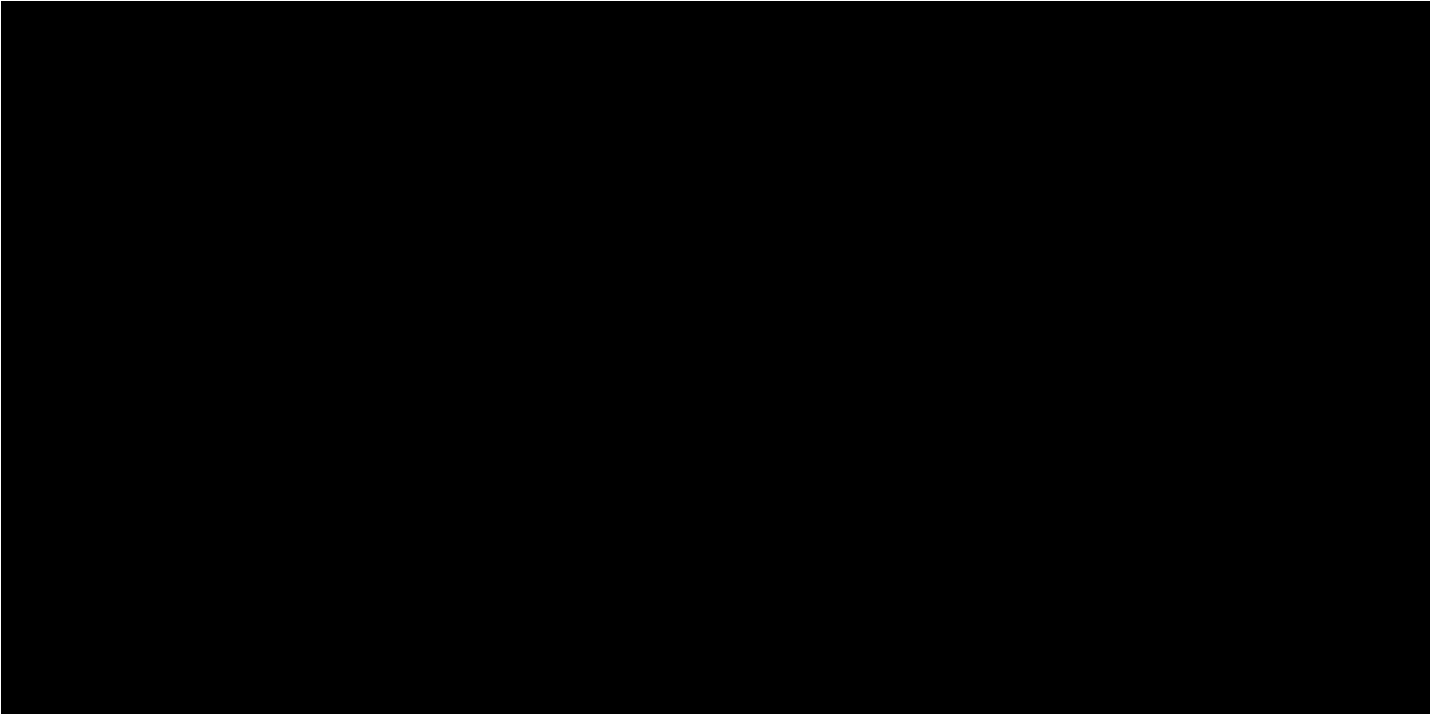
NOV 18 2020

UNITED STATES

LeeAnn Flynn Hall, Clerk of Court

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.



MEMORANDUM OPINION AND ORDER

The Foreign Intelligence Surveillance Court today addresses 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,” filed on October 19, 2020 (“October 19, 2020, Submission”). This Submission is subject to review under Section 702 of the Foreign Intelligence Surveillance Act (FISA) as amended, codified at 50 U.S.C. § 1881a. The government’s request for approval of the certifications and related procedures is *granted* for the reasons stated in this Memorandum

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

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

Opinion and Order, subject to certain reporting and other requirements set forth at the end of this document.

This Submission is largely a status-quo replacement of certifications and procedures approved by the Court in its Memorandum Opinion and Order dated December 6, 2019. See Docket Nos. [REDACTED] Mem. Op. and Order, Dec. 6, 2019 (“December 6, 2019, Opinion”). Part I of this Opinion summarizes the government’s submissions. In Part II, the Court finds that the certifications before it contain the elements required by Section 702(h). Part III addresses the targeting procedures. The Court examines the proposed minimization procedures and querying procedures in Part IV, concluding that they satisfy the requirements of the statute.

In Part V, the Court evaluates the proposed procedures under the requirements of the Fourth Amendment and finds that, as written, they are consistent with those requirements. Part VI examines issues regarding implementation of, and compliance with, Section 702 procedures, again concluding that the overall state of compliance and implementation permits a finding that the procedures, as implemented, comport with statutory and Fourth Amendment requirements.

Finally, in Part VII, the Court summarizes its disposition and imposes certain reporting and other requirements on the government.

I. THE GOVERNMENT’S SUBMISSION

A. The 2020 Certifications and Amendments

The October 19, 2020, Submission includes [REDACTED] certifications executed by the Attorney General and the Director of National Intelligence pursuant to Section 702: [REDACTED]

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

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

[REDACTED]

Each of those certifications (collectively referred to as “the 2020 Certifications”) is accompanied by:

- (1) Supporting affidavits of the Director of the NSA, the Director of the FBI, the Director of the CIA, and the Director of the National Counterterrorism Center (NCTC);
- (2) Two sets of targeting procedures, which govern NSA and the FBI, respectively. The targeting procedures for NSA appear as Exhibit A to each certification, and those for the FBI appear as Exhibit C. The targeting procedures for each certification are identical;
- (3) Four sets of minimization procedures, which govern NSA, the FBI, the CIA, and NCTC, respectively. The minimization procedures for NSA appear as Exhibit B to each certification, those for the FBI appear as Exhibit D, those for the CIA appear as Exhibit E, and those for NCTC appear as Exhibit G. (Exhibit F [REDACTED] identifies the individuals or entities targeted under those certifications, [REDACTED]) The minimization procedures for each certification are identical; and
- (4) Four sets of querying procedures, which govern NSA, the FBI, the CIA, and NCTC, respectively. The querying procedures for NSA appear as Exhibit H to each certification, those for the FBI appear as Exhibit I, those for the CIA appear as Exhibit J, and those for NCTC appear as Exhibit K. The querying procedures for each certification are identical.

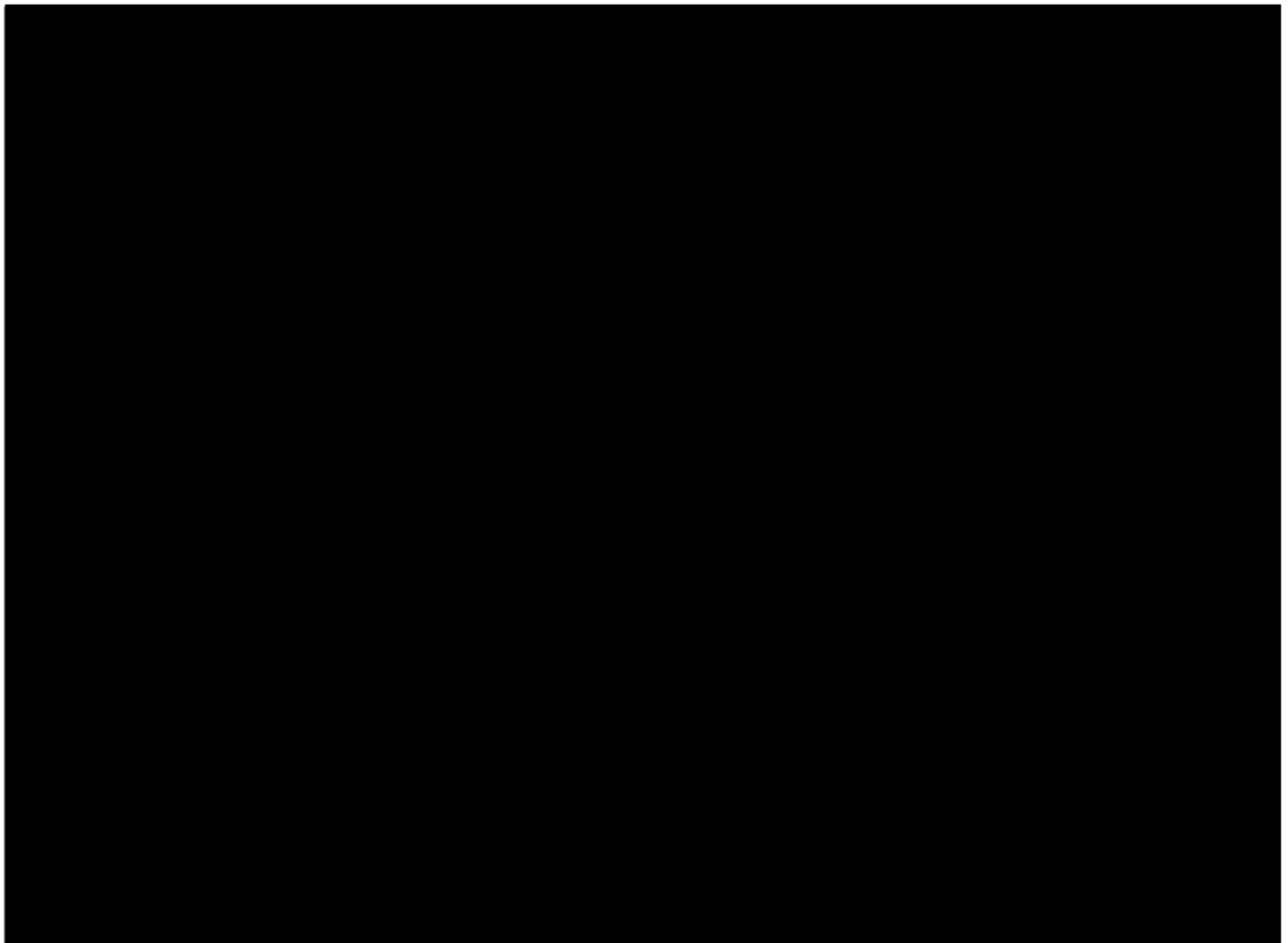
Except where otherwise noted, references to any of the procedures just described are to the version of those procedures accompanying the 2020 Certifications. The October 19, 2020, Submission also includes an explanatory memorandum prepared by the Department of Justice (“October 19, 2020, Memorandum”). The Court is required to review and rule on the certifications and procedures within 30 days of their submission – i.e., by November 18, 2020, see § 702(j)(1)(B), which it has done.

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

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

B. Subject Matter of the Certifications

Each certification involves “the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information.”



The 2020 Certifications generally propose to continue acquisitions of foreign-intelligence information now being conducted under prior certifications that were initially submitted on September 17, 2019 (“the 2019 Certifications”), and addressed by the Court in its December 6, 2019, Opinion. See Oct. 19, 2020, Memorandum at 2. The 2019 Certifications are similarly

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

Page 4

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

differentiated by subject matter [REDACTED] covering the same subjects as the corresponding 2020 Certifications.

The 2019 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. See Docket Nos [REDACTED]

[REDACTED] Those docket numbers, together with Docket Numbers [REDACTED] are collectively referred to as “the Prior 702 Dockets.”

The government also seeks approval of amendments to the certifications in the Prior 702 Dockets, such that NSA, the CIA, the FBI, and NCTC henceforward would apply the same minimization and querying procedures to information obtained under prior certifications as they would to information to be obtained under the 2020 Certifications. See Oct. 19, 2020, Memorandum [REDACTED]

II. REVIEW OF THE 2020 CERTIFICATIONS AND PRIOR CERTIFICATIONS, AS AMENDED

The Court must review a Section 702 certification “to determine whether [it] contains all the required elements.” § 702(j)(2)(A). Its examination of the 2020 Certifications confirms that:

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

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

(1) the certifications have been made under oath by the AG and the DNI, as required by § 702(h)(1)(A), see [REDACTED]

(2) the certifications contain the attestations required by § 702(h)(2)(A), see [REDACTED]

(3) as required by § 702(h)(2)(B), each certification is accompanied by targeting procedures and minimization procedures adopted in accordance with § 702(d) and (e), respectively;

(4) each certification is supported by affidavits of appropriate national-security officials, as described in § 702(h)(2)(C); and

(5) each certification includes an effective date in compliance with § 702(h)(2)(D) – specifically, the certifications become effective on November 18, 2020, or the date upon which the Court issues an order concerning the certifications under § 702(i)(3), whichever is later. See [REDACTED]

[REDACTED] (The statement described in § 702(h)(2)(E) is not required because there was no “exigent circumstances” determination under § 702(c)(2).)

The Court, accordingly, concludes that the 2020 Certifications contain all the required statutory elements. Similarly, it has reviewed the certifications in the Prior 702 Dockets, as amended by the 2020 Certifications, and finds that they also contain all the elements required by the statute. Those amendments have the same effective dates as the 2020 Certifications. See [REDACTED]

The requisite procedural boxes having been checked, the Court moves on to proposed targeting, querying, and minimization procedures. The following discussion primarily focuses on proposed changes to the previously approved procedures, but the procedures as a whole must be consistent with statutory and constitutional requirements. Some technical, conforming edits and other changes are not specifically discussed because they raise no issues material to the Court’s

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

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

review (to include changes to the Executive Branch's classification determinations with respect to certain portions of the procedures).

III. THE TARGETING PROCEDURES

Targeting procedures must be “reasonably designed” to “ensure that any acquisition authorized under [§ 702(a)] 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.” § 702(d)(1); see also § 702(b)(1) (acquisitions “may not intentionally target any person known at the time of acquisition to be located in the United States”); § 702(b)(4) (acquisitions “may not intentionally acquire 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”). Additionally, the government uses the targeting procedures to ensure that acquisitions do “not intentionally target a United States person reasonably believed to be located outside the United States.” § 702(b)(3). Pursuant to § 702(j)(2)(B), the Court assesses whether the targeting procedures satisfy those criteria. It must also determine whether such procedures, along with the querying and minimization procedures, are consistent with the requirements of the Fourth Amendment. See § 702(j)(3)(A)-(B).

A. Background on Acquisition and Targeting Under Section 702

The government targets a person under Section 702 by tasking for acquisition one or more selectors (e.g., identifiers for email or other electronic-communication accounts) associated with that person. Section 702 encompasses different forms of acquisition. The government may acquire information “upstream,” as it transits the facilities of an Internet backbone

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

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

carrier, as well as “downstream,” from systems operated by providers of services [REDACTED] Traditional telephone communications may also be acquired upstream . . .

[REDACTED] Mem. Op. and Order, Oct. 18,

2018, at 11 (citation omitted) (“October 18, 2018, Opinion”).

NSA is the lead agency in making targeting decisions under Section 702. It may not task a selector without first determining that the target is reasonably believed to be a non-U.S. person outside the United States (a “foreignness determination”). In making such determinations, NSA reviews certain categories of information about the proposed target and evaluates “the totality of the circumstances based on the information available with respect to that person,” [REDACTED]

[REDACTED] NSA Targeting Procedures § I at 1. An NSA targeting decision must also be supported by a “particularized and fact-based” assessment that “the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information” relevant to the subject matter of an authorized Section 702 certification. *Id.* at 4.

NSA is also required to conduct post-targeting analysis “to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States is located in the United States.” NSA Targeting Procedures § II at 7. This post-targeting analysis involves routinely comparing each tasked selector against independently acquired information for indications that a tasked selector may be used

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

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

inside the United States, and examination of the content of communications obtained through surveillance of a tasked selector for indications that a targeted person is now in, or may enter, the United States. Id. at 7-8. If NSA concludes that a target is in the United States [REDACTED]

Id. § II at 8, § IV at 10.

NSA tasks selectors for [REDACTED]

[REDACTED] The FBI is the agency responsible for [REDACTED]

[REDACTED] and in that role is governed by its targeting procedures. Under those procedures, the FBI may [REDACTED] selectors that have already been approved for tasking [REDACTED] by NSA under its targeting procedures. See FBI Targeting Procedures § I.1. “Thus, the FBI Targeting Procedures apply in addition to the NSA Targeting Procedures,” [REDACTED] See Docket No. [REDACTED] Mem. Op., Sept. 4, 2008, at 20 (emphasis in original) (“September 4, 2008, Opinion”).

NSA [REDACTED] requests to the FBI and provides an explanation of its prior foreignness determination for each requested selector (or “Designated Account”). See FBI Targeting Procedures §§ I.1, I.2. The FBI, “in consultation with NSA, will review and evaluate the sufficiency of” that determination. Id. § I.3. The FBI also runs certain checks of information in its possession in the course of that review and evaluation.

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

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

“Unless the FBI [REDACTED] that the user of the Designated Account is a United States person or is located inside of the United States, the FBI will [REDACTED]

[REDACTED] Id. § I.5. “If the FBI [REDACTED]

[REDACTED] the Designated Account is not appropriate for tasking . . . , the FBI will inform NSA” and will not [REDACTED] that account unless and until it “determines that the Designated Account is in fact appropriate for tasking.” Id. § I.8.

Improvements to the procedures for information-sharing and coordination among FBI, NSA, and CIA on targeting decisions was a significant feature of the procedures accompanying the 2019 Certifications. The implementation of those revised procedures is discussed in Part VI below.

B. NSA Targeting Procedures

Only one noteworthy change is proposed to NSA’s Targeting Procedures. Certain notices that were previously required to be sent by NSA to the Office of the Director of National Intelligence Civil Liberties Protection Officer (ODNI CLPO) are now required to be sent to the ODNI Office of Civil Liberties, Privacy and Transparency. The required reports relate to certain incidents of noncompliance and incidents in which a person reasonably believed to be located outside the United States, and targeted under Section 702, is later determined to be inside the United States, or an individual reasonably believed to be a non-United States person is later assessed to be a United States person. See NSA Targeting Procedures § IV at 10.

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

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

The government states that this change was merely “to make clear where reporting will be directed.” Oct. 19, 2020, Memorandum at 5. The Court has no reason to believe that reports previously directed to the ODNI CLPO were ever confined to his exclusive purview, to the exclusion of other members of his office. Thus, as the Court understands it, there is no actual broadening of the universe of people who would have access to the reports at issue. The procedures simply now acknowledge that these reports are made to the office within ODNI that is charged with the protection of privacy and civil liberties, which the Court finds entirely appropriate. This change has no substantive impact on the overall reasonableness of the NSA procedures.

C. FBI Targeting Procedures

Likewise, the only noteworthy change to the FBI Targeting Procedures is that the FBI is now required to report incidents of noncompliance with its targeting procedures to the ODNI Office of Civil Liberties, Privacy and Transparency, rather than the ODNI CLPO. See FBI Targeting Procedures § III.15. Again, the government characterizes this as a clarifying edit, see Oct. 19, 2020, Memorandum at 5, and the Court finds that it has no impact on the overall reasonableness of the FBI procedures.

D. Conclusion

This Court has previously found the current versions of the FBI and NSA’s targeting procedures to comply with statutory requirements. See Dec. 6, 2019, Opinion at 23, 78. The modest changes to those procedures discussed above have no substantive impact on it’s prior conclusions in this regard. The Court concludes, accordingly, that the

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

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

2020 NSA Targeting Procedures and the 2020 FBI Targeting Procedures, as written, are reasonably designed, as required by Section 702(d)(1), to: (1) ensure that any acquisition authorized under the 2020 Certifications is limited to targeting persons reasonably believed to be located outside the United States, and (2) 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. For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, moreover, it 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 31-35 infra.

IV. THE MINIMIZATION PROCEDURES AND QUERYING PROCEDURES

Pursuant to § 702(j)(2)(C), the Court must also assess whether the minimization procedures comply with specified statutory requirements. Section 702(e)(1) requires that the procedures “meet the definition of minimization procedures under [50 U.S.C. § 1801(h) or 1821(4)].” That definition requires

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

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)],

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

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

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[.]

§ 1801(h). The definition of “minimization procedures” at § 1821(4) is substantively identical to the definition at § 1801(h) (although § 1821(4)(A) refers to “the purposes . . . of the particular physical search”). For simplicity, subsequent citations refer only to § 1801(h).

In applying these statutory requirements, the Court is mindful that Section 702 acquisitions target persons reasonably believed to be non-U.S. persons outside the United States. Although such targets may communicate with or about U.S. persons, Section 702 acquisitions, as a general matter, are less likely to acquire information about U.S. persons that is unrelated to the foreign-intelligence purpose of the acquisition than, for example, electronic surveillance or physical search of a home or workplace within the United States that a target shares with U.S. persons. Different minimization protections, accordingly, may be appropriate for other forms of collection that are directed at persons within the United States.

The AG, in consultation with the DNI, also must “adopt querying procedures consistent with the requirements of the fourth amendment . . . for information collected” pursuant to a Section 702 certification, see § 702(f)(1)(A), and must “ensure” that those

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

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

procedures “include a technical procedure whereby a record is kept of each United States person query term used for a query.” § 702(f)(1)(B). The FISC must determine whether querying procedures satisfy the requirements of § 702(f)(1). See § 702(j)(3)(A)-(B).

Each agency’s procedures make clear that the querying and minimization procedures are to be read and applied together. See, e.g., NSA Querying Procedures § I (“These querying procedures should be read and applied in conjunction with [the separate] minimization procedures, and nothing in these procedures permits any actions that would otherwise be prohibited by those minimization procedures.”); FBI Querying Procedures § I (same); NSA Minimization Procedures § I (“These minimization procedures apply in addition to separate querying procedures. . . . [They] should be read and applied in conjunction with those querying procedures, and nothing in these procedures permits any actions that would otherwise be prohibited by those querying procedures.”); FBI Minimization Procedures § I.A (same). The Court will, as a result, also assess whether each agency’s querying procedures, in conjunction with the minimization procedures, satisfy the standard of § 1801(h).

A. Background on Section 702 Minimization and Querying

Each agency with access to “raw,” or unminimized, information obtained under Section 702 (NSA, FBI, CIA, and NCTC) is governed by its own set of minimization procedures in handling that information. This opinion uses the terms “raw” and “unminimized” interchangeably. The NCTC Minimization Procedures define “raw” information as:

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

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

section 702-acquired information that (i) is in the same or substantially the same format as when NSA or FBI acquired it, or (ii) has been processed only as necessary to render it into a form in which it can be evaluated to determine whether it reasonably appears to be foreign intelligence information or to be necessary to understand foreign intelligence information or assess its importance.

NCTC Minimization Procedures § A.3.d.

There are significant differences among the various sets of minimization procedures based on factors such as the agencies' differing missions, legal and policy constraints, and technical infrastructure, but they share several important features in common. Regarding acquisition, NSA is required to conduct acquisitions "in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition." NSA Minimization Procedures § 4(a). The FBI must follow its targeting procedures in conducting acquisitions. See FBI Minimization Procedures § II.A.1. (As discussed above, NSA and the FBI are the only agencies that conduct Section 702 acquisitions, and the FBI applies its targeting procedures to, and acquires data for, only selectors that NSA has approved for tasking under its targeting procedures. See pages 7-10 supra).

Post-acquisition, in broad outline, each agency's procedures:

- set criteria for the indefinite retention of information of or concerning United States persons and generally applicable timetables for destroying information that does not meet those criteria, see NSA Minimization Procedures § 4; FBI Minimization Procedures §§ III.C.1.b, III.D.4, III.E.4; CIA Minimization Procedures §§ 2, 3; NCTC Minimization Procedures §§ B.2, B.3;

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

Page 15

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

- provide special rules for protecting attorney-client communications, see NSA Minimization Procedures § 5; FBI Minimization Procedures §§ III.D.5, III.E.6; CIA Minimization Procedures § 7.a; NCTC Minimization Procedures § C.5;
- set standards and procedures for disseminating information, see NSA Minimization Procedures §§ 6, 7(b); FBI Minimization Procedures § IV; CIA Minimization Procedures §§ 5, 7.c; NCTC Minimization Procedures § D; and
- prescribe procedures for obtaining technical or linguistic assistance from other agencies and/or from foreign governments, see NSA Minimization Procedures § 9(b); FBI Minimization Procedures § IV.D; CIA Minimization Procedures § 7.b; NCTC Minimization Procedures § D.5.

The procedures also speak to situations in which the government reasonably believed at the time of acquisition that the target was a non-U.S. person outside the United States, but when the target was in fact a U.S. person or was inside the United States. The Court has concluded that the government is authorized to acquire such communications under Section 702. See Sept. 4, 2008, Opinion at 25-27. Nonetheless, the procedures of each agency require destruction of information obtained under those circumstances, unless the head of the agency authorizes its retention after making certain findings for the specific information to be retained. See NSA Minimization Procedures § 4(d); FBI Minimization Procedures § III.A.3; CIA Minimization Procedures § 8; NCTC Minimization Procedures § B.4.

In addition, each agency's querying procedures contain recordkeeping requirements for the use of U.S.-person query terms in response to § 702(f)(1)(B). See NSA Querying Procedures § IV.B; FBI Querying Procedures § IV.B; CIA Querying

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

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

Procedures § IV.B; NCTC Querying Procedures § IV.B. They permit investigative and analytical personnel at the CIA, NSA, and NCTC to conduct queries of unminimized Section 702 information if the queries are reasonably likely to return foreign-intelligence information. See NSA Querying Procedures § IV.A; CIA Querying Procedures § IV.A; NCTC Querying Procedures § IV.A. Their FBI counterparts may conduct such queries if they are reasonably likely to return foreign-intelligence information or evidence of a crime. See FBI Querying Procedures § IV.A.

The October 19, 2020, Submission does not propose any changes to the NSA or CIA minimization procedures; nor does it propose changes to the FBI or CIA querying procedures. See Oct. 19, 2020, Memorandum at 3 n.3. Changes to the FBI Minimization Procedures are limited to an updated statutory citation and classification markings. Nothing detracts from the Court's earlier findings that these procedures as written are statutorily and constitutionally sufficient. Proposed substantive changes to the NCTC minimization procedures and NCTC and NSA querying procedures are discussed in the following sections B, C, and D, respectively. Section E addresses clarifications made by the government regarding its interpretation of provisions of the NSA, CIA, and NCTC minimization procedures relating to the retention and internal handling of attorney-client privileged communications.

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

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

B. NCTC Minimization Procedures

The government proposes to change all references to “NCTC employees” in NCTC’s minimization procedures to “NCTC personnel.” The NCTC procedures previously defined the term “NCTC employee” to include:

(i) individuals directly employed by NCTC, (ii) personnel detailed to NCTC from other departments or agencies who work under NCTC management and supervision in a manner substantially the same as individuals directly employed by NCTC, and (iii) contractors working under NCTC management and supervision who are authorized to perform services in support of NCTC on FISA-related matters.

2019 NCTC Minimization Procedures § A.3.b.

The proposed new definition of “NCTC personnel” in the NCTC procedures faithfully tracks the prior definition of “NCTC employees,” with the exception of substituting the word “individuals” for “personnel” in part (ii) thereof, presumably to avoid circularity. See NCTC Minimization Procedures § A.3.b. The government explains that this change in terminology “more clearly reflect[s] the scope of application, as defined therein to include employees as well as certain individuals detailed to NCTC and contractors working under NCTC management and supervision.” Oct. 19, 2020, Memorandum at 7.

The Court views this as a change of emphasis rather than of substance. The effective scope of the operative definition remains unchanged. It also better reflects the nature of NCTC’s multifaceted workforce. As the NCTC website points out:

NCTC is staffed by more than 1,000 personnel from across the [Intelligence Community], the Federal government, and federal contractors. Forty percent

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

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

of NCTC's workforce represents approximately 20 different departments and agencies – a tribute to the recognition by the intelligence, homeland security, and law enforcement communities of NCTC's role in protecting the Nation against terrorist threats.

National Counterterrorism Center, <http://www.dni.gov/index.php/nctc-who-we-are/history> (visited Oct. 21, 2020).

In other changes, references to two positions are altered in Sections B.2.a and B.2.b of the proposed NCTC Minimization Procedures, governing retention of Section 702-acquired information. The former provision allows holders of these two positions to waive the requirement that unreviewed information must be purged from NCTC systems five years after the expiration date of the certification authorizing the collection, provided certain findings are made by one of these individuals. The latter provision requires approval from a holder of one of these two positions to access data that has been reviewed, but not identified as meeting the standard for retention, more than ten years after the expiration of the certification authorizing the collection.

For purposes of these provisions, references to the Deputy Director for Intelligence are replaced with the Assistant Director for Intelligence. References to the Deputy Director of Terrorist Identities are replaced with the Assistant Director for Identity Intelligence. The government represents that the proposed substitutions “reflect internal renaming of the positions at NCTC,” and that the “referenced position[s] and duties of the individuals in these positions remain the same.” Oct. 19, 2020, Memorandum at 8.

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

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

In contrast, a change proposed to Section D.3.b, relating to disseminations, expands the universe of individuals who may, in coordination with the office of NCTC Legal Counsel, approve disseminations of Section 702-acquired information concerning United States persons to [REDACTED]

[REDACTED] Previously, such approval had to come from the NCTC

Director “or a designee who shall hold a position no lower than Group Chief within the NCTC Directorate of Intelligence.” 2019 NCTC Minimization Procedures § D.3.b. The proposed revised procedures would extend to such an individual within the separate Directorate of Identity Intelligence. See NCTC Minimization Procedures § D.3.b.

The government represents that this change is precipitated by an “internal NCTC realignment moving an analytic group responsible for identifying and locating members of terrorist networks from the Directorate of Intelligence to the Directorate of Identity Intelligence. The group’s chief and functions remain unchanged.” Oct. 19, 2020, Memorandum at 8. The government reiterates that the change is designed to preserve the Director’s ability to continue to delegate dissemination determinations to “this group chief.” Id.

This proposed change gives the Court pause. That the change is purportedly necessitated by the transfer of one analytic group to another directorate does not mean that the practical effect of the proposed change would be limited to that group. Presumably there are other groups within the Directorate of Identity Intelligence, and, on its face, this change would allow the NCTC Director to delegate dissemination

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

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

determinations to chiefs of those other groups, as well as to other, more senior officials within the Directorate of Identity Intelligence, none of whom currently can be delegated such authority.

To be sure, the Court does not second-guess internal organizational decisions made by the Executive. The Court, moreover, has no objection in principle to the maintenance of the status quo vis-à-vis the group, previously within the Directorate of Intelligence, and now within the Directorate of Identity Intelligence, that is “responsible for identifying and locating members of terrorist networks.” *Id.* But the Court has not been provided enough information about other groups within the Directorate of Identity Intelligence to know whether extension of delegated authority to chiefs of those other groups to authorize [REDACTED] disseminations is equally appropriate. The Court will approve the proposed change, but require the government to report in the future on the exercise of the delegation authority to any group chief or official within the Directorate of Identity Intelligence other than the one specifically discussed in the government’s submission.

Finally, another change, made at the Court’s suggestion, is now reflected in Section B.3 of the NCTC Minimization Procedures. That section allows essentially indefinite retention of information concerning a U.S. person that meets specified standards. As amended, it concludes with the following caveat: “Information that is evidence of a crime . . . but is not foreign intelligence information, may only be retained and disseminated for law enforcement purposes.” NCTC Minimization Procedures § B.3 (emphasis added). Previously, there was an “or” in place of the emphasized “and.”

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

Page 21

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

The Court was concerned that, if read disjunctively, the “or” might have been interpreted to allow NCTC to retain information, purportedly for a valid law-enforcement purpose, whether or not it disseminated the information to appropriate law-enforcement officials. The revised provision makes clear that NCTC, which has no law-enforcement mission or authority, may only retain “evidence-of-a-crime” information that is not foreign-intelligence information for purposes of disseminating it to law-enforcement authorities.

The Court has examined the foregoing provisions, as revised in the NCTC Minimization Procedures, and concludes that they are consistent with finding that the proposed procedures satisfy the applicable definition of “minimization procedures.”

C. NCTC Querying Procedures

Consistent with its revised minimization procedures, and for the same reasons discussed above, NCTC has proposed to replace references to “NCTC employees” in its querying procedures with the term “NCTC personnel.” The Court concludes that the NCTC querying procedures, with this change, continue to comport with the statutory standards for such procedures.

D. NSA Querying Procedures

A single change is proposed to NSA’s querying procedures. Those procedures provide generally that queries of unminimized Section 702 information contained in NSA systems must be reasonably likely to return foreign-intelligence information as defined by FISA, unless an exception specified in the procedures applies. See NSA Querying

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

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

Procedures § IV.A. Among the exceptions are enumerated circumstances in which non-conforming queries may be necessary to perform “lawful oversight functions of NSA’s personnel or systems.” Id. § IV.C.6. Those functions include remediating compliance incidents, remediating spills of classified information, identifying data subject to purge, and performing quality control and auditing functions. Id. NSA is also permitted to deviate from the procedures to perform other oversight functions, not specifically enumerated in the procedures, provided it consults with NSD and ODNI prior to conducting such a query. NSD, in turn, is required to promptly report the deviation to the Court. Id.

In a notice filed on January 22, 2020, the government informed the Court that NSA had developed a method, [REDACTED] of known or suspected child-exploitation material (including child pornography), to identify and remove such material from NSA systems. To test this methodology, NSA ran the [REDACTED] [REDACTED] against a sample of FISA-acquired information in NSA systems. The government concedes that queries conducted for such purposes do not meet the generally applicable querying standard; nor do they fall within one of the lawful oversight functions enumerated in the existing NSA querying procedures. Nevertheless, NSD/ODNI opined that “the identification and removal of child exploitation material . . . from NSA systems is a lawful oversight function under section IV.C.6,” and that the deviation from the querying procedures was “necessary to perform this lawful oversight function of NSA

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

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

systems.” Notice of Deviation from Querying Procedures, January 22, 2020, at 3; see Oct. 19, 2020, Memorandum at 10.

NSA anticipates using such queries going forward, likely on a recurring basis, to proactively identify and remove child-exploitation material from its systems. The government submits that doing so is necessary to “prevent [NSA] personnel from unneeded exposure to highly disturbing, illegal material.” October 19, 2020, Memorandum at 10. The Court credits this suggestion and likewise finds that performance of these queries qualifies as a lawful oversight function for NSA systems. But the Court encouraged the government to memorialize this oversight activity in § IV.C.6, among the other enumerated lawful oversight functions that are recognized exceptions to the generally applicable querying standards.

The government has done so. Section IV.C.6 now includes a new provision for “identify[ing] and remov[ing] child exploitation material, including child pornography, from NSA systems.” NSA Querying Procedures § IV.C.6.f. The Court finds that the addition of this narrow exception has no material impact on the sufficiency of the querying procedures taken as a whole.

E. Clarification Regarding Segregation of Attorney-Client Privileged Communications by NSA, CIA, and NCTC

NSA, CIA, and NCTC’s minimization procedures require that certain attorney-client privileged communications acquired pursuant to Section 702 be “segregated” by the respective agency – specifically, those pertaining to a criminal charge in the United

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

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

States, [REDACTED]

See NSA Minimization Procedures § 5(c)

and (e); CIA Minimization Procedures § 7.a.(3) and (5); NCTC Minimization Procedures § C.5.c. and e. The FBI, as a law-enforcement agency, has more detailed procedures for handling attorney-client privileged communications, including, in the case of an individual charged with a crime in the United States, a requirement that the FBI sequester privileged communications relating to the charged offense with the Court. See FBI Minimization Procedures § III.D.5.a and b.

In response to questions from the Court about the manner in which the segregation requirement was being implemented by NSA, CIA, and NCTC, the government offered clarification in the memorandum accompanying the 2019 Certifications. It reported that access to such communications at CIA is limited to “personnel who require access in order to evaluate and process the communication under the attorney-client provisions of CIA’s procedures.” Sept. 17, 2019, Memorandum at 59. The government later clarified that the same was true with respect to NCTC. See Government’s Ex Parte Notice of Clarification Regarding NCTC’s Minimization Procedures, Docket Nos. [REDACTED]

[REDACTED] Although NCTC analysts would be made aware of the existence of the segregated communication, the analysts would not be able to view the contents of the communication. Id. Only a “small number” of technical and compliance personnel would be allowed such access. Id.

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

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

The only change noted in the current submission relates to NSA's implementation of the segregation requirement. In connection with the 2019 Certifications, the government represented that

when communications containing information protected by the attorney-client privilege are segregated at NSA, NSA personnel mark the communications for quarantine on NSA's Master Purge List (MPL). Communications that are marked for quarantine on the MPL remain discoverable by NSA personnel but may not be used in taskings made pursuant to section 702, any FISA application submitted to the Court, or any reporting product, except as permitted by the dissemination restrictions in the attorney-client privilege provisions of the procedures.

Sept. 17, 2019, Memorandum at 59.

The Court expressed concern that this construct, in which the attorney-client privileged communication remained accessible to all NSA analytic personnel who were otherwise authorized to access Section 702-acquired information, did not constitute "segregation" as that term was used in the procedures and was insufficiently protective of the privilege inherent in those communications.

In response to the Court's concerns, the government now reports that

NSA is implementing a process, which will be in place no later than October 30, 2020, adjusting the attorney-client communication segregation process previously described to the Court, which restricted authorized use of attorney-client privileged communications. This new process will limit access to each segregated communication. Only a designated number of individuals, who require access for a specific foreign intelligence purpose, will be authorized to access these communications. This access control is accomplished [REDACTED]

[REDACTED] that prevent access to content. This process is consistent with NSA's data modernization efforts and will limit access, use, and dissemination to those NSA personnel who are authorized for the specific [REDACTED] at issue, rather than

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

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

all NSA personnel with general access to section 702-acquired information. The specific number of NSA personnel provided with access based on a [REDACTED] will vary based on the foreign intelligence contained in the acquired communication; however, the total number is unlikely to exceed [REDACTED] personnel agency-wide, at any given time.

Oct. 19, 2020, Submission at 13-14. The duration of authorized access to the information in the [REDACTED] will “vary based on the specific context of the intercepted communication,” and any dissemination will be in accordance with otherwise applicable procedures. Id. at 14.

NSA’s procedures place numerous restrictions on the dissemination of privileged communications in the categories described above. Disseminations of such information must be limited [REDACTED] NSA Minimization Procedures § 5(g), (h). Among other requirements:

- [REDACTED]
- [REDACTED]

- The dissemination must be labeled as privileged, only for use for intelligence purposes, and not for use in any trial, hearing, or other proceeding without the express approval of the Attorney General. Further dissemination must be approved by the AAG/NS. See NSA Minimization Procedures § 5(g); and

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

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

•

The Court acknowledges that the revised NSA process described above, utilizing  better comports with the common-sense meaning of the term “segregate,” and represents a significant improvement in the implementation of the segregation requirement in the NSA’s procedures. But the Court also notes that NSA continues to interpret the segregation requirement differently from the CIA and NCTC, both of which forgo analytic use of these sensitive categories of communications and limit access to technical and compliance personnel charged with implementing the attorney-client privilege requirements of their respective procedures.

The government does little by way of justifying the differing treatment of privileged communications by NSA. The Act makes clear that “no otherwise privileged communication obtained in accordance with” its provisions “shall lose its privileged character.” §1806(a). Protections for attorney-client privileged communications have long featured prominently in FISA minimization procedures, and the Court relies on them in assessing the overall reasonableness of those procedures.

On the other hand, the Court has previously approved the dissemination provisions in the NSA procedures highlighted above, which unambiguously contemplate the dissemination of attorney-client privileged communications of the types being

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

Page 28

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

discussed here [REDACTED] subject to certain limitations and requirements. Implicit in those dissemination provisions is the premise that NSA can use privileged communications in its possession for analytic purposes, with appropriate handling restrictions. The only question of moment is what it means for these communications to be “segregated” within NSA pursuant to its procedures.

Focusing on that narrower issue, the first question asks what the law requires. There is no statutory bar to analytic use of attorney-client privileged communications for valid foreign-intelligence purposes. Section 1806(a), discussed above, was included in the statute to make clear that a privileged communication did not lose its character as such by virtue of having been overheard by a third party (in this case, by the government, surreptitiously). See H.R. Rep. No. 95-1283 part I, at 87 (1978) (noting that this provision was designed “to change existing law as to the scope and existence of privileged communications only to the extent that it provides that otherwise privileged communications do not lose their privileged character because they are intercepted by a person not a party to the conversation”). The government does not challenge the privileged character of these communications by virtue of its having intercepted them.

Minimization procedures, in turn, need only be “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.” §1801(h)(1)

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

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

(emphasis added). As noted above, there are meaningful limitations in NSA's procedures on the retention, handling, and dissemination of privileged communications. Those procedures have been found to be constitutionally and statutorily sufficient on numerous prior occasions.

The further restriction of privileged communications to [REDACTED] enhances the privacy protection afforded those communications under NSA's procedures. The Court again concludes that NSA's procedures, as a whole and as applied to it, an agency with no law-enforcement mission or authority, are reasonably designed to protect the substantial privacy interests in attorney-client communications, consistent with the need to exploit those communications for legitimate foreign-intelligence purposes.

That being said, the government is admonished to guard against the possibility that NSA, in compliance with its procedures, might disseminate to FBI a report based on a privileged communication described in Section 5(c) of the NSA procedures (pertaining to a criminal charge in the United States) that, had the FBI obtained it through its own collection efforts, the FBI would be required to sequester with the Court under FBI Minimization Procedures § III.D.5.a and b. As noted above, such a dissemination could only be made by NSA with the approval of the AAG/NS.

F. Conclusion

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that, as written, the proposed minimization procedures for the FBI, NSA, CIA, and NCTC, in conjunction with the querying procedures for those agencies,

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

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

satisfy the definition of minimization procedures at 50 U.S.C. § 1801(h); and that those querying procedures satisfy the requirements of Section 702(f)(1).

V. FOURTH AMENDMENT REQUIREMENTS

The Court must also assess whether the proposed targeting, minimization, and querying procedures are consistent with the requirements of the Fourth Amendment. See § 702(j)(3)(A). That Amendment states:

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

“The touchstone of the Fourth Amendment is reasonableness.” In re Certified Question of Law, 858 F.3d 591, 604 (FISA Ct. Rev. 2016) (per curiam) (“In re Certified Question”). Although “[t]he warrant requirement is generally a tolerable proxy for ‘reasonableness’ when the government is seeking to unearth evidence of criminal wrongdoing, . . . it fails properly to balance the interests at stake when the government is instead seeking to preserve and protect the nation’s security from foreign threat.” Id. at 593. A warrant is not required therefore to conduct surveillance “to obtain foreign intelligence for national security purposes . . . directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.” In re Directives Pursuant to Section 105B of FISA, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (“In re Directives”). The FISC has repeatedly reached the same conclusion regarding Section 702 acquisitions. See, e.g., Docket Nos. [REDACTED]

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

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

Mem. Op. and Order, Nov. 6, 2015, at 36-37 (“November 6, 2015, Opinion”); Sept. 4, 2008, Opinion at 34-36.

In prior reviews of Section 702 procedures, the Court has assessed the reasonableness of the government’s procedures as a whole. See, e.g., Nov. 6, 2015, Opinion at 39 (assessing “the combined effect” of the targeting and minimization procedures); Oct. 18, 2018, Opinion at 85-88 (declining invitation of amici curiae to conduct Fourth Amendment evaluation of querying practices in isolation). Restrictions on how the government targets acquisitions under Section 702 and how it handles information post-acquisition limit the degree of intrusion on individual privacy interests protected by the Fourth Amendment. For reasons explained above, the Court has found that the proposed targeting procedures, as written, are reasonably designed to limit acquisitions to those targets reasonably believed to be non-United States persons located outside the United States. The Fourth Amendment does not protect the privacy interests of such individuals. See, e.g., Nov. 6, 2015, Opinion at 38; Sept. 4, 2008, Opinion at 37 (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990)).

To the extent U.S.-person information is acquired under Section 702 – e.g., when a communication between a U.S. person and a Section 702 target is intercepted – the government can reduce the intrusiveness of the acquisition for Fourth Amendment purposes by restricting use or disclosure of such information. See In re Certified Question at 609. The FISC has previously found that “earlier versions of the various agencies’ targeting and minimization procedures adequately protected the substantial

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

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

Fourth Amendment interests that are implicated by the acquisition of communications of such United States persons.” Nov. 6, 2015, Opinion at 38-39 (citing Docket Nos. [REDACTED] [REDACTED] Mem. Op. and Order, Aug. 26, 2014 (“August 26, 2014, Opinion”); Docket Nos. [REDACTED] Mem. Op., Aug. 30, 2013, at 6-11 (“August 30, 2013, Opinion”)). Specifically, “the combined effect of these procedures” was “to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated’ and to ensure that ‘non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary.’” Nov. 6, 2015, Opinion at 39 (citing Aug. 26, 2014, Opinion at 40).

The Court takes all of these factors into account in assessing the reasonableness of the procedures under the Fourth Amendment. Under the applicable totality-of-circumstances approach, it must balance “the degree to which [governmental action] intrudes upon an individual’s privacy” against “the degree to which it is needed for the promotion of legitimate governmental interests.” In re Certified Question at 604-05 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)). “The more important the government’s interest, the greater the intrusion that may be constitutionally tolerated.” In re Directives at 1012.

The Court regards the privacy interests at stake in Section 702 acquisition as substantial. The government tasks [REDACTED]

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

Page 33

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

non-U.S. persons for acquisition under Section 702. See, e.g., DNI Statistical Transparency Report Regarding Use of National Security Authorities (April 2020), at 14 (reporting an estimated number of 204,968 Section 702 targets in 2019, up from 164,770 in 2018). Although not separately quantified, there is thus presumably a substantial amount of information of or concerning United States persons acquired under Section 702.

On the other side of the constitutional balance, acquiring “foreign intelligence with an eye toward safeguarding the nation’s security serves . . . a particularly intense interest.” In re Certified Question at 606 (internal quotation marks omitted). For that reason, the FISC has observed that “the government’s investigative interest in cases arising under FISA is at the highest level and weighs heavily in the constitutional balancing process.” Id. at 608.

Measures to protect individual privacy can be decisive in the proper balancing of these interests:

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.

In re Directives at 1012.

In this case, the Court has carefully considered how the proposed procedures seek to protect private U.S.-person information from misuse. It concludes that, in combination, the proposed targeting, minimization, and querying procedures will

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

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

adequately guard against error and abuse, taking into account the individual and governmental interests at stake. It therefore finds that those procedures, as written, are consistent with the requirements of the Fourth Amendment.

VI. IMPLEMENTATION AND COMPLIANCE ISSUES

FISC review of the sufficiency of Section 702 procedures is not limited to the procedures as written, but also encompasses how they are implemented. See, e.g., Oct. 18, 2018, Opinion at 68. It is appropriate, accordingly, to examine significant issues regarding such implementation.

A. Targeting Procedures

[REDACTED] NSA and the CIA are required to provide certain target-identifying information to the FBI. See Dec. 6, 2019, Order at 23. Such identifying information expressly includes: [REDACTED]

[REDACTED] additional identifying information of the user of the Designated Account, to the extent that NSA assesses it would be useful to FBI for purposes of application of [the FBI's targeting] procedures."

2019 FBI Targeting Procedures § I.2. [REDACTED]

[REDACTED] The Court found that in providing greater specificity, these information-sharing requirements "should enhance the FBI's ability to research and

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

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

evaluate whether a target is a U.S. person or in the United States [REDACTED]

[REDACTED] December 6, 2019, Order at 23.

Because the government was unable to immediately implement these requirements given various system formatting, classification, and training issues, it committed to submitting progress reports to the Court every 45 days. Id. at 17. The Court has closely monitored this progress through review of seven reports submitted by the government. Notable reported improvements include, for example, training NSA's workforce to "document [REDACTED] and the development of procedures for passing [REDACTED] information in a format that is compatible with FBI's [REDACTED] See 45-Day Report Regarding Implementation of the Federal Bureau of Investigation Section 702 Targeting Procedures, Mar. 23, 2020, at 8 (45-Day Targeting Report). The CIA upgraded its FISA tasking system to accommodate [REDACTED] along with guidance to users on determining whether the additional information is known, "reliable," and "useful" to the FBI in applying its targeting procedures. See 45-Day Targeting Report, June 22, 2020 at 12-13. NSA has also trained its workforce [REDACTED] document and send known and reliable [REDACTED] information and continues to work with the FBI to document [REDACTED] compatible with FBI's [REDACTED] The FBI for its part trained its staff as of January 6, 2020, to [REDACTED] provided by NSA [REDACTED]

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

Page 36

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

as part of its querying process. See 45-Day Targeting Report, May 7, 2020, at 11-12. In its final report, the government advised that each agency has completed workforce training on the need to provide all specified target-identifying information and has in place the previously described procedural and technical elements to facilitate it. See 45-Day Targeting Report, Aug. 6, 2020.

In addition, there is reason to think that the revised procedures may be helping to protect against targeting U.S. persons or persons in the United States. [REDACTED]

[REDACTED] NSA terminated its collection of the tasked facility. See Preliminary Notice of Compliance Incident Regarding Section 702-tasks number, Oct. 19, 2020 (reporting a delay in detasking).

The government, however, is currently investigating a potential compliance incident involving NSA's not providing [REDACTED] information [REDACTED]

See FBI Targeting Procedures § 1.4. The Court

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

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

expects to be promptly advised of the results of the government's investigation of this potential compliance incident, and it will continue to monitor whether the implementation of these enhanced specificity requirements adequately protects against targeting U.S. persons or persons in the United States.

B. FBI Querying Issues

In conjunction with the 2019 Certifications, this Court approved amended FBI querying procedures on September 4, 2019. See Docket Nos. [REDACTED]

[REDACTED] Mem. Op. and Order, Sept. 4, 2019, at 16-17 ("September 4, 2019, Opinion"). Those procedures require the FBI:

(1) to keep records that identify which terms used to query unminimized Section 702 information are U.S.-person query terms, id. at 7-8, and

(2) to document in writing why a query involving a U.S.-person query term satisfies the querying standard before accessing the contents of communications retrieved by the query (except for queries that are subject to Section 702(f)(2)). Id. at 8-9. (This documentation requirement adopts a recommendation made by amici curiae. See Oct. 18, 2018, Opinion at 92-93, 96-97.)

See Dec. 6, 2019, Opinion at 62; FBI Querying Procedures § IV.B. In addition, the Court modified a previously imposed reporting requirement to require the government to report to the Court whenever the FBI conducted a query that did not relate to national security and was not covered by Section 702(f)(2). Id. at 71-73.

Because the FBI needed time to make necessary changes in its systems to comply with the new recordkeeping and documentation requirements, the Court ordered periodic reporting on their implementation. See Sept. 4, 2019, Opinion at 14-15, 17. At the time the Court approved the 2019 Certifications, the government had filed two such reports.

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

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

See Dec. 6, 2019, Opinion at 64. On March 5, 2020, it informed the Court that the FBI had concluded implementation of its amended Section 702 Querying Procedures, including deploying mandatory training, via its Virtual Academy platform, for all FBI personnel with access to unminimized Section 702-acquired information. See Report Regarding the FBI's Implementation of the FBI's Section 702 Querying Procedures, Docket Nos. [REDACTED] Mar. 5, 2020, ("Query Implementation Report, March 5, 2020"). For the reasons discussed below, the Court continues to be concerned about FBI querying practices involving U.S.-person query terms, including (1) application of the substantive standard for conducting queries; (2) queries that are designed to retrieve evidence of crime that is not foreign-intelligence information; and (3) recordkeeping and documentation requirements.

1. Violations of the Querying Standard

NSD has reported a number of compliance incidents that were discovered during oversight reviews at FBI field offices, which suggest that the FBI's failure to properly apply its querying standard when searching Section 702-acquired information was more pervasive than was previously believed. For example, between April 11, 2019, and July 8, 2019, a technical information specialist in the [REDACTED] who was conducting "limited background investigations" conducted approximately 124 queries of Section 702-acquired information using the names and other identifiers of: 1) individuals who had requested to participate in FBI's "Citizens Academy" – a program for business, religious, civic, and community leaders designed to foster greater understanding of the role of

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

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

federal law enforcement in the community; 2) individuals who needed to enter the field office in order to perform a particular service, such as a repair; and 3) individuals who entered the field office seeking to provide a tip or to report that they were victims of a crime. See Notice of compliance incidents regarding the FBI's querying of raw FISA-acquired information Feb. 5, 2020, at 2.

Similarly, between August 1, 2019, and October 18, 2019, a task-force officer in the FBI's [REDACTED] conducted approximately 69 queries using the names and identifiers of individuals [REDACTED]

[REDACTED] the officer conducted queries to determine whether the FBI could provide additional information on those persons. Id.

Other reported violations apparently resulted from the failure of FBI personnel to opt out of querying raw FISA-acquired information. See, e.g., Quarterly Report Concerning Compliance Matters Under Section 702, Mar. 2020, at 85-86 (Intelligence Analyst in [REDACTED] conducted 110 queries for analytic paper using [REDACTED]

[REDACTED] but did not intend for queries to run against all raw FISA-acquired information); see also Notice of compliance incidents regarding the FBI's [REDACTED] querying of raw FISA-acquired information, June 1, 2020 (analyst conducted queries for purpose of ongoing vetting of

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

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

confidential human sources, as well as conducting overly broad queries (e.g., [REDACTED]), and mistakenly failed to opt out of querying against raw FISA-acquired information).

The Court acknowledges, however, that the majority of these queries occurred prior to the implementation of the FBI's system changes and training regarding the requirement to document in writing why a query involving a U.S.-person query term is reasonably likely to return foreign-intelligence information or evidence of crime. In addition, the COVID-19 pandemic severely limited the government's ability to monitor the FBI's compliance once the system changes were implemented and users received training on those changes. See Quarterly Report concerning compliance matters under Section 702, June 2020, at 2 n. 2 ("June 2020 Quarterly Report") (NSD and ODNI temporarily suspended all onsite reviews at NSA, CIA, NCTC, and FBI).

The Court has previously assessed that the additional documentation requirements should "help ensure that FBI personnel . . . have thought about the querying standard and articulated why they believe it has been met" and prompt them "to recall and apply the guidance and training they have received on the querying standard." Dec. 6, 2019, Opinion at 68. In the absence of evidence to the contrary, and under these unique circumstances, the Court is willing to again conclude that the improper queries described above do not undermine its prior determination that, with implementation of the documentation requirement, the FBI's querying and minimization procedures meet statutory and Fourth Amendment requirements.

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

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

2. Failure to Get FISC Order Before Reviewing Results of Evidence-of-Crime Queries

Over the past year, the government has reported numerous incidents involving U.S.-person queries that were designed to return evidence of a crime unrelated to foreign-intelligence, as permitted by Section IV.A.1 of the FBI's Query Procedures. The government has never applied to the FISC for an order under Section 702(f)(2). But the manner in which the FBI's systems displayed Section 702-acquired information returned in response to such queries permitted users to view Section 702 contents under circumstances in which they were required to first obtain an order in accordance with Section 702(f)(2), or to report to the Court pursuant to the modified reporting requirement. See Dec. 6, 2019, Opinion at 70, 81.

For example, during an oversight review of the FBI's [REDACTED] the government discovered 40 queries that had been conducted in support of predicated criminal investigations relating to health-care fraud, transnational organized crime, violent gangs, domestic terrorism involving racially motivated violent extremists, as well as investigations relating to public corruption and bribery [REDACTED]

[REDACTED] None of these queries was related to national security, and they returned numerous Section 702-acquired products in response. See Notice of compliance incidents regarding the FBI's [REDACTED] querying of raw FISA-acquired information, Oct. 15, 2020, at 3-4. Another analyst ran a "batch query" using [REDACTED] accounts as query terms in connection with predicated criminal investigations relating to domestic terrorism that returned 33 Section

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

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

702-acquired products, but the FBI was unable to confirm whether any products were opened. Id. at 4.

The government discovered these and a number of similar violations during oversight reviews at seven FBI field offices. Of the reported instances in each field office, the FBI advised that none of the Section 702-acquired information returned was used in a criminal or civil proceeding or otherwise used for any investigative or evidentiary purpose, even when the Section 702 product displayed had been opened and reviewed. See, e.g., Notice of compliance incident regarding an FBI query of Section 702-acquired information designed to return evidence of a crime unrelated to foreign intelligence, May 4, 2020, at 2-3 (staff operations specialist opened and reviewed Section 702-acquired product that was returned in response to query designed to vet potential source in predicated criminal investigation relating to public corruption).

These reported violations are similar to those referenced in the December 6, 2019, Opinion, which suggests that similar violations of Section 702(f)(2) likely have occurred across the Bureau. See Dec. 6, 2019, Opinion at 70. But these query violations were discovered during a limited number of oversight reviews that occurred before NSD and ODNI suspended on-site reviews at FBI field offices because of the COVID-19 pandemic. Therefore, the reported violations involved queries that were conducted prior to the FBI's implementation of the systems changes in late November 2019, and prior to completion of the mandatory training on these new features or the Querying Procedures as amended.

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

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

While the Court is concerned about the apparent widespread violations of the querying standard — including violations of Section 702(f)(2) — it lacks sufficient information at this time to assess the adequacy of the FBI system changes and training, post-implementation. Under these unique circumstances, and in the absence of evidence to the contrary, the Court is willing to again conclude that the improper queries described above do not undermine its prior determination that, with implementation of the documentation requirement, the FBI's querying and minimization procedures meet statutory and Fourth Amendment requirements. The number and nature of the reported querying violations nonetheless suggest that ongoing monitoring and auditing will be critical to evaluating whether the current measures are adequate.

3. Recordkeeping and Documentation Requirements for U.S.-Person Query Terms

a. FBI's

As noted above, on March 5, 2020, the government informed the Court that the FBI had concluded implementation of its Section 702 Querying Procedures, including deploying training to FBI personnel with access to unminimized Section 702-acquired information. See Query Implementation Report, Mar. 5, 2020. The report explained that when a user is prompted to indicate whether a U.S.-person query is conducted to find only evidence of a crime, the system's default answer is "No." Unless the user changes the answer to "Yes," the system will permit a user to access the Section 702-acquired contents — even if a non-foreign-intelligence evidence-of-crime justification is entered. This sequencing mechanism differs from what the Court understood based on the

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

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

government's earlier representation that "a user must provide both a justification for the query, and an affirmative indication as to whether the query is an evidence-of-a-crime query." Query Implementation Report, Mar. 5, 2020, at 5-6 (emphasis in original).

In response to questions raised at a hearing conducted by secure teleconference on October 28, 2020, with representatives of the NSD, the FBI, and the ODNI, the FBI provided the Court with screenshots taken from the FBI's [REDACTED] of the sequence involved when conducting queries. See [REDACTED]

[REDACTED] Nov. 3, 2020 ("Nov. 3, 2020, letter"). The screenshots included the initial search page presented to [REDACTED] users, which allows users to choose whether to run queries against Section 702 information or to exclude Section 702 information. A radio button is displayed for each option, but the system defaults to include Section 702 information. If the user affirmatively selects to not include Section 702 information, the system will exclude such information from subsequent searches for 30 minutes, after which the system notifies the user that the "session" has expired, and it reverts to the default that includes Section 702 information.

Id.

When Section 702 information is included, a pop-up box appears, labeled "702 Query Term," and presents a drop-down menu requiring a user to select whether her query term is a "USPER, Presumed USPER, or Other (non-USPER or query term does not relate to a person)." Id. When FBI personnel indicate that they are conducting a

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

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

U.S.-person query, the system automatically blocks access to all Section 702-acquired content returned as a result of that query.

If a user tries to access the Section 702-acquired contents, she is prompted by another pop-up box to indicate whether the “Query [was] ONLY for Evidence of a Crime.” While the pop-up box has two radio buttons labeled “Yes” and “No,” the system automatically defaults to “No.” Id. An information icon available here states: “[I]f your query is being conducted solely to identify Evidence of a Crime (not Foreign Intelligence Information) and is in connection with a predicated criminal investigation that does not relate to the national security of the United States, then you must obtain a FISA court order or have exigent circumstances prior to viewing the content of any 702 results.” Id.

If a user accepts the default “No,” the system requires her to provide a justification indicating that the query was reasonably likely to retrieve foreign-intelligence information or evidence of a crime. This is done by selecting from a pre-populated list of options, or by selecting “other” and typing a justification in a free-text box. Once a justification is provided, the system will give the user access to the Section 702-acquired information even if she enters a non-foreign-intelligence evidence-of-crime justification in the text box. See Query Implementation Report, Mar. 5, 2020, at 4-5.

As currently configured, only if the user affirmatively clicks on “yes,” will the system prevent her from accessing Section 702-acquired content. At this point, she must choose between three “Authorization” options: 1) Court order, 2) Exigent Circumstances, or 3) Neither. See Nov. 3, 2020, letter. Selecting either option 1) or 2)

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

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

will allow the user to access the contents, and if the system permits such access, it will send an alert to an FBI attorney, who then follows up to determine whether the "yes" response was correct. At the hearing, the FBI reported that this alert feature was put into effect in late July 2020; since then, there have been 12 instances in which users had toggled to "Yes," indicating that they were conducting a U.S. person, evidence-of-crime-only query, and were nonetheless permitted access to view Section 702-contents. Based on its subsequent review, however, the FBI determined that none of the 12 queries was "exclusively" conducted to find evidence of crime, and the user had therefore incorrectly toggled to "yes." So far no one has selected the box indicating that she has obtained a court order to review the information.

If "Neither" is selected, the system blocks access to any responsive Section 702-acquired content, and an "Alert" message appears on the screen reminding the user that if "conducting an Evidence of Crime ONLY query against Section 702 FISA-acquired information using a USPER query term [she] must either obtain FISA Court Authorization or have exigent circumstances prior to reviewing content." Nov. 3, 2020 letter.

The government assesses that this system design will prevent a user from accessing the contents of Section 702-acquired information under circumstances that would require a report to the Court pursuant to the modified reporting requirement maintained in the December 6, 2019, Opinion. See Query Implementation Report, March 5, 2020, at 5 n.3. But the Court is wary of the default-choice architecture in the 

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

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

system because of how it may influence behavior or lead to misunderstandings by FBI personnel querying Section 702-acquired information. See supra at 40-41. In particular, it is concerned that FBI personnel, when conducting queries not designed to find and extract foreign-intelligence information, may: 1) mistakenly accept the default "No"; 2) enter a justification from the drop-down menu, or select "other" as the justification and indicate in the text box that the query was for a non-national-security-related criminal investigation; and 3) proceed to review the results returned in response. This would violate the statute in cases where the query was conducted in connection with a predicated criminal investigation, and it could hamper the government's ability to gather the information needed to comply with the modified reporting requirement regarding other evidence-of-crime-only queries.

The government asserts that the mandatory FISA training provides adequate assurance that personnel "should be aware" of the requirement to obtain an order from the Court for queries subject to Section 1881a(f)(2), as well as the "need to answer the [ONLY evidence of a crime] question correctly." See Query Implementation Report, Mar. 5, 2020, at 5 n.4. In the same report, however, the government also acknowledged that the system changes and the currently available Virtual Academy training do not address the modified reporting requirement. See id. at 11. The government confirmed at the hearing on October 28, 2020, moreover, that it has not yet reviewed or revised its training to address the modified reporting requirement; instead it restated that the training

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

Page 48

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

rolled out in November 2019, addressed the requirements to identify U.S.-person queries and record query justifications.

On November 13, 2020, the government informed the Court that the FBI was prepared to begin storing unminimized Section 702-acquired information in its [REDACTED] system. See Update Regarding the FBI's Implementation of Section 702 Querying Procedures for its [REDACTED], Nov. 13, 2020, at 4. The querying process described for [REDACTED] appears to be similar to the one described above [REDACTED] with one critical difference. When the user is asked whether the query was conducted to find only evidence of a crime, she must select either "Yes" or "No" because, unlike [REDACTED] the system will not default to "No." Id. This should provide useful data and may enable the government to assess whether the default rule in [REDACTED] results in a different error rate from that in [REDACTED].

As noted above, the Court lacks sufficient information at this time to assess whether the government's training efforts and changes to its system are having the desired effect. It is also not this Court's place to tell the government how to design its computer systems. For these reasons, the Court is prepared to again approve the FBI's Querying Procedures, but will add to the existing reporting obligations regarding evidence-of-a-crime (only) queries. The Court has previously found that querying, when conducted to find evidence of crime at earlier stages of a criminal investigation that is unrelated to national security, likely implicates Fourth Amendment concerns. See Dec. 6, 2019, Opinion at 73. It intends to continue to closely monitor the government's reporting in

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

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

order to evaluate whether the querying procedures are being implemented in a manner consistent with the statute and the Fourth Amendment. See §§ 1881a(j), (f)(1).

B. Bulk Queries Revisited

The government has reported another recordkeeping issue regarding the “bulk search” feature in [REDACTED] which permits users to conduct “batch” queries using multiple query terms. See Notice of compliance incident involving the FBI’s [REDACTED] [REDACTED] Oct. 9, 2020. [REDACTED] failed to record whether the query terms were U.S.-person query terms and allowed users to view the content of Section 702-acquired information without entering a justification in the system. Id. Apparently, the bulk-search feature operated in this manner since changes [REDACTED] were deployed in late November 2019. Id. The FBI made changes [REDACTED] to correct this issue on October 7, 2020, and determined that approximately 92 users had conducted approximately 353 bulk queries using 310 unique query terms. Id.; Nov. 3, 2020, letter at 3.

The failure to require a written justification for a bulk query involving a U.S.-person query term is particularly concerning given the indiscriminate nature of such queries. Indeed, the Court emphasized the importance of this documentation requirement in approving the FBI’s querying procedures. See Dec. 6, 2019, Opinion at 68. For example, in considering other bulk queries that the FBI had previously conducted for persons [REDACTED] the Court assessed that the requirement to provide a written justification before examining the contents returned by a U.S.-person query should “help ensure that FBI personnel . . . have thought about the querying standard and

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

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

articulated why they believe it has been met” and prompt them “to recall and apply the guidance and training they have received on the querying standard.” *Id.* (quoting Oct. 18, 2018, Opinion at 93).

The fact that this system failure went undetected or unreported for nearly a year highlights the ramifications of technical shortcomings in implementation of the procedures – e.g., failing to detect improper queries before they occur, and logging required information to enable proper oversight. The automated safeguards built into a system are helpful, but not foolproof, and training alone has proven to be an insufficient backstop. For these reasons and given the broad, suspicionless nature of past bulk queries, the Court is requiring the government to report on a quarterly basis the number of bulk queries run against Section 702-acquired information using U.S.-person query terms, the number of written justifications provided for such queries that were reviewed by OI, and the number NSD assessed did not have a reasonable basis to believe that queries of each individual identifier would be likely to retrieve foreign-intelligence information or evidence of a crime at the time the queries were conducted.

C. [REDACTED]

The government previously advised that, in order to comply with the recordkeeping and documentation requirements for U.S.-person queries conducted in a system called [REDACTED] the FBI implemented a process that required users to document in a SharePoint site whether the query satisfies the querying standard before viewing any contents returned by the query. *See* Dec. 6, 2019, Opinion at 65. At that time, the

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

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

government was still considering possible system changes in [REDACTED] Id. In its March 2020 report, the government advised that, given the time and anticipated cost of modifying [REDACTED] coupled with the relatively low number of users, it had decided to maintain the SharePoint site as a long-term solution for documenting query requirements. See Query Implementation Report, Mar. 5, 2020, at 7-8.

In September, the government advised that the FBI had discovered that the SharePoint site contained entries that were not in [REDACTED] which they attributed to an auto-preview feature in [REDACTED] that allowed a user to see the results of a U.S.-person query without a record being made of that query in [REDACTED] See Notice of a compliance incident involving the FBI's [REDACTED] system, Sept. 24, 2020. The FBI disabled this feature on August 3, 2020. [REDACTED] will now only present query results to users once the full query term(s) has been entered and will log every query. This should provide a better means for comparing [REDACTED] against the records in Sharepoint to assist in evaluating compliance with query-documentation requirements through the use of the FBI Sharepoint site. This change in implementation provides reason to expect improvement in the government's compliance with the querying procedures.

C. FBI Retention/Searching of FISA Data on Archival Email System and Instant Messaging System

The FBI has maintained in [REDACTED] archive system [REDACTED] all email messages sent to or from FBI's [REDACTED] email system since 2011, some of which contain raw FISA-acquired information. The FBI also stores copies of messages from its classified instant-messaging systems in a separate archival system. See Dec. 6, 2019,

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

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

Opinion at 42. These archival systems are used for records management, processing discovery and requests under FOIA, as well as by the FBI's [REDACTED] [REDACTED] for investigative purposes. Id.

In a notice filed July 2, 2020, the FBI advised that it had created a system called [REDACTED] designed to replace and receive data from legacy systems in order to assist the FBI's Information Management Division (IMD) in its obligations pursuant to FOIA and the Privacy Act, and to assist FBI personnel in managing discovery obligations in litigation matters. See Letter Regarding FBI's [REDACTED] System [REDACTED] [REDACTED] July 2, 2020 [REDACTED] will store data that has been exported from the FBI's [REDACTED]

[REDACTED] The government treats the data [REDACTED] as potentially containing raw FISA-acquired information subject to the FBI's Section 702 Standard Minimization Procedures applicable to archival systems. Id. at 5.

The provisions governing retention in archival systems provide that if FBI personnel identify unminimized Section 702 information in one of these archival systems, they must remove it from the system unless (1) it meets generally applicable retention criteria and is not otherwise subject to purge; or (2) "it is necessary to retain [it] for the purposes served by" the archival system in question, in which case the retention, and the reason therefor, must be included in the next quarterly report to the Court on Section 702

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

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

compliance matters, and the FBI must delete the information when it is no longer needed for such purpose. See 2019 FBI Minimization Procedures §§ III.F.5, III.F.6. No changes to these provisions are proposed in the 2020 certifications.

The Court approved this reporting requirement on a prospective basis, in view of the prohibition against putting unminimized Section 702 collection in classified email or IM systems as approved in the October 18, 2018, Opinion, but did not excuse the government from its obligation to report instances of retention required by that Opinion. It did so noting that the government had “unjustifiably disregarded” the October 2018 reporting requirement, in part, by taking so long to issue guidance to its personnel on the requirement. See Dec. 6, 2019, Opinion at 44. When the FBI policy was issued on December 14, 2019, to instruct personnel with access to the archival systems on the requirements of section III.F.5, III.F.6, and III.F.7 of the FBI Section 702 Minimization Procedures, it did not address the reporting requirement in the October 18, 2018 Order. See [REDACTED] letter at 4.

Perhaps owing to that gap in training, the government has not, to date, reported any instance of retention, as identified by FBI personnel between October 18, 2018, and December 6, 2019, of unminimized Section 702-acquired information, regardless of whether that information met the generally applicable retention criteria. Nor has the Court been notified of any reported instances in the Section 702 quarterly reports of retention of Section 702-acquired information in an archival system in accordance with the new provisions in Section III.F.5 and III.F.6.

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

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

Searches of these archival systems have also been excluded from the definition of “query” and, therefore, from the requirements of the FBI Querying Procedures.

Specifically, the definition of “query” in the FBI Querying Procedures exempts “searches conducted in the [archival] systems defined in Sections III.F.5 and 6 of the FBI’s section 702 minimization procedures in furtherance of an authorized use specified in those provisions.” 2019 FBI Querying Procedures § III.A. The minimization provisions authorize searching such systems “to assist in security, insider threat, inspection, and FBI-internal counterintelligence inquiries, functions, and investigations, and to respond to inquiries related to records management and discovery.” 2019 FBI Minimization Procedures §§ III.F.5, III.F.6 (emphasis added). See Dec. 6, 2019, Opinion at 45-46.

With regard to the FBI’s [REDACTED] system, the government advised that the [REDACTED] users will consist of IMD personnel who are trained to work on FOIA and Privacy Act matters. See [REDACTED] letter at 6. Only a limited number of [REDACTED] users (approximately 10) have the ability to search for data [REDACTED] all user activity will be logged, and [REDACTED] personnel will not have access [REDACTED]

[REDACTED] Id. at 6-7. [REDACTED] also has a purge process that can be initiated during a FISA compliance incident, resulting in the deletion or redaction of records, including archived source-provided files and loaded records. Id. at 7.

As described, the FBI’s [REDACTED] system appears to adhere to the current safeguards for archival systems required by Section III.F.5 and III.F.6 (including the

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

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

prohibition on placing raw FISA in these systems, access restrictions, limited number of authorized users, and purge processes). Given that searches in furtherance of records management and discovery will generally not be formulated to retrieve unminimized information about U.S. persons acquired under Section 702, the creation of this new archival system does present any new cause for concern. The government is again admonished, however, to report any instance of retention, as identified by FBI personnel, of unminimized Section 702-acquired information subject to the reporting requirement in the October 18, 2018, Opinion.

D. Retention/Searches of UAM Systems

Similar retention and reporting requirements apply for Section 702-acquired information in User-Activity Monitoring (UAM) systems under Section III.F.7 of the 2019 FBI Minimization Procedures. The December 6, 2019, Opinion directed the government to update its descriptions of these UAM systems and processes employed by the FBI, CIA, and NSA by no later than March 26, 2021 – i.e., two years from the government's prior UAM submissions. The update shall describe the UAM activities being undertaken by each agency and provide an assessment as to whether those activities are being conducted in a manner consistent with applicable Section 702 procedures. See Dec. 6, 2019, Opinion at 82-83. This reporting requirement shall remain in effect.

E. Failure to Purge Recalled Reports

In March 2019, the government reported that NCTC systems did not purge NSA reports that were subsequently recalled by NSA. See Preliminary Notice of Compliance

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

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

Incident Regarding Incomplete Purges of Data Acquired Pursuant to FISA, Mar. 13, 2019. As a result, NCTC analysts continued to have access to reports that potentially contained FISA information and had been recalled due to compliance incidents. Id. at 2.

Subsequent investigation revealed that the CIA and NSA also had systems that did not purge reports when they were recalled, including for FISA-compliance reasons. See Docket Nos. [REDACTED] Report in Response to Order Dated Oct. 3, 2019, Nov. 4, 2019, at 4-7, The December 6, 2019, Opinion directed the government to report by February 28, 2020, on: 1) the steps taken or to be taken by the FBI, NSA, CIA, and NCTC to identify to recipient agencies when reports are recalled for FISA-compliance reasons; 2) other steps the government has taken or will take to improve processes for identifying and removing reports that are recalled for FISA-compliance reasons; and 3) an anticipated timetable for completing any steps that remain to be taken. See Dec. 6, 2019, Opinion at 82.

The government's timely filing stated that ODNI had revised its DNI Intelligence Community policy memorandum to add a new category under which intelligence products could be recalled: "FISA-compliance recall." Docket Nos. [REDACTED] [REDACTED] Report in Response to Mem. Op. and Order Dated Dec. 6, 2019, Feb. 28, 2020, at 5. This new category will be used to notify recipients that a product has been recalled specifically for a FISA-compliance reason. Id. The revised IC policy memo requires a FISA-compliance recall notice to "explicitly state the product is being recalled for a FISA-compliance reason and must be removed with steps taken to prevent

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

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

its further use or disclosure.” Id. The revised DNI IC policy memo also requires each revision or recall notice to specify a point of contact who can provide additional details on why the notice was issued. Id. The revised DNI policy was signed and issued on February 27, 2020, but the government was not able to provide an estimated timeline for implementation of the revised policy. Id. at 5-6.

According to the September 2020 Quarterly Report, the revised policy directs all IC elements to revise their internal regulations to implement the new procedures. See Quarterly Report Concerning Compliance Matters Under Section 702, Sept. 18, 2020, at 63 (“Sept. 2020 Quarterly Report”). FBI, NSA, CIA, and NCTC will review their internal regulations and procedures and take the necessary actions to comply with the revised policy to include system modifications to create the new FISA-compliance recall category in the reporting process. Id. As of that report, the government was still in the process of creating a timeline for implementation based upon agencies’ review of the revised policy and their relevant internal regulations and procedures. Id.

While the Court is pleased with the revisions that have been made to the DNI IC policy memo, those revisions must be implemented in order to be effective. The Court accordingly, is ordering the government to provide regular reports on the status of implementation.

F. Other Incidents of Non-Compliance

The government has reported a number of other incidents of noncompliance since the December 6, 2019, Opinion. For example, NSA has sometimes erred in tasking

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

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

facilities for acquisition because of insufficient or incomplete foreignness checks, incorrect processing of requests for administrative updates on a facility that resulted in NSA retasking the facility without fully applying its targeting procedures; or because the connection between the targeted user and an authorized foreign power or foreign territory was sufficiently attenuated. See, e.g., June 2020 Quarterly Report at 8-17; Sept. 2020 Quarterly Report at 8-14. In other incidents, NSA failed to timely detask facilities when required to do so under applicable targeting procedures because of human error, including reasons such as misunderstanding the procedures and communication failures among agencies. Some of these delays have been exacerbated from reduced staffing as a result of the ongoing coronavirus pandemic. See, e.g., June 2020 Quarterly Report at 17-26; Sept. 2020 Quarterly Report at 16-21. There have also been incidents in which the FBI approved requests [REDACTED] prior to completing all required [REDACTED] procedures. See, e.g., June 2020 Quarterly Report at 46; Preliminary Notice of Compliance Incidents Regarding Section 702-Tasked Accounts, July 6, 2020 (FBI-approved [REDACTED] inappropriate for tasking).

In one reported instance, the FBI failed to timely establish a review-team process to protect attorney-client communications after a Section 702 target had been charged with a federal crime. See Preliminary notice of compliance incident regarding [REDACTED] 702-tasked facilities, Feb. 12, 2020. [REDACTED]

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

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

FBI advised that no information was acquired from the tasked facility between the charge date and the time the review team was set up; nor was any attorney-client privileged communication identified from the other tasked facilities that had been sequestered to the review-team space. Id.

After considering the matters discussed above and other incidents reported by the government and assessing the overall state of implementation of the current targeting, querying, and minimization procedures, the Court finds that the proposed procedures, as reasonably expected to be implemented, comply with applicable statutory and Fourth Amendment requirements. It will, however, continue to monitor the government's implementation of the procedures, especially regarding U.S.-person queries.

VII. CONCLUSION

For the foregoing reasons, the Court finds that:

(1) The 2020 Certifications, as well as the certifications in the Prior 702 Dockets, as thereby amended, contain all the required statutory elements;

(2) The targeting procedures for acquisitions conducted pursuant to the 2020 Certifications are consistent with the requirements of Section 702(d) and of the Fourth Amendment;

(3) With respect to information acquired under the 2020 Certifications, the minimization procedures and querying procedures are consistent with the requirements of Section 702(e) and Section 702(f)(1), respectively, and of the Fourth Amendment;

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

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

(4) With respect to information acquired under the certifications in the Prior 702 Dockets, as amended, the minimization procedures (including, as referenced therein, the requirements of the respective agencies' querying procedures) are consistent with the requirements of Section 702(e) and of the Fourth Amendment; and

(5) The querying procedures approved for use

are consistent with the requirements of Section

702(f)(1) and of the Fourth Amendment. (The Court does not make an equivalent finding regarding the other certifications in the Prior 702 Dockets because Section 702(f) only applies "with respect to certifications submitted under [Section 702(h)] . . . after January 1, 2018." Reauthorization Act § 101(a)(2).); and, accordingly,

IT IS HEREBY ORDERED AS FOLLOWS:

(1) The government's October 19, 2020, Submission is approved, as set out below:

- a. The 2020 Certifications and the certifications in the Prior 702 Dockets, as amended, are approved;
- b. The use of the targeting procedures for acquisitions conducted pursuant to the 2020 Certifications is approved;
- c. With respect to information acquired under the 2020 Certifications, the use of the minimization procedures and querying procedures is approved; and

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

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

d. With respect to information acquired under the certifications in the Prior 702 Dockets, the use of the minimization procedures (including, as referenced therein, the requirements of the respective agencies' querying procedures) is approved;

(2) Separate orders memorializing the dispositions described above are being issued contemporaneously herewith pursuant to Section 702(j)(3)(A);

(3) The following provisions of the December 6, 2019, Opinion (as supplemented by the Supplemental Order Regarding Reporting Requirements entered on December 10, 2019) shall remain in effect for the reasons stated therein. Prospectively, the government need not comply with reporting requirements imposed by the December 6, 2019, Opinion, or other FISC opinions and orders in the Prior 702 Dockets, except as reiterated below:

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

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

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

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

c. The government shall promptly submit a written report describing each instance in which an agency invokes the provision of its minimization or querying procedures providing an exemption for responding to congressional mandates, as discussed in Part IV.D.3 of the October 18, 2018, Opinion. Each such report shall describe the circumstances of the deviation from the procedures and identify the specific mandate on which the deviation was based;

d. The government shall submit in the Quarterly report on Section 702 compliance matters a report of each instance in which FBI personnel accessed unminimized Section 702-acquired contents information that was returned by a query that used a U.S.-person query term and was not designed to find and extract foreign-intelligence information. The report should include a detailed description of the information at issue and the manner in which it has been or will be used for analytical, investigative, or evidentiary purposes. It shall also identify the query terms used to elicit the information and provide the FBI's basis for concluding that the query was consistent with applicable procedures. This report shall also include: 1) the number of U.S.-Person queries run by the FBI against Section 702-acquired information, and 2) the number of such queries in which the documented justifications indicated an evidence-of-crime-only purpose. The government need not file such a report for a query for which it files an application with the FISC pursuant to Section 702(f)(2);

e. The government shall continue to submit reports to the Court on a quarterly basis on its use  under Section 702. This report

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

Page 63

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

shall: (i) describe [REDACTED]

(ii) explain how the government is

ensuring that it will only acquire communications to or from a Section 702 target [REDACTED]

and (iii) describe methods the government is using to

monitor compliance with the abouts limitation [REDACTED] and

report on the results of such monitoring;

f. No later than ten days after tasking for upstream collection under

Section 702 [REDACTED]

the government shall submit a notice to the Court. This notice shall: (i) describe [REDACTED]

(ii) explain how [REDACTED] will comply with the

abouts limitation; and (iii) describe steps that will be taken during the course of the

proposed acquisition to ensure that [REDACTED] is only acquiring

communications to or from authorized Section 702 targets;

g. The reporting requirement regarding retention of unminimized Section 702 information in FBI archival systems that appears at page 138 of the October 18, 2018, Opinion shall remain in effect for instances of retention that the government is currently obligated to report pursuant to that requirement;

h. On or before December 31 of each calendar year, the government shall submit in writing a report to the Court containing the following information: (a) the

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

Page 64

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

number of Section 702-acquired products disseminated or disclosed to the National Center for Missing and Exploited Children (NCMEC); and (b) the number of disseminations or disclosures by the NCMEC to other law-enforcement entities of Section 702-acquired information. At the government's election, this reporting may be combined with the NCMEC-related reporting required in the August 11, 2014, Opinion;

i. Prior to implementing changes to policies or practices concerning (a) the release of Section 702-acquired information from the NCMEC to Interpol's International Child Sexual Exploitation database or (b) approval to use Section 702-acquired information disseminated to the NCMEC in any proceeding, the government shall make a written submission to the Court describing such changes and explaining why implementing them would be consistent with applicable minimization procedures and statutory minimization requirements. At the government's election, this reporting may be combined with the NCMEC-related reporting required in the August 11, 2014 Opinion;

j. The government shall submit an update by February 28, 2021, specifying, as applicable: (1) steps taken or to be taken by the FBI, NSA, CIA, and NCTC to identify to recipient agencies when reports are recalled for FISA-compliance reasons; (2) other steps the government has taken or will take to improve processes for identifying and removing reports that are recalled for FISA-compliance reasons; and (3) an anticipated timetable for completing any steps that remain to be taken; and

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

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

k. The requirement to report, on or before March 26, 2021, an update to each agency's user activity monitoring (UAM) submission filed on March 29, 2019, that appears on pages 82-83 of the December 6, 2019 Opinion shall remain in effect.

(4) For the reasons stated herein, the government shall comply with the following requirements:

a. No later than ten days after the NCTC Director delegates authority to any group chief or official within the Directorate of Identity Intelligence, other than the one specifically discussed in the October 19, 2020, Memorandum at 8, to make the determination required under NCTC Minimization Procedures § D.3.b., the government shall submit a notice to the Court. This notice shall: (i) identify the individual to whom the delegation was made; (ii) describe the duties of such individual; and (iii) explain the reason(s) for the delegation to such individual and the scope and duration of the delegation;

b. On a quarterly basis, beginning January 15, 2021, and every 90 days thereafter, the government shall submit a notice to the Court that shall report: 1) the number of bulk queries run in [REDACTED] against Section 702-acquired information using U.S. person query terms; 2) the number of written justifications provided for such queries that were reviewed by OI; and 3) the number NSD assessed did not have a reasonable basis to believe that queries of each individual identifier would be likely to retrieve foreign-intelligence or evidence of a crime at the time the queries were conducted.

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

Page 66

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

ENTERED at 12:05 p.m. Eastern Time this 18th day of November, 2020.


_____
JAMES E. BOASBERG
Judge, United States Foreign
Intelligence Surveillance Court

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

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

Page 67