~~TOP SECRET/COMINT/NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted] Docket Nos. [redacted]

OPINION AND ORDER REQUIRING DESTRUCTION OF INFORMATION OBTAINED BY UNAUTHORIZED ELECTRONIC SURVEILLANCE

For the reasons explained below, the Court is ordering the government to destroy information obtained by unauthorized electronic surveillance that it conducted under color of orders issued in the above-referenced dockets pursuant to the electronic surveillance provisions of the Foreign Intelligence Surveillance Act (FISA), codified as amended at 50 U.S.C. §§ 1801-1812.

I. Background[1]

The authorized surveillance target in this case was the [redacted]. The unauthorized electronic surveillance involved [redacted] Compliance notice filed on Aug. 26, 2010, at 1. The duration of unauthorized surveillance [redacted] ranged from approximately 15 months to three years and collectively involved over [redacted] improperly intercepted communications. Id. at 2-8.

Under its standard minimization procedures, NSA was obligated to "monitor the acquisition of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications outside the authorized scope of the surveillance or information concerning United States persons not related to the purpose of the surveillance." Standard Minimization Procedures for Electronic Surveillance Conducted by the NSA ("SMPs") § 3(b). The Court has found, and the government has not disputed, that NSA's failure "to comply with

[1] See Opinion and Order Regarding Fruits of Unauthorized Electronic Surveillance issued on Dec. 10, 2010, at 1-3 ("December 10, 2010 Opinion") for a discussion of the procedural history of this matter prior to that date. The December 10, 2010 Opinion is incorporated herein by reference.

this requirement resulted directly in the unauthorized intercept of [redacted] December 10, 2010 Opinion at 5. Also contributing to the duration and volume of unauthorized surveillance in this case was the government's submission of [redacted] applications that falsely stated that [redacted]

The government proposed to retain the fruits of this unlawful surveillance, insofar as they reside in an NSA database called [redacted] See Letter filed on Dec. 3, 2010 ("December 3, 2010 Letter"). In support of this proposal, the government argued that the SMPs did not apply to the fruits of unlawful surveillance, but only to interceptions authorized pursuant to the Court's orders. December 3, 2010 Letter at 2 n.3. Secondly, it argued that the criminal prohibition codified at 50 U.S.C. § 1809(a)(2) only prohibits use or disclosure of unlawfully obtained information for investigative or analytic purposes. Id. at 4-6.

The Court addressed both of these contentions in its December 10, 2010 Opinion. After examining the SMPs and the statutory provisions relating to minimization, the Court rejected the government's contention that the SMPs do not apply to over-collected information.[3] December 10, 2010 Opinion at 3-6. The Court also noted that the SMPs appeared to require the destruction of at least some of the over-collected information. Id. at 5.

With regard to Section 1809(a)(2), the Court found unpersuasive the government's argument that the unqualified language of this prohibition only encompasses use or disclosure for investigative or analytic purposes. December 10, 2010 Opinion at 6-7. However, the Court recognized a narrower implicit exception from this prohibition for use or disclosure of "the results of unauthorized surveillance [that is] needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future." Id. at 8.

Based on the information available at the time of the December 10, 2010 Opinion, the Court could not ascertain whether or to what extent the over-collected information in this case might fall within this implicit exception to Section 1809(a)(2). Id. The Court ordered the

---

[2] See e.g., Docket No. [redacted], Declaration of [redacted], NSA, at 3-4 [redacted]

[3] The Court uses the term "over-collected" to refer to information obtained by unauthorized electronic surveillance.

government to make a submission by January 31, 2011, providing additional information and analysis. Id. at 8-9. With the benefit of extensions, the government completed this submission on April 8, 2011, after filing an interim update on February 14, 2011. At the request of the government, a hearing was conducted in this matter on May 10, 2011.

II. The Current Status of the Over-Collected Information

Since the December 10, 2010 Opinion, NSA has completed its efforts to locate and purge the information obtained from this unauthorized electronic surveillance from data repositories other than [redacted] Verified Factual Update filed on Feb. 14, 2011 ("Verified Factual Update"), at 4-5. Information from [redacted] records was used in this process. Id. at 5. More specifically, NSA reports that it [redacted] Id. at 4-5. NSA assesses that it is "highly unlikely" that information obtained from this unauthorized surveillance exists in any repository other than [redacted] Id. at 3 n.2.

Within [redacted] information from this unauthorized surveillance is retained in [redacted]. Government's Response submitted on April 8, 2011 ("Government's Response") at 6. [redacted]

[redacted]

[redacted]

4 [redacted]

[redacted]

Each [redacted] record corresponding to the over-collected information in this case has been marked as "subject to purge." Verified Factual Update at 5. The government proposes to retain, use, and disclose the over-collected information in [redacted] subject to certain restrictions that are discussed infra at page 6.

III. Analysis – Section 1809(a)(2)

Section 1809(a) states without qualification: "A person is guilty of an offense if he intentionally . . . (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by statute. The December 10, 2010 Opinion recognized a narrow implicit exception to this prohibition for "actions that are necessary to mitigate or prevent the very harms at which Section 1809(a)(2) is addressed." December 10, 2010 Opinion at 8 (emphasis in original). The Court observed that this exception "must be carefully circumscribed, so that it does not lead to an unjustified departure from the terms of the statute." Id. The Court indicated that this exception would encompass "use" or "disclosure" in the course of "actions in direct response to unauthorized surveillances" that are "necessary to avoid similar instances of over-collection (e.g., by identifying and remedying a technical malfunction) or to remedy a prior over-collection (e.g., by aiding the identification of over-collected information in various storage systems)." Id. at 7. The Court was doubtful that future use or disclosure of the over-collected information in this case could fall within this narrow exception, "now that the over-collection has been conclusively attributed" to "failure to recognize and respond properly to [redacted] and that "apparently all of the [over-collected] information . . . has been purged or marked for purging." Id. at 8.

A. Scope of the Implicit Exception

Because the outcome of this case depends on the scope of this exception, a full explanation of why Section 1809(a)(2) admits only a narrowly focused exception is appropriate. "Federal crimes are defined by Congress, and so long as Congress acts within its constitutional power in enacting a criminal statute," a court "must give effect to Congress' expressed intention concerning the scope of conduct prohibited." United States v. Kozminski, 487 U.S. 931, 939

(1988); accord, e.g., United States v. Lanier, 520 U.S. 259, 267 n.6 (1997) ("Federal crimes are defined by Congress, not the courts," and in construing criminal statutes courts are "oblige[d] . . . to carry out congressional intent as far as the Constitution will admit."). This generally means that, "in applying criminal laws," courts "must follow the plain and unambiguous meaning of the statutory language," United States v. Albertini, 472 U.S. 675, 680 (1985), and bear in mind that it is for Congress to resolve "the pros and cons of whether a statute should sweep broadly or narrowly." United States v. Rodgers, 466 U.S. 475, 484 (1984).

More specifically, courts should not attempt "to restrict the unqualified language of a [criminal] statute to the particular evil that Congress was trying to remedy – even assuming that it is possible to identify that evil from something other than the text of the statute itself." Brogan v. United States, 522 U.S. 398, 403 (1998). Thus, even if it were established that Congress enacted Section 1809(a)(2) in order to curb investigative abuses, that provision would still properly apply to non-investigative uses or disclosures. See Albertini, 472 U.S. at 682 (criminal prohibition applies even though enacting Congress "very likely gave little thought" to circumstances in question). The exception recognized in the December 10, 2010 Opinion stands on narrower but firmer ground: that in limited circumstances, prohibiting use or disclosure of the results of unauthorized electronic surveillance would be "so 'absurd or glaringly unjust' . . . as to [call into] question whether Congress actually intended what the plain language" of Section 1809(a)(2) "so clearly imports." Rodgers, 466 U.S. at 484 (quoting Sorrells v. United States, 287 U.S. 435, 450 (1932)); accord Chapman v. United States, 500 U.S. 453, 463-64 (1991); see also United States v. Rutherford, 442 U.S. 544, 552 (1979) ("Exceptions to clearly delineated statutes will be implied only where essential to prevent absurd results or consequences obviously at variance with the policy of the enactment as a whole.") (internal quotations omitted).

B. Application of the Implicit Exception

In accordance with the narrowness of the exception it had articulated, the Court ordered the government to "specifically explain why [the] particular information" at issue in this case "is now needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future." December 10, 2010 Opinion at 8-9 (emphasis added). The government has not done so. At the May 10, 2011 hearing, the government conceded that there were no plausible circumstances in which further use or disclosure of the information obtained by the unauthorized surveillance in this case and now residing in [redacted] would prove necessary to these ends. See also Government's Response at 9 ("The [redacted] compliance incident resulted from a set of discrete and specific facts . . . . [I]t did not result from technological problems and appears to be the result of human error.").

Instead, the government argues that certain restrictions on access to the over-collected information in [redacted] will ensure that future use and disclosure will comport with Section 1809(a)(2). The Court disagrees for reasons explained below.[5]

The government reports that all records in [redacted] that are marked as subject to purge, including the records containing the over-collected information in this case, are only accessible to a limited number of authorized personnel, termed [redacted] Verified Factual Update at 5-6. And, pursuant to a policy adopted after the December 10, 2010 Opinion, "information from unauthorized electronic surveillance in [redacted] and marked as subject to purge will be used only when reasonably necessary (1) to remedy or prevent the 1809(a) harms[6] arising from a particular incident of unauthorized electronic surveillance or (2) to evaluate and, when necessary, adjust NSA's processes and procedures designed to remedy or prevent the 1809(a) harms." Government's Response at 13. As explained above, it is untenable that further use or disclosure of the over-collected information in this case is necessary for the first enumerated purpose.

In the government's view, actions taken as "reasonably necessary" to the second enumerated purpose would include steps to implement "an enterprise-wide compliance program," to include third-party audits and assessments, as well as monitoring and assessment of NSA's internal controls. Id. at 14-15. The Court is unpersuaded that uses and disclosures of the over-collected information in this case would comply with Section 1809(a)(2) simply because they are in furtherance of this second purpose. That is not because the Court doubts the importance of an enterprise-wide compliance program in remedying or preventing 1809(a) harms. Rather, it is because there is no reason to believe that further use or disclosure of the specific over-collected information in this case will be needed for such a program to be effective, now that the cause of the unauthorized surveillance has been identified as discrete human error and all of the over-collected information has been purged or marked as subject to purge. After all, in a happier world where NSA had not unlawfully intercepted [redacted] under color of the orders in this case, NSA presumably would still have the wherewithal to devise and implement an effective compliance program. There is no reason to think that

---

[5] The government also identifies adverse consequences that might follow from a general requirement to destroy over-collected information in [redacted] Because this argument goes to the retention or destruction of over-collected information, rather than its use or disclosure, the Court addresses it in the context of minimization. See infra pp. 8-9.

[6] The government has adopted the term "1809(a) harms" as shorthand for unauthorized electronic surveillance or use or disclosure of the results of such surveillance. See, e.g., Government's Response at 12-13, 17.

information about [redacted] is necessary for an effective, real-world compliance program, now that the particular incidents to which it pertains have been addressed.

The most that the government can claim is that, as an undifferentiated class, [redacted] records marked as subject to purge are needed for an effective compliance program. See Government's Response at 7-8, 10-11; Declaration of [redacted] Director of Compliance, NSA ("[redacted] Declaration") at 4 (submitted as Attachment B to the Government's Response). But it does not follow from this premise that use or disclosure of any information within that undifferentiated class would comport with Section 1809(a)(2), so long as it is made in furtherance of a compliance program designed to prevent or remedy 1809(a) harms at a programmatic level. Because the specific over-collected information at issue no longer has any distinctive utility for NSA's compliance efforts, it is neither absurd, nor glaringly unjust, nor obviously at variance with the policy of FISA as a whole, see supra p. 5, to conclude that Section 1809(a)(2) prohibits its further use or disclosure, even in the context of external auditing, monitoring of internal controls, or other aspects of an enterprise-wide compliance program.

IV. Analysis – SMPs

The Court's December 10, 2010 Opinion noted that Section 5(a) of the SMPs appears to require the destruction of at least some of the information over-collected in this case, December 10, 2010 Opinion at 5, and directed the government to "[a]ddress in detail . . . how the SMPs apply to the proposed retention and use of information obtained from this unauthorized surveillance." Id. at 8 (emphasis added). In response, the government has stated that the "SMPs do not explicitly address the Government's authority to retain, use, or disclose information from unauthorized electronic surveillance for the purpose of preventing or remedying . . . 1809(a) harms," and that the government "is assessing an appropriate amendment to the SMPs to account" for such situations. Government's Response at 17-18. The Court understands this response to its December 10, 2010 Opinion to concede that the SMPs, as now in effect, do not explicitly permit the retention of the over-collected information in this case.

Apart from this concession, it seems clear that the SMPs explicitly require NSA to destroy most, if not all, of the over-collected information in this case, and would do so even if the information had been lawfully acquired. The SMPs divide communications into two types: foreign communications and domestic communications. "Communications identified as domestic communications shall be promptly destroyed," subject to exceptions that appear inapplicable to this case. SMPs § 5(a). Similarly, foreign communications "of or concerning United States persons" may only be retained under specified circumstances that do not appear to be present in this case, and otherwise "shall be promptly destroyed." Id. §§ 3(e), 6(a). One category of communications is not subject to a general destruction requirement: foreign communications that are not of or concerning a U.S. person. Id. § 7. Given the definitions of the operative terms and

the nature of the unauthorized surveillance in this case, this category would consist of [redacted] communications in which (1) at least one communicant was outside the United States; (2) no communicants were U.S. persons; and (3) no non-public information concerning a U.S. person was divulged. See id. § 2(b), (c), (e). Because [redacted], one would expect that only a small percentage of the unlawful intercepts – if any – would satisfy all three conditions.

In any event, the government – notwithstanding the Court's requiring a detailed discussion of how the SMPs apply to this case – has not addressed the effect of specific provisions or the status of particular types of communications. Instead, it requests the Court to recognize an implicit exception to the destruction requirements of the SMPs, despite the fact that this information was unlawfully acquired. For the reasons stated supra at pages 5-7, the Court concludes that further use or disclosure of the over-collected information in this case would not be consistent with Section 1809(a)(2). No lawful benefit can plausibly result from retaining this information, but further violation of law could ensue. Accordingly, the Court declines to find that the over-collected information in this case is subject to an implicit exception from the destruction requirements of the SMPs.

The government also describes various ways in which it might be burdensome or counterproductive to require NSA to purge from [redacted] information obtained by unauthorized electronic surveillance. It takes effort to identify information in [redacted] See Verified Factual Update at 9-10. NSA anticipates difficulties in determining when records pertaining to a particular unauthorized electronic surveillance are no longer needed and asserts that premature destruction may impede NSA's compliance efforts in ways not foreseen when a decision to destroy is made. Government's Response at 9-12; [redacted] Declaration at 7-10. It is feared that NSA personnel may draw erroneous conclusions from the resulting gaps in data. [redacted] Declaration at 7.

To a considerable extent, these objections are directed at cases not before the Court. The records pertaining to the over-collected information in this case have already been identified and isolated, see Government's Response at 6; Verified Factual Update at 9, and there is no difficulty in concluding that this over-collected information is no longer needed to prevent or remedy 1809(a) harms, see supra pp. 5-7. This case is therefore distinguishable from those that may require a longer period of technical examination or exploitation to understand and remedy causes of unauthorized surveillance or to identify and segregate over-collected information.

In this case, the government's objections fall well short of establishing a need to exempt the over-collected information from the destruction requirements of the SMPs. It could be asserted that any requirement to destroy information "on a case-by-case basis . . . might have negative unintended consequences." [redacted] Declaration at 10 (emphasis added). Nevertheless,

the SMPs routinely require NSA personnel to apply retention criteria on a case-by-case basis to information that was lawfully acquired, and promptly destroy information that does not satisfy those criteria. See supra pp. 7-8. There is no reason to think that this approach is distinctively unworkable for unlawfully acquired information. Indeed, a case-by-case assessment is most appropriate for over-collected information because, except in narrow circumstances, intentionally using or disclosing such information is a crime.

V. Conclusion

Information about these private, non-target communications should have never been acquired. Now that its further use or disclosure cannot reasonably be expected to be lawful, it should be destroyed.

For the reasons stated herein, the government is ORDERED to destroy all information in [redacted] that was obtained by the unauthorized electronic surveillance in this case. Although the Court cannot comprehensively identify such information based on the record before it, such information includes, to the extent it exists for each unlawfully intercepted [redacted] communication: [redacted] The government may accomplish this destruction by deleting entire records in [redacted] or by deleting all of the fields within records that contain information obtained by the unauthorized electronic surveillance, so long as all information obtained from this unauthorized electronic surveillance and contained in [redacted] is in fact destroyed. The government shall submit a written report no later than June 17, 2011, and at monthly intervals thereafter, describing the process by which it is destroying such information, until such time as the destruction process has been completed.

Entered this 13th day of May, 2011, in Docket Nos. [redacted].

for FREDERICK J. SCULLIN, JR.
Judge, United States Foreign
Intelligence Surveillance Court