

~~TOP SECRET/COMINT/NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

Docket Nos. [REDACTED]

OPINION AND ORDER REGARDING FRUITS
OF UNAUTHORIZED ELECTRONIC SURVEILLANCE

For the reasons explained below, the Court is ordering the government to submit additional information regarding its proposed retention and use of the results of unauthorized electronic surveillance that it conducted under color of orders issued in the above-referenced dockets.

Background

On June 30, 2010, the government notified the Foreign Intelligence Surveillance Court (FISC) that, under color of orders issued in one or more of the above-referenced dockets, the National Security Agency (NSA) had continued electronic surveillance of [REDACTED]

[REDACTED] Compliance notice filed on June 30, 2010 ("June 30 Notice"). On July 12, 2010, the government disclosed to the FISC similar over-collection for [REDACTED]

[REDACTED] Compliance notice filed on July 12, 2010 ("July 12 Notice"). These notices provided little information regarding the unauthorized surveillance, but stated that after further investigation, the government would "provide a thorough explanation." June 30 Notice at 2; July 12 Notice at 1.

The government submitted an application for continued electronic surveillance of other facilities [REDACTED] on August 4, 2010, which the Court granted on the same date. See Docket No. [REDACTED]. The application did not contain any further information about the unauthorized surveillance. The Court, through its staff, orally directed the government to submit its fuller report by August 16, 2010.

On August 16, 2010, the government filed another notice, which provided more information about the scope of the unauthorized electronic surveillance of some [REDACTED]. [REDACTED] Compliance notice filed on August 16, 2010 ("August 16 Notice"). In a subsequent notice, filed on August 26, 2010 ("August 26 Notice"), the government described the unauthorized surveillance of all [REDACTED], for periods ranging from

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

approximately 15 months to three years, and resulting in over [REDACTED] improperly intercepted communications. August 26 Notice at 2-8.¹

The August 26 Notice also addressed the disposition of the results of the unauthorized surveillance.² [REDACTED]

The August 26 Notice also stated that, “[w]ith the exception of [REDACTED] NSA reports that it knows of no other repository in which the overcollected communications would currently be stored.” *Id.* at 2 n.1. [REDACTED]

FISC staff informally sought from the government additional information regarding the retention of information from this unauthorized surveillance in [REDACTED]. On November 17, 2010, the Court, through its staff, orally directed the government to submit, by December 3, 2010, additional information regarding such retention, including an explanation of why, in the

¹ FISC approval of continued surveillance of [REDACTED] resulted from government misstatements. See e.g., Docket No. [REDACTED] Declaration [REDACTED], NSA, at 3-4 [REDACTED]

² At all relevant times, the FISC Rules have required the government, in the event of an unauthorized surveillance, to report to the FISC, among other things, “how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.” Rule 10(c)(iv) of FISC Rules effective on Feb. 17, 2006; Rule 13(b)(4) of FISC Rules effective on Nov. 1, 2010.

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

government's opinion, continued retention and any anticipated use are consistent with both the applicable minimization procedures and 50 U.S.C. § 1809(a)(2).

The government made a responsive submission on December 3, 2010 ("December 3 Submission"). The December 3 Submission discusses the proposed retention and use of information from the unauthorized surveillance; the non-applicability, in the government's view, of the Court-approved minimization procedures to the retained information; and the government's reasons for believing that the proposed retention and use are not prohibited by 50 U.S.C. § 1809(a)(2). The Court will address these three discussion items seriatim.

Proposed Retention and Use

In contrast to the August 26 Submission, which referred to the information retained in [REDACTED] the December 3 Submission advised that "a portion of the information from the unauthorized collection may not constitute merely [REDACTED] in the Government's filings with the FISC." December 3 Submission at 1 n.1 (emphasis added). The government did not disclose what information is being retained, other than to assert that [REDACTED] . . . are not contained in [REDACTED] Id. (emphasis added).

The government states that "only a limited number of NSA individuals³ are authorized to access this information in order to perform compliance and technical support functions, . . . but they are not authorized to access this information to perform intelligence analysis." Id. at 2. Authorized compliance and technical support functions include [REDACTED]

Application of Minimization Procedures

The government asserts, without supporting analysis, that

NSA's standard minimization procedures (SMPs) are inapplicable to the communications from unauthorized collection. The SMPs only govern authorized

³ The government describes these personnel as [REDACTED]

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

electronic surveillance, whereas section 1809(a)(2) applies only to “information obtained through [unauthorized] electronic surveillance.” Accordingly, the information from unauthorized collection, like that described in the [August 26 Notice], is subject to 1809(a)(2), but not the SMPs.

December 3 Submission at 2 n.3 (emphasis added). For reasons explained below, the Court finds this assertion unpersuasive.

First, the government’s contention finds no support in the definition of “minimization procedures” at 50 U.S.C. § 1801(h), or the provisions regarding FISC review of those procedures at §§ 1804(a)(4), 1805(a)(3), and 1805(c)(2)(A), or government compliance with them at § 1806(a).⁴ Indeed, the definition of “minimization procedures” weighs against the government’s contention, by requiring procedures “that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination” of U.S. person information, “consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” § 1801(h)(1). Here, “[t]he sole purpose of this surveillance” was to acquire “foreign intelligence information concerning [REDACTED]

[REDACTED] Docket No. [REDACTED] Certification of William J. Lynn III, Deputy Secretary of Defense, at 1-2 (emphasis added). Communications that are unrelated to [REDACTED], such as those in question, are irrelevant to “the purpose . . . of the particular surveillance,” and are unlikely to further the government’s ability “to obtain, produce, and disseminate foreign intelligence information.” § 1801(h)(1). One would expect the procedures’ restrictions on retaining and disseminating U.S. person information to apply most fully to such communications, not, as the government would have it, to fail to apply at all.

An examination of the applicable minimization procedures supports this conclusion. There is no question that these procedures applied at the inception of the surveillance, when [REDACTED] By their

⁴ Section 1806(a) states: “Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter [i.e., 50 U.S.C. §§ 1801-1812].” In this case, the surveillance was described in an application made pursuant to Section 1804, and conducted under color of a FISC authorization issued pursuant to Section 1805, with the aid of persons compelled to assist pursuant to Section 1805(c)(2)(B). There is no difficulty in finding this electronic surveillance to have been “conducted pursuant to” 50 U.S.C. §§ 1801-1812 for purposes of Section 1806(a).

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

terms, these procedures “apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is collected in the course of electronic surveillance as ordered by the [FISC].” Standard Minimization Procedures for Electronic Surveillance Conducted by the NSA (“SMPs”) § 1. This language is broad enough to encompass electronic surveillance conducted under color of a FISC order that adopts the SMPs, even if, in some respects, the surveillance exceeds the limitations of the order.

Other provisions of the SMPs indicate that this is the only logical interpretation of the SMPs’ scope. Most pertinently to this case, the SMPs require that,

[a]t the initiation of the electronic surveillance, the NSA or the Federal Bureau of Investigation, if providing operational support, shall verify that the communication lines or telephone numbers being targeted are the lines or numbers of the target authorized by court order Thereafter, collection personnel will 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.

SMPs § 3(b). Failure to comply with this requirement resulted directly in the unauthorized intercept of [REDACTED]

[REDACTED] These communications presumably are unrelated to [REDACTED] or any other subject of foreign intelligence interest. Several provisions of the SMPs restrict the retention and use of such communications, even when they have been properly acquired. *See, e.g.*, SMPs § 5(a) (requiring domestic communications to “be promptly destroyed,” subject to exceptions that do not appear to apply in this case); § 3(c)(5) (a communication “may be processed” only if it is “to or from the targeted premises and is reasonably believed to contain foreign intelligence information or evidence of a crime”). To say the least, it would be anomalous if a violation of the SMPs, resulting in acquisition of [REDACTED] communications, somehow exempted the government from compliance with the SMPs’ restrictions on the retention and use of those communications. There is no persuasive reason to give the SMPs the paradoxical and self-defeating interpretation advanced by the government.⁵

⁵ The Court does not agree with the government’s apparent premise that such an interpretation is necessary to resolve a conflict between the requirements of the SMPs and Section 1809(a)(2). Both sets of rules apply by their terms, and in circumstances governed by both, the government must comply with them both. The Court discerns no basis for anticipating an irreconcilable conflict, *i.e.*, a case where a use or disclosure prohibited by Section 1809(a)(2) (continued...)

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~Application of Section 1809(a)(2)

Section 1809(a)(2) states: "A person is guilty of an offense if he intentionally . . . discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance [that was] not authorized." The provision does not define or limit the terms "discloses or uses." Nevertheless, the government puts forward several reasons in support of a narrow interpretation, under which "use" or "disclosure" is prohibited only when it involves "an analytic or investigative action," and not when it involves "a technical or compliance-related action." December 3 Submission at 4-6.

The government suggests that the Court look to language in other parts of the statute to limit the breadth of the uses or disclosures prohibited by Section 1809(a)(2). It points to certain provisions of Section 1806, which apply when the government intends "to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any [state or federal] court, department, officer, agency, regulatory body or other authority." § 1806(c), (d). Other provisions of Section 1806 regulate use or disclosure outside of proceedings, and do not contain such language. See § 1806(a) (certain surveillance information "may be used and disclosed . . . only in accordance with the minimization procedures"); § 1806(b) (concerning surveillance information "disclosed for law enforcement purposes"). Selectively focusing on those provisions of Section 1806 that contain the limiting language, the government argues that those provisions provide a "context" in which "discloses or uses" should be understood, for Section 1809(a)(2) purposes, to be limited to analytic or investigative actions. December 3 Submission at 4. Examined as a whole, however, the statute merely suggests that when Congress intended a provision to apply only to uses or disclosures made in narrow circumstances, or for specific purposes, it employed language in that provision to make the limitation explicit.

The government also relies on legislative history for its narrow interpretation of Section 1809(a)(2). First, it claims that the legislative history "indicates an intention on the part of Congress to not criminalize intelligence agency personnel access to information for the purpose of ensuring compliance with the law and applicable court orders and procedures." December 3 Submission at 4 (citing H.R. Rep. No. 95-1283, pt. 1, at 96-97 (1978)). But the cited passage does not have the weight of authority the government claims. That passage had to do with a proposed criminal provision in a predecessor bill that was substantially different from the

⁵(...continued)

would be required by the SMPs. In any event, a theoretical possibility of a conflict would provide insufficient grounds to render the SMPs wholly inapplicable, particularly in regard to a large volume of non-pertinent communications.

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

provision subsequently enacted and codified at Section 1809(a)(2). See H.R. Rep. No. 95-1283, pt. 1, at 11 (proposal to criminalize the intentional violation of certain statutory requirements or of “any court order issued pursuant to this title”). Moreover, the cited passage says nothing about the use or disclosure of the results of unauthorized surveillance for compliance purposes, or for any other purpose. The closest that the passage comes to discussing compliance purposes is in an inapposite reference to a proposal to criminalize the intentional destruction of “records required by the bill to be retained for oversight purposes.” Id. at 97.

From other legislative history, the government argues that the purpose of Section 1809(a)(2) is “to deny an intelligence agent the fruits of his unlawful actions in civil and criminal proceedings.” December 3 Submission at 4. Specifically, the government suggests that Section 1809(a)(2) “was designed to mirror the prohibitions in . . . 18 U.S.C. § 2511(1),”⁶ which in turn “were intended to deny a perpetrator of an unlawful intercept the fruits of his unlawful actions in civil and criminal proceedings.” December 3 Submission at 4 (internal quotations omitted). But even if one accepted the suggested equivalence of Section 1809(a)(2) with Section 2511(1), the limitation desired by the government would not follow. In accordance with the breadth of the operative terms, courts have found that uses and disclosures, outside the context of proceedings and for purposes other than investigation or intelligence analysis, can violate Section 2511(1).⁷

On the other hand, the government validly points out that it is reasonable, and consistent with Congressional purpose, to countenance certain actions in direct response to unauthorized surveillances that literally could involve forms of “use” or “disclosure” – for example, to the extent 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). December 3 Submission at 4-6.

⁶ Section 2511(1) subjects to criminal liability “any person who,” inter alia, “intentionally discloses . . . to any other person,” or “intentionally uses, . . . the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.” 18 U.S.C. § 2511(1)(c), (d).

⁷ See, e.g., Peavy v. WFAA-TV, Inc., 221 F.3d 158, 174-76 (5th Cir. 2000) (television station’s public broadcast of intercept information, and reporters’ pre-broadcast uses and disclosures of such information in news gathering, could constitute violations of § 1811(1)); see also Bartniki v. Vopper, 532 U.S. 514 (2001) (private party’s disclosure of contents of intercepted conversation between teachers union officials to school board members and media representatives violated language of § 1811(1), but application of statute in circumstances presented would contravene First Amendment).

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

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

On the information submitted, the Court is unable to ascertain whether the proposed use of the information in [REDACTED] falls within the limited circumstances in which the results of unauthorized surveillance are needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future. This is partly because the government has been so sparing in its description of the information being retained. It is also due in part to the circumstances in which this unauthorized surveillance occurred. In this instance, the over-collection did not result from technological problems, but simply from a failure to recognize and respond properly to [REDACTED]. It is not apparent to the Court why it is necessary to retain any of this over-collected information for compliance or oversight purposes, now that the over-collection has been conclusively attributed to this cause, and apparently all of the information from the unauthorized surveillance has been purged or marked for purging. See December 3 Submission at 1 (over-collected communications have been deleted from [REDACTED] id. at 3 n.5 (information in [REDACTED] obtained from the unauthorized surveillance “have been marked as being subject to purge”).

* * *

Accordingly, it is hereby ORDERED that the government shall make a written submission by January 31, 2011. The submission shall:

(1) Confirm whether all information obtained from this unauthorized surveillance has been destroyed, except insofar as such information is retained in [REDACTED]
[REDACTED]
[REDACTED]

(2) Address in detail, in a manner consistent with the foregoing interpretation of the statute and the SMPs, how the SMPs apply to the proposed retention and use of information obtained from this unauthorized surveillance.

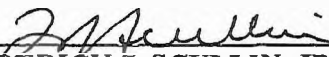
(3) Specifically describe the types of information obtained from this unauthorized surveillance and retained in [REDACTED] and specifically explain why this particular information

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

is now needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future.

Entered this 10 day of December, 2010, in Docket Nos. [REDACTED]
[REDACTED]


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

~~TOP SECRET/COMINT/NOFORN~~

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