

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

surveillance⁶⁶ against a United States person who is physically outside of the United States for foreign intelligence or counterintelligence purposes unless the surveillance is approved by the Attorney General. Although it does not specifically use the term "agent of a foreign power," Procedure 5, Part 2.C provides what is tantamount to such a definition. Specifically, it requires that a request for Attorney General approval contain a statement of facts supporting a finding of probable cause that the target of the electronic surveillance is one of the following:

- (1) A person who, for or on behalf of a foreign power is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, or activities in preparation for international terrorist activities; or who conspires with, or knowingly aids and abets a person engaging in such activities;
- (2) A person who is an officer or employee of a foreign power;
- (3) A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;
- (4) A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
- (5) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to

⁶⁶ "Electronic surveillance" is defined under the DoD Procedures (Appendix A) as the

[a]cquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication, or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter. (Electronic surveillance within the United States is subject to the definitions in the Foreign Intelligence Surveillance Act of 1978 (reference (b)).)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

information or material classified by the United States to which such person has access.^[67]

In the context of the certifications at issue, the question becomes whether a finding of probable cause by the Attorney General that comports with Procedure 5, Part 2.C, is sufficient to invoke the foreign intelligence exception to the Warrant Clause. The Court finds that the answer is yes for the following reasons.

First, the Attorney General is an appropriate official to make the probable cause finding. See United States v. Bin Laden, 126 F. Supp. 2d at 279 & n.18. Second, the descriptions in Procedure 5, Part 2.C, regarding what makes a United States person an acceptable target (i.e., an agent of a foreign power), themselves pass muster. Certainly in common sense terms, a United States person who falls into any of the five categories can reasonably be believed to be an "agent" of a foreign power.⁶⁸ Moreover, it also seems clear that categories 1, 3, and 5 suffer from no constitutional or other legal infirmities. See In re Sealed Case, 310 F.3d at 719 (U.S. citizen target was an agent of a foreign power because there was probable cause that he or she was

⁶⁷ Procedure 7.C, which is applicable to physical searches, contains materially identical language as to a showing of probable cause concerning the target.

⁶⁸ The Procedures independently define a "foreign power" as "[a]ny foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities." DoD Procedures, Appendix A. However, the particular foreign powers at issue here are further constrained by the certifications, which by their terms are directed at

cf. 50 U.S.C.A. § 1801(a)(1) & (a)(4) (defining "foreign power" under FISA as including foreign governments, as well as groups engaged in international terrorism or activities in preparation for international terrorism).

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

aiding, abetting, or conspiring with others in international terrorism); Bin Laden, 126 F. Supp. 2d at 278 (agent of al Qaeda). Similarly, to the extent the certifications contemplate targeting entities abroad as agents, the Court finds it unlikely that category four has any constitutional impediments either, at least not in the context of the foreign powers at issue (see supra note 68). Cf. 50 U.S.C.A. § 1801(a)(6) (even for purposes of a FISA order within the United States, the term "foreign power" includes an entity directed and controlled by a foreign government or governments). Finally, the second category admittedly does go beyond what FISA permits the government to do in the United States, cf. 50 U.S.C.A. § 1801(b)(1)(A) (limiting definition of "agent of foreign power" to a non-U.S. person acting in the U.S. as an officer or employee of a foreign power). Nonetheless, the Court concludes that it is constitutionally appropriate for the government to acquire for foreign intelligence purposes the communications of a United States person abroad who is acting as an officer or employee of a foreign government or terrorist group. Indeed, were it otherwise, then the United States government would be routinely prevented from obtaining necessary foreign intelligence [REDACTED]

[REDACTED] Such a result would be untenable.

Based on the above analysis, the Court holds that the foreign intelligence exception to the warrant requirement is applicable to the directives issued to Yahoo. The Court must therefore address whether the directives are reasonable under the Fourth Amendment.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

2. The Directives are Reasonable Under the Fourth Amendment

The Fourth Amendment analysis merely begins with the finding that the government need not obtain a warrant to acquire the communications it seeks to obtain from Yahoo through the issuance of directives. In order for those directives to comport with the Fourth Amendment, they must also be reasonable. United States v. Knights, 534 U.S. 112, 118-19 (2001) ("The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))). And, to assess the reasonableness of the directives issued to Yahoo pursuant to the PAA, this Court must examine the totality of the facts and circumstances. Samson v. California, 547 U.S. 843, 848 (2006); Ohio v. Robinette, 519 U.S. 33, 39 (1996).

The acquisitions at issue in this case present this Court with the challenge of balancing the government's interest in acquiring foreign intelligence information against the privacy interests of those United States persons whose communications will be acquired.⁶⁹ There is little doubt about the weightiness of the government's interest, as this Court accepts the government's assertion that the information it seeks to acquire from Yahoo would "advance the government's compelling interest in obtaining foreign intelligence information to protect national security. . . ."

⁶⁹The foreign intelligence that the government seeks to obtain from Yahoo is not limited to the communications of United States persons. Indeed, there is every reason to assume that most of the accounts that will be targeted will be ones used by non-United States persons overseas who do not enjoy the protections of the Fourth Amendment. See *supra* note 60.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

Mem. in Support of Gov't Motion at 14; see also Gov't's Supp. Brief on the Fourth Amend. at 6 ("... It is obvious and unarguable that no government interest is more compelling than the security of the Nation." (citing Haig v. Agee, 453 U.S. 280, 307 (1981))).

In furtherance of this objective, the government seeks to obtain from Yahoo communications that include communications to or from United States persons. See supra note 54. The directives at issue require Yahoo to provide to the government a [REDACTED] information relating to targeted accounts, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Declaration of [REDACTED] January 16, 2008; Declaration of [REDACTED] January 23, 2008 at 2 (noting, however, Yahoo's understanding that, at least initially, the government would only expect Yahoo to produce [REDACTED])

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

[REDACTED] Declaration of [REDACTED] January 23, 2008.⁷⁰ As noted above, the government concedes that at least some of this information is protected by the Fourth Amendment, and there is no question that extremely sensitive, personal information could be acquired through the directives, akin to electronic eavesdropping of telephone conversations.

Thus, unlike those circumstances involving a disparity between the importance of the government's interest and the degree of intrusiveness required to serve that interest, see, e.g., United States v. Martinez-Fuerte, 428 U.S. 543, 557-58 (1976) (analyzing traffic stops in which the government need is great but the intrusion is minimal), here there are weighty concerns on both sides of the equation. This Court, however, is not the first to assess the reasonableness of [REDACTED] surveillance.⁷¹ Since the enactment of the Foreign Intelligence Surveillance Act, two particularly significant opinions have examined the Fourth Amendment reasonableness of the acquisition by the government of foreign intelligence information through the interception of communications of United States persons: the FISC in In re Sealed Case, 310 F.3d 717 and the United States District Court for the Southern District of New York in United States v. Bin Laden, 126 F. Supp. 2d 264.

⁷⁰As may be obvious by the enumeration, this acquisition also will obtain [REDACTED] [REDACTED] communications of those persons who send communications to or receive communications from targeted accounts, regardless of whether these communicants are located outside the United States and without regard to whether such individuals are agents of foreign powers. See infra Part III.B.2.e for a further discussion of these communications.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

In determining the reasonableness of the acquisition at issue here, this Court will look to the factors considered by both courts, even though the facts of this case more closely resemble those presented in Bin Laden. However, because this Court is bound by the holding in In re Sealed Case, it must accord special consideration to that case in determining the extent to which the FISC's findings are applicable to a case such as this one, involving surveillance of United States persons abroad rather than within the boundaries of the United States.

a. In re Sealed Case

In re Sealed Case involved electronic surveillance conducted in the United States of the [REDACTED] communications of a United States person located in the United States.⁷² As noted above, the FISC implicitly found that the FISA orders fell within the parameters of the foreign intelligence exception to the warrant requirement. But, as this Court is also required to do, the FISC closely examined various facts and circumstances to determine whether the issuance of those orders was reasonable under the Fourth Amendment. In re Sealed Case, 310 F.3d at 736-42.

The FISC began its reasonableness analysis by looking to the requirements for the issuance of a warrant: issuance by a neutral detached magistrate, demonstration of probable

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

cause, and particularity. *Id.* at 738. The FISCRC compared the procedural framework of the surveillance at issue in that case with the procedures required by the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C.A. § 2510 *et seq.* (West 2000 & Supp. 2007) (Title III)⁷³ and noted that to the extent a FISA order differed from a Title III order, “few of those differences have any constitutional relevance.” *Id.* at 737. While it appears that the FISCRC determined that the three factors recited above were the essential factors to consider in assessing the constitutionality (and hence, the reasonableness) of a FISA order, the FISCRC also analyzed several other factors noting, “[t]here are other elements of Title III that at least some circuits have determined are constitutionally significant - that is, necessity, duration of surveillance, and minimization.” *Id.* at 740 (citation omitted). The following factors all appear to have been considered by the FISCRC in determining that the FISA orders were reasonable under the Fourth Amendment.

i. Prior Judicial Review

The FISCRC assessed that Title III and FISA were virtually identical so far as the requirement for prior judicial approval. As such, the FISCRC devoted little attention to analyzing this factor. However, given that the FISCRC highlighted prior judicial review as one of the three essential requirements of the Fourth Amendment Warrant Clause, it seems apparent that the FISCRC considered this to be a critical element in its reasonableness assessment.

⁷³ “[I]n asking whether FISA procedures can be regarded as reasonable under the Fourth Amendment, we think it is instructive to compare those procedures and requirements with their Title III counterparts. Obviously, the closer those FISA procedures are to Title III procedures, the lesser are our constitutional concerns.” *In re Sealed Case*, 310 F.3d at 737.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

ii. Probable Cause

The FISCER noted that orders issued pursuant to FISA and Title III required different probable cause findings. Under FISA, the FISC need only find probable cause to believe "that the target is a foreign power or an agent of a foreign power," *id.* at 738 (citing 50 U.S.C.A. § 1805(a)(3)), while Title III requires "'probable cause for belief that an individual is committing, has committed, or is about to commit' a specified predicate offense," *id.* (quoting 18 U.S.C.A. § 2518(3)(a)). The FISCER acknowledged that while the FISA probable cause showing was not as great as that required under Title III, FISA incorporated "another safeguard not present in Title III," *id.* at 739 - a probable cause requirement, if the target is an agent, that "the target is acting 'for or on behalf of a foreign power'," *id.* The FISCER concluded that the import of this additional showing is that it would ensure that FISA surveillance was only authorized to address, "certain carefully delineated, and particularly serious, foreign threats to national security." *Id.*

iii. Particularity

In addressing particularity, the FISCER focused on two components: one concerning the nature of the communications to be obtained through the surveillance and the second concerning the relationship between the facilities to be targeted and the activity or person being investigated. *Id.* at 739-40. With regard to the former, FISA mandates that a senior executive branch official⁷⁴ certify the purpose of the surveillance, including the type of foreign intelligence information

⁷⁴FISA identifies the officials authorized to make certifications as "the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate." 50 U.S.C.A. § 1804(a)(7).

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

sought. 50 U.S.C.A. § 1804(a)(7). The FISC judge considering the application is obliged to grant such certification great deference. *Id.* at 739. Only when the target is a United States person does the FISC even make a substantive finding concerning that certification and even then, the standard of review is merely clear error. 50 U.S.C.A. § 1805(a)(5).⁷⁵

The findings made with regard to the facilities to be targeted are significantly different between the two statutes. Under FISA, the FISC must find probable cause to believe that the target is using or about to use the targeted facility, without regard to the purpose for which the facility will be used by the target. 50 U.S.C.A. § 1805(a)(3)(B); compare 18 U.S.C.A. § 2518(3)(d). As the FISC noted, “[s]imply put, FISA requires less of a nexus between the facility and the pertinent communications than Title III, but more of a nexus between the target and the pertinent communications.” *Id.* at 740.

iv. Necessity

The FISC noted that while both statutes impose a necessity requirement, under FISA the assessment of necessity is made by the above-mentioned certifying official (a requirement not mandated by Title III), albeit subject to the above-described deferential standard of judicial review. *Id.* at 740.

v. Duration

Both statutes also address the length of time orders may remain in effect. FISA permits a longer duration than does Title III, but the FISC found the difference between 30 days and 90

⁷⁵Title III, on the other hand, requires that a judge make a probable cause finding that particular communications concerning the offense will be obtained. 310 F.3d at 739 (citing 18 U.S.C.A. § 2518(3)(b)).

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

days to be reasonable in light of the "nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information.'" *Id.* (citations omitted). The FISCER took further comfort in the fact that "the longer surveillance period is balanced by continuing FISC oversight of minimization procedures during that period." *Id.*

vi. Minimization

Finally, in addressing the requirement for minimization that is embodied in both statutes, the FISCER acknowledged that Title III focuses on minimization at the time of acquisition (thus, more effectively protecting the privacy interests of non-target communications), while FISA permits minimization at both the acquisition and retention stages. *Id.* at 740. This discrepancy, according to the FISCER, "may well be justified[.] . . . Given the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots." *Id.* at 741.⁷⁶

In summary, the FISCER relied upon a variety of factors in finding the FISA statute constitutional, and thus, that orders issued pursuant to it were reasonable under the Fourth Amendment. While the FISCER appears to have placed great stock in the fact that FISA applications must be subjected to prior judicial scrutiny, the Court did not find it constitutionally problematic that a senior government official, rather than a detached magistrate, made findings

⁷⁶The FISCER also addressed the amici filers' concerns that FISA does not parallel Title III's notice requirements or its requirement that a defendant may obtain the Title III application and order when challenging the legality of the surveillance. *Id.* at 741. The FISCER distinguished FISA from Title III in these two contexts and refused to find that the absence of these requirements undermined the reasonableness of the FISA orders under consideration. *Id.*

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

comparable to those that Title III requires a judge to make. *Id.* at 739-41. The FISCER was also satisfied with the probable cause findings made under FISA, *id.* at 738-39, as well as with the extended duration of orders issued under it. *Id.* at 740. Both particularity requirements in FISA weighed into the FISCER's analysis and the FISCER did not negatively opine on the fact that one of those findings was made by a senior executive branch official rather than a judge.

So, from the FISCER's opinion in *In re Sealed Case*, it is logical to assume that electronic surveillance targeted against United States persons within the United States is reasonable under the Fourth Amendment under the following circumstances: (1) there is some degree of prior judicial scrutiny, (2) there is probable cause to believe that the target is an agent of a foreign power (or a foreign power itself), (3) there is probable cause to believe that the facility to be targeted is being used or is about to be used by the target, (4) at least some constitutionally required determinations are made by the senior executive branch officials designated in the statute, subject to a highly deferential degree of judicial review, (5) the duration may extend to 90 days, particularly when there is Court oversight over minimization procedures, and (6) such minimization procedures are in place and being applied.

It is not clear from the FISCER opinion how much importance the Court attached to each of the above-described factors. For that reason, it is difficult to discern what effect the modification or removal of one of the factors would have on the overall determination of reasonableness. Nor is there clear guidance on how the requirements of reasonableness might vary for targets who are United States persons located outside of the United States.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

b. United States v. Bin Laden

A case that far more closely resembles the case now before this Court is United States v. Bin Laden, which involved search and surveillance targeted at a United States person located overseas. The facts there were the following.

In its investigation of al Qaeda in Kenya, in August 1996, the intelligence community began monitoring telephone lines used by certain persons associated with al Qaeda, including Wadih El-Hage, an American citizen. Bin Laden, 126 F. Supp. 2d at 269. Although the government was aware that El-Hage was a United States person, it was not until eight months later, on April 4, 1997, that the Attorney General specifically authorized search and surveillance of El-Hage pursuant to E.O. 12333, § 2.5. Id. at 269 & n.23.

At his criminal trial, El-Hage filed a motion to suppress evidence seized during the search of his home and the surveillance of his telephone and cellular telephone in Kenya, arguing that the search and surveillance violated his Fourth Amendment rights. Id. at 268, 270. The District Court found that the searches and surveillance conducted subsequent to the Attorney General's E.O. 12333 authorization fell under the foreign intelligence exception to the Fourth Amendment's warrant requirement and were reasonable; therefore, the evidence was lawfully acquired and not subject to suppression. Id. at 279, 288. However, the District Court found that surveillance conducted prior to April 4, 1997, was not incidental, as the government argued, and because the government had not obtained the Attorney General's authorization, was "not embraced by the foreign intelligence exception to the warrant requirement." Id. at 279. Further, because no warrant had issued, the Court found that the surveillance violated El-Hage's Fourth

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

Amendment rights. Id. at 281-82. However, for reasons not relevant to this matter, the Court declined to apply the exclusionary rule to the evidence that had been seized and intercepted. Id. at 282-84.

As the District Court in Bin Laden noted, in order to find that the surveillance did not offend the Fourth Amendment, the Court needed to find not only that the government met the requirements of the foreign intelligence exception to the warrant requirement, but also that the conduct of the surveillance was reasonable. Id. at 284. There, the Court identified three factors as being essential in order to find that electronic surveillance targeted against a United States person abroad fit within the foreign intelligence exception to the warrant requirement: (1) the target must be an agent of a foreign power, (2) the primary purpose of the surveillance must be to acquire foreign intelligence, and (3) the President or the Attorney General must authorize the surveillance. Id. at 277.⁷⁷ The Bin Laden Court found that all three criteria were satisfied by virtue of the Attorney General's E.O. 12333 authorization.

The District Court in Bin Laden then analyzed the reasonableness of the surveillance. Id. at 284-86. In response to El-Hage's concerns, the District Court acknowledged that the duration

⁷⁷These criteria appear to derive directly from the holding in United States v. Truong, 629 F.2d 908 at 915. See Bin Laden, 126 F. Supp. 2d at 275, 277-79. As already noted, the FISC took exception with Truong's articulation of the primary purpose requirement in its opinion in In re Sealed Case, 310 F.3d at 744. See supra pp. 61-62. Following the lead of the FISC, as discussed above, this Court holds that the foreign intelligence exception to the warrant requirement requires only that a significant purpose of the acquisition is to obtain foreign intelligence information, there is probable cause to believe the individual who is targeted is an agent of a foreign power and that such probable cause finding is made by a sufficiently authoritative official, such as the Attorney General.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

of a surveillance may be a factor to consider in analyzing reasonableness. *Id.* at 286. However, the District Court accepted the government's argument that "more extensive monitoring and 'greater leeway' in minimization efforts are permitted in a case like this given the 'world-wide, covert and diffuse nature of the international terrorist group(s) targeted.'" *Id.* (citations omitted). As this quote suggests, the Court appears to have found that the existence of minimization procedures bears upon reasonableness, although the Court did not address the necessary parameters of such procedures. *Id.* Finally, as part of its reasonableness analysis, the District Court, citing *United States v. Scott*, 516 F.2d 751, 759 (D.C. Cir. 1975), found it significant that the telephones were used communally by al Qaeda agents, thereby making it more reasonable for the government to monitor them than it would be if the phones were primarily used for legitimate, non-foreign intelligence-related purposes. *Id.*

Thus, the factors the *Bin Laden* Court appears to have relied upon to assess the reasonableness of the surveillance were: (1) the existence of minimization procedures, (2) the duration of the monitoring as balanced against both the minimization procedures and the nature of the threat being investigated, and (3) the extent to which the targeted facilities are used in support of the activity being investigated.

c. Reasonableness Factors

i. Common Factors Utilized in Both *In re Sealed Case* and *Bin Laden*

Comparing the factors relied upon by the FISC in *In re Sealed Case* and by the District Court in *Bin Laden*, some factors are common in both cases. These factors can provide the starting point for this Court's reasonableness analysis of the directives issued to Yahoo. Both

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

courts favorably noted that probable cause findings were made with regard to the target being an agent of a foreign power, In re Sealed Case, 310 F.3d at 738; Bin Laden, 126 F. Supp. 2d at 277-78, with the District Court expressly finding this factor to be an essential criterion for meeting the requirements of the foreign intelligence exception to the warrant requirement, id. at 277. Both Courts also relied upon the existence of minimization procedures in finding the surveillance at issue reasonable. In re Sealed Case, 310 F.3d at 740-41; Bin Laden, 126 F. Supp. 2d at 286. In addition, both Courts examined the duration of the authorized surveillance and both intimated that a longer duration must be balanced by more rigorous minimization procedures than might be reasonable for a shorter period of surveillance. In re Sealed Case, 310 F.3d at 740; Bin Laden, 126 F. Supp. 2d at 285-86. On this point, the FISC found a 90-day duration reasonable and the District Court seemed to find a several month duration to be reasonable (although it is not clear whether the District Court predicated its assessment on the 90-day re-authorization by the Attorney General in July 1997). Id.⁷⁸ Both Courts found it reasonable that at least some findings were made by high level executive branch officials, even though not made by a judge. In re Sealed Case, 310 F.3d at 739-40; Bin Laden, 126 F. Supp. 2d at 279. The District Court specifically found it necessary that the Attorney General or the President make the probable cause findings, id. at 279, while the FISC was satisfied that other senior executive branch officials make at least some of the necessary findings. In re Sealed Case, 310 F.3d at 739. The

⁷⁸The District Court seemed to accept the defendant's assertion that the surveillance against him had continued for many months. Bin Laden, 126 F. Supp. 2d at 285-86. It is unclear from the District Court opinion the significance it attached to the fact that the Attorney General, in accordance with E.O. 12333, re-authorized the surveillance 90 days after her initial authorization. Id. at 279.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

FISCR explicitly relied upon the fact that there was a finding as to the facilities being targeted, distinct from and in addition to the finding that the targeted individual is an agent of a foreign power. Id. at 739-40. The District Court, while it did not directly hold that there is a requirement for a prior finding concerning the targeted facilities, favorably noted that it was "highly relevant" that the targeted telephones were "'communal' phones which were regularly used by al Qaeda associates." Bin Laden, 126 F. Supp. 2d at 286.

ii. Factors Weighed Differently by the Two Courts

Two of the factors considered by the courts appear to have been weighed differently. The District Court explicitly rejected the requirement of prior judicial review of the government's application, id. at 275-77, while the FISCR found this to be an important consideration, In re Sealed Case, 310 F.3d at 738. And, while the FISCR explicitly addressed the requirement that there be a prior finding of probable cause to believe that a particular facility is being or will be used by the targeted agent, id. at 739-40, the District Court referred to this consideration only peripherally, Bin Laden, 126 F. Supp. 2d at 286.

* Prior Judicial Review Not Required

The FISCR favorably noticed that FISA orders are subject to prior judicial approval. The District Court, on the other hand, determined that such approval was not necessary under the circumstances of the case before it. While the FISCR was considering a request to conduct surveillance of a United States person located within the United States, the individual targeted in the matter presented to District Court, also a United States person, was located outside the United States.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

Without question, Congress is aware, and has been for quite some time, that the intelligence community conducts electronic surveillance of United States persons abroad without seeking prior judicial authorization. In fact, when Congress enacted FISA in 1978, it explicitly excluded overseas surveillance from the statute, as reflected in a House of Representatives Report that states, "this bill does not afford protections to U.S. persons who are abroad . . ." H.R. Rep. No. 95-1283, pt. 1 at 51 (1978). See also Bin Laden, 126 F.Supp. 2d at 272 n.8 (noting that FISA only governs foreign intelligence searches conducted within the United States). The Bin Laden Court examined the issue of prior judicial approval in the same context presented to the Court in this case, and observed that "[w]arrantless foreign intelligence collection has been an established practice of the Executive Branch for decades." Id. at 273 (citation omitted). Citing Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 610 (1952) ("[A] systematic, unbroken, executive practice, long pursued to the knowledge of Congress and never before questioned, engaged in by Presidents who have also sworn to uphold the Constitution, making as it were such exercise of power part of the structure of our government, may be treated as a gloss on 'Executive Power' vested in the President by § 1 of Art. II.") and Payton v. New York, 445 U.S. 573, 600 (1980) ("A longstanding, widespread practice is not immune from constitutional scrutiny. But neither is it to be lightly brushed aside."), the District Court further noted that, "[w]hile the fact of [congressional and Supreme Court silence with regard to foreign intelligence collection abroad] is not dispositive of the question before this Court, it is by no means insignificant." Bin Laden, 126 F. Supp. 2d at 273. This Court finds the reasoning of the District Court persuasive and therefore accepts as a general principle, that prior judicial approval of an

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

acquisition of foreign intelligence information targeted against a United States person abroad is not an essential element for a finding of reasonableness under the Fourth Amendment.

* Probable Cause to Believe that the Targeted Facility is Being or is About to be Used

The FISCRC directly, and favorably, addressed the requirement in FISA that a prior showing be made that the targeted individuals were using or were about to use the targeted facilities. In re Sealed Case, 310 F.3d at 739-40. The District Court considered this factor more obliquely. Bin Laden, 126 F. Supp. 2d at 286.

The FISCRC characterized the judicial finding of probable cause to believe the targeted facility is being or is about to be used by the targeted agent as a particularity requirement, and therefore, one of the required elements of a Fourth Amendment warrant. Given that the FISCRC analyzed reasonableness in relation to the warrant requirement, it is not surprising that the FISCRC found this factor to be constitutionally significant in assessing reasonableness. In re Sealed Case, 310 F.3d at 739-40. The District Court in Bin Laden expressed no direct view on this factor, nor does its opinion make clear if the Attorney General's authorizations included a probable cause finding regarding the use of the facilities to be targeted. However, as noted above, the District Court did consider the use of the targeted facilities in its reasonableness assessment. Bin Laden, 126 F. Supp. 2d at 286. The disparity between the attention given to this factor by the two Courts may well be explained by the fact that the FISCRC was considering the conduct of electronic surveillance within the United States while the District Court was analyzing surveillance conducted overseas. The Fourth Amendment particularity requirement serves, in large part, as a check to minimize the likelihood that persons who have a reasonable expectation

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

of privacy are not mistakenly subjected to government surveillance.⁷⁹ When the surveillance activity is conducted against persons outside the United States, the persons who would be inappropriately surveilled most likely would be non-United States persons. And, this is not a class of persons who enjoy the protections of the Fourth Amendment. Therefore, it seems reasonable that, in the overseas context, there is less of a need to require a prior showing of probable cause to believe that a properly targeted individual is using or is about to use a specific, targeted facility.

iii. Necessity

The FISCER noted that FISA incorporates a “necessity” provision, as does Title III. In re Sealed Case, 310 F.3d at 740. The District Court in Bin Laden, however, makes no mention of necessity. A showing of necessity is not always a prerequisite for reasonableness. Illinois v. Lafayette, 462 U.S. 640, 647 (1983) (“[t]he reasonableness of any particular governmental activity does not necessarily or invariably turn on the existence of alternative ‘less intrusive’ means”). And, this Court is not persuaded that, in the context of the PAA, any ameliorative purpose would be served by requiring the government to demonstrate that less intrusive means have been attempted. Indeed, the very purpose of the PAA is to provide the government with “flexible procedures to collect foreign intelligence from foreign terrorists overseas . . . [that do]

⁷⁹While discussions of the particularity requirement typically focus on the “property to be sought” rather than the person using that property, Berger v. New York, 388 U.S. 41, 59 (1967), it is clearly the privacy interests of the individual that the Constitution protects. Verdugo-Urquidez, 494 U.S. at 266. Thus, in the context of electronic surveillance of email communications, if the government surveils the wrong email account, the harm would be against the privacy interests of persons whose communications were improperly acquired.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

not impose unworkable, bureaucratic requirements that would burden the intelligence community.” 153 Cong. Rec. H9954 (daily ed. Aug. 4, 2007) (statement of Rep. Smith). Therefore, this Court will not consider the availability of less intrusive means as a factor in determining the reasonableness of the directives issued to Yahoo.

iv. Warrant Exception Criteria Are Factors to Consider in Assessing Reasonableness.

The factors that provide the basis for the foreign intelligence exception to the warrant requirement (a significant foreign intelligence purpose and probable cause to believe that any United States person who is targeted is an agent of a foreign power) are also key elements that weigh in assessing reasonableness.

d. Application of the Reasonableness Factors to the Acquisition of Targeted United States Persons’ Communications Through the Directives Issued to Yahoo

In assessing the Fourth Amendment reasonableness of the acquisition of foreign intelligence information through the directives issued to Yahoo, this Court relies on the findings made above in Part III.B.1 of this Opinion, in which it found that the surveillance satisfies the requirements for the foreign intelligence exception to the warrant requirement. In addition, this Court will consider the following factors relied upon by the FISC in In re Sealed Case and the District Court in Bin Laden: (1) minimization, (2) duration, (3) authorization by a senior government official, and (4) identification of facilities to be targeted.

But, first, this Court must acknowledge the statutory framework that governs the proposed acquisitions. The PAA only authorizes “the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States ...” 50

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

U.S.C.A. § 1805b(a) (emphasis added). The statute further requires that “there are reasonable procedures in place for determining that the acquisition of foreign intelligence under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 105C of this Act.” 50

U.S.C.A. § 1805b(a)(1) (emphasis added).⁶⁰

This Court sees no reason to question the presumption that the vast majority of persons who are located overseas are not United States persons and that most of their communications are with other, non-United States persons,⁶¹ who also are located overseas. Thus, most of the communications that will be obtained through the directives issued to Yahoo likely will be communications between non-United States persons abroad, *i.e.*, persons who do not enjoy the protection of the Fourth Amendment.⁶² So, to the extent “reasonable” procedures represent an effort to minimize the likelihood of targeting the wrong facility or the wrong person or of obtaining the communications of non-targeted communicants, a program such as this, which is focused on overseas collection, presents fewer Fourth Amendment concerns than does a program

⁶⁰See *supra* Part II.B for this Court’s resolution of the ambiguities related to this provision.

⁶¹This common sense presumption is embodied in the Department of Defense procedures governing the collection of information about United States persons, which state, “[a] person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person’s communications or other available information concerning the person give rise to a reasonable belief that such person is a United States citizen or permanent resident alien.” DoD Procedures, Procedure 5, Part 3.B.4.

⁶²*Supra* note 69.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

that focuses on domestic communications within the United States.⁸³ It is against this backdrop that this Court will assess the appropriate reasonableness factors.

i. Minimization

By statute, the communications that will be acquired through the directives issued to Yahoo will be subject to minimization procedures that are supposed to comport with the definition of “minimization procedures” under 50 U.S.C.A. § 1801(h). 50 U.S.C.A. § 1805b(a)(5). This Court has reviewed the minimization procedures applicable to these directives and finds that they are virtually the same procedures the government uses for many non-PAA FISA collections. Feb. 2008 Classified Appendix at [REDACTED]

[REDACTED] In other contexts, this Judge has (as other Judges on the FISC have) found these non-PAA procedures to be reasonable under circumstances in which the government is intercepting private email communications.

This Court, therefore, finds the minimization procedures filed by the government to be sufficiently robust to protect the interests of United States persons whose communications might be acquired through the acquisition of information obtained through the directives issued to

⁸³This Court appreciates Yahoo’s concern that “it is possible that the ‘target’ may return to the U.S. during the surveillance period. Therefore, the Directives may target U.S. citizens who may be in the U. S. when under surveillance.” Yahoo’s Mem. in Opp’n at 9. However, the Court has reviewed the government’s targeting procedures and notes that the government has specifically addressed this issue and has robust procedures in place to [REDACTED] cease such surveillance “without delay[]” when it is determined that the target is in the United States. Feb. 2008 Classified Appendix at [REDACTED] see also *id.* at [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

Yahoo, and that these procedures satisfy the definition of "minimization procedures" under 50 U.S.C.A. § 1801(h).

ii. Duration

The PAA permits the Director of National Intelligence and the Attorney General to authorize the acquisition of foreign intelligence information for a period of up to one year. 50 U.S.C.A. § 1805b(a). However, in each of the certifications filed with this Court, the Director of National Intelligence and the Attorney General assert that prior to targeting a United States person, the government must obtain Attorney General authorization using the procedures under E.O. 12333, § 2.5. Feb. 2008 Classified Appendix at [REDACTED] One of the provisions of those procedures is that surveillance conducted pursuant to the Attorney General's authorization may not exceed 90 days. DoD Procedures, Procedure 5, Part 2.C.6. Thus, for those targeted individuals who have Fourth Amendment protection, *i.e.*, United States persons, the Court assumes that the Attorney General will re-authorize the acquisition every 90 days in order for the acquisition under the PAA to continue.⁸⁴

Ninety days is the identical duration the FISC found reasonable in the matter it considered. The FISC noted in *In re Sealed Case* that the longer duration under FISA (*i.e.*, 90 days rather than the 30-day duration in Title III) "is based on the nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information.'" 310 F.3d at 740 (citations omitted). However, the FISC also suggested

⁸⁴It is therefore also this Court's assumption that if the Attorney General does not issue a new authorization, surveillance of the targeted account will cease.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

that the 90-day duration was reasonable in part because the FISC exercised oversight over the minimization procedures while a surveillance is being conducted. *Id.* But, the PAA does not provide a similar role for the FISC. Notably, though, under the PAA, the target of the surveillance will be located overseas, and presumably, so will be a significant number of the persons who communicate with that target, while under a domestic FISA surveillance, it is feasible, and indeed likely, that the bulk of the information obtained would be to, from, or about United States persons. Therefore, to the extent judicial oversight over minimization serves to enhance the protection afforded United States persons whose communications are intercepted, the importance of such oversight wanes when a reduced proportion of United States person information will be acquired. Indeed, in Bin Laden, there was no judicial oversight of the minimization procedures whatsoever. And, in that case, the Court did not find a duration of approximately eight months to be unreasonable.⁸⁵ Therefore, on balance, this Court finds a 90-day duration for the acquisition of communications targeting United States persons under the circumstances presented in this case, even without judicial oversight of the application of the minimization procedures, reasonably limited.

iii. Senior Official Approval

Prior to the issuance of its directives to Yahoo, as required by the statute, the Attorney General and the Director of National Intelligence determined, through written certifications under

⁸⁵Supra note 78 and accompanying text.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

oath, that were supported by affidavits from the Director of NSA, that

there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under section 105B . . . concerns persons reasonably believed to be located outside the United States[.] . . . the acquisition does not constitute electronic surveillance as defined in section 101(f) of the Act[.] the acquisition involves obtaining foreign intelligence information from or with the assistance of communications service providers . . .[.] a significant purpose of the acquisition is to obtain foreign intelligence information and [.] the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h) of the Act.

Feb. 2008 Classified Appendix at [REDACTED] see also id. at [REDACTED]

[REDACTED] It is this Court's view that the certifications of these two officials represent a sufficient restraint on the exercise of arbitrary action by those in the executive branch who are effecting the actual acquisition of information, see In re Sealed Case, 310 F.3d at 739 (characterizing congressional intent that the certification by senior officials, "typically the FBI Director [with approval by] the Attorney General or the Attorney General's Deputy," would provide written accountability and serve as "an internal check on Executive Branch arbitrariness") (citation omitted); H.R. Rep. 1283 at 80, and thus weighs favorably in assessing the reasonableness of the directives issued to Yahoo.

iv. Identifying Targeted Facilities

The final factor to consider in determining the reasonableness of the directives is the identification of the accounts to be targeted. As discussed above, the manner in which accounts are targeted for surveillance is an important consideration in determining the reasonableness of a

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

warrantless surveillance.⁸⁶ For the following reasons, the Court finds that the current procedures employed by the government are reasonable, given all the facts and circumstances of the anticipated acquisition.

In a typical foreign intelligence case where the intelligence activity is conducted within the United States, the government first establishes probable cause to believe that a particular individual is an agent of a foreign power and then identifies the specific facility the person is using that the government wants to monitor. By establishing probable cause to believe that the target is using a particular facility (as is required under the non-PAA provisions of FISA, 50 U.S.C.A. §§ 1804(a)(3)(B) & 1805(a)(3)(B)), the government is demonstrating the nexus between the person being targeted and the facility that is going to be monitored. This nexus requirement diminishes the likelihood that the government will monitor the communications of a completely innocent United States person, which would, on its face, appear to be an unreasonable search, and thus, violative of the Fourth Amendment.

The PAA, by its terms, however, only allows the acquisition of communications which are reasonably believed to be used by persons located outside the United States. 50 U.S.C.A. §§ 1805a & 1805b(a). As stated above,⁸⁷ this Court can envision no reason to question the presumption that most people who are located outside the United States are not United States

⁸⁶The Court is mindful that the PAA specifically provides that "[a] certification under subsection (a) is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed." 50 U.S.C.A. § 1805b(b); see also supra Part II.C.

⁸⁷Supra note 81.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

persons. So, even if, after establishing probable cause to believe a particular United States person is an agent of a foreign power, the government, pursuant to the PAA, mistakenly targets an account used by someone other than that United States person, the likelihood is that the person whose privacy interests are implicated is a person who does not enjoy the protection of the Fourth Amendment.

Moreover, by the terms of Lt. Gen. Alexander's affidavit, upon which the Director of National Intelligence and the Attorney General relied when making their certifications, Feb. 2008 Classified Appendix at [REDACTED] the government will only target accounts (whether the user is a United States person or not) if there is some basis for believing that such account will likely be used to communicate information concerning one of the foreign powers specified in the certification. So, even if a targeted account is mistakenly associated with an incorrect user, that account would have been targeted only after United States intelligence analysts had assessed that there is some basis for believing the particular account is being used to convey information of foreign intelligence interest related to the certifications. Therefore, given the provision of the statute that limits acquisition to persons reasonably believed to be located outside the United States, coupled with the process articulated by Lt. Gen. Alexander for limiting surveillance to those accounts that are likely to provide foreign intelligence information related to the certifications, this Court finds that the procedures in place to identify the facilities to be targeted contribute favorably to the reasonableness of the directives issued to Yahoo.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

- v. In Sum, the Acquisition of Foreign Intelligence Information Targeting United States Persons Abroad Obtained Pursuant to the Directives Issued to Yahoo is Reasonable Under the Fourth Amendment.

Having considered the totality of the facts and circumstances, including:

- (1) the statute, which by its terms, limits acquisition to foreign intelligence communications of persons reasonably believed to be located outside the United States and requires written procedures for establishing the basis for making these determinations, procedures that have been reviewed by the Court;
- (2) United States persons will not be targeted unless the Attorney General has determined, in accordance with E.O. 12333, § 2.5 procedures, that there is probable cause to believe that such person is an agent of a foreign power;
- (3) the Director of National Intelligence and the Attorney General have certified that a significant purpose of the acquisition is to obtain foreign intelligence information;
- (4) each authorization for the acquisition of targeted United States person communications is limited to 90 days;
- (5) there are reasonable minimization procedures in place, which meet the definition of "minimization procedures" under 50 U.S.C.A. § 1801(h); and
- (6) there are written procedures in place to ensure that surveillance of the facilities to be targeted likely will obtain foreign intelligence information,

this Court is satisfied that the government currently has in place sufficient procedures to ensure that the Fourth Amendment rights of targeted United States persons are adequately protected and

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

that the acquisition of the foreign intelligence to be obtained through the directives issued to Yahoo, as to these individuals, is reasonable under the Fourth Amendment.

c. The Reasonableness of Incidentally Acquiring Communications of United States Persons

The previous section of this Opinion concerned the Fourth Amendment rights of those United States persons whose communications are targeted. However, the universe of communications that will be acquired through the directives issued to Yahoo will include the communications of persons who communicate with the targeted accounts.⁸⁸ Yahoo argues, Yahoo's Mem. in Opp'n at 9, and the government concedes, "[t]he directives therefore, implicate, to varying degrees, the Fourth Amendment rights of ... persons, whether abroad or inside the United States, who are communicating with foreign intelligence targets outside the United States." Gov't.'s Supp. Brief on the Fourth Amend. at 2. This Court agrees that some subset of non-target communicants located in the United States and non-target communicants who are United States persons, whether located in the United States or abroad, enjoy Fourth Amendment protection. United States v. Verdugo-Urquidez, 494 U.S. 259.

As the District Court in Bin Laden noted, "... incidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment." 126 F. Supp. 2d at 280 (citations omitted). Likewise, the Second Circuit has held,

⁸⁸It is this Court's understanding that the directives issued to Yahoo will result in the acquisition of non-target communications only if the non-targeted account is in direct communication with a targeted account or if a communication of the non-targeted account is forwarded to a targeted account. See Declaration of [REDACTED] January 16, 2008; Declaration of [REDACTED] January 23, 2008.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

"[i]f probable cause has been shown as to one such participant, the statements of the other participants may be intercepted if pertinent to the investigation." United States v. Tortorello, 480 F.2d 764, 775 (2d Cir. 1973). As discussed earlier in this opinion, supra Part II, this Court has found that the acquisition of communications obtained through the directives issued to Yahoo adheres to the requirements of the PAA. And, as discussed immediately above, this Court has found that the acquisition of the communications of targeted United States persons obtained through the directives issued to Yahoo is reasonable and therefore complies with the Fourth Amendment.

This Court also notes that, in addition to the underlying surveillance being lawful, the government has in place minimization procedures designed to protect the privacy interests of United States persons. As required by the PAA, the government must have procedures in place that comport with the definition of minimization procedures under section 1801(h) of FISA.

That definition specifies that such procedures must be

- (1) specific procedures ... 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;
- (2) procedures that require that nonpublicly available information, which is not foreign intelligence information ... 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[.]

50 U.S.C.A. § 1801(h)(1) & (2) (emphasis added). This Court agrees with the government that these minimization procedures adequately protect the privacy interests of persons whose

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

communications might be incidentally acquired. Mem. in Support of Gov't Motion at 19; see also Feb. 2008 Classified Appendix at [REDACTED]

Based on the above considerations, this Court finds that any incidental acquisition of the communications of non-targeted persons located in the United States and of non-targeted United States persons, wherever they may be located, is also reasonable under the Fourth Amendment.

IV. Conclusion


There are times when there is an inevitable tension between the interests protected by the Fourth Amendment on the one hand and the federal government's obligation to protect the security of the nation on the other hand. This reality has been particularly acute in an era of ever increasing communications and intelligence technology, when at the same time the threat of global terrorism has intensified, ultimately reaching the American mainland with devastating consequences on September 11, 2001. That is the landscape which confronted the United States Congress when the legislation that is the subject of this Opinion was enacted. Congress obviously sought to strike the proper balance between the sometime conflicting interests of individual privacy and national security when it adopted the PAA. But as illustrated by the painstaking and complex constitutional and statutory analysis this Court had to conduct to resolve the dispute in this case, the balance is not easily achieved. Despite the concerns the Court has expressed regarding several aspects of the legislation, for the reasons set forth above, this Court finds that the directives issued by the government to Yahoo satisfy the requirements of the PAA, do not offend the Fourth Amendment, and are otherwise lawful. Accordingly, Yahoo

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

is instructed to comply with the directives and an Order directing Yahoo to do so is being issued contemporaneously with this Opinion.

ENTERED this 25th day of April, 2008 in Docket Number 105B(g): 07-01.


REGGIE B. WALTON
Judge, Foreign Intelligence Surveillance Court

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

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

Page 98

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE PRODUCTION OF TANGIBLE THINGS FROM :

[REDACTED] :
[REDACTED] :
[REDACTED] :

Docket No.: BR 08-13

SUPPLEMENTAL OPINION

This Supplemental Opinion memorializes the Court's reasons for concluding that the records to be produced pursuant to the orders issued in the above-referenced docket number are properly subject to production pursuant to 50 U.S.C.A. § 1861 (West 2003 & Supp. 2008), notwithstanding the provisions of 18 U.S.C.A. §§ 2702-2703 (West 2000 & Supp. 2008), amended by Public Law 110-401, § 501(b)(2) (2008).

As requested in the application, the Court is ordering production of telephone "call detail records or 'telephony metadata,'" which "includes comprehensive communications routing information, including but not limited to session identifying information . . . , trunk identifier, telephone calling card numbers, and time and duration of [the] calls," but "does not include the substantive content of any communication." Application at 9; Primary Order at 2. Similar productions have been ordered by judges of the Foreign Intelligence Surveillance Court ("FISC"). See Application at 17. However, this is the first application in which the government has identified the provisions of 18 U.S.C.A. §§ 2702-2703 as potentially relevant to whether such orders could properly be issued under 50 U.S.C.A. § 1861. See Application at 6-8.

Pursuant to section 1861, the government may apply to the FISC "for an order requiring the production of any tangible things (including books, records, papers, documents, and other items)." 50 U.S.C.A. § 1861(a)(1) (emphasis added). The FISC is authorized to issue the order, "as requested, or as modified," upon a finding that the application meets the requirements of that section. Id. at § 1861(c)(1). Under the rules of statutory construction, the use of the word "any" in a statute naturally connotes "an expansive meaning," extending to all members of a common set, unless Congress employed "language limiting [its] breadth." United States v. Gonzales, 520 U.S. 1, 5 (1997); accord Ali v. Federal Bureau of Prisons, 128 S. Ct. 831, 836 (2008)

(“Congress’ use of ‘any’ to modify ‘other law enforcement officer’ is most naturally read to mean law enforcement officers of whatever kind.”).¹

However, section 2702, by its terms, describes an apparently exhaustive set of circumstances under which a telephone service provider may provide to the government non-content records pertaining to a customer or subscriber. See § 2702(a)(3) (except as provided in § 2702(c), a provider “shall not knowingly divulge a record or other [non-content] information pertaining to a subscriber or customer . . . to any governmental entity”). In complementary fashion, section 2703 describes an apparently exhaustive set of means by which the government may compel a provider to produce such records. See § 2703(c)(1) (“A governmental entity may require a provider . . . to disclose a record or other [non-content] information pertaining to a subscriber . . . or customer . . . only when the governmental entity” proceeds in one of the ways described in § 2703(c)(1)(A)-(E)) (emphasis added). Production of records pursuant to a FISC order under section 1861 is not expressly contemplated by either section 2702(c) or section 2703(c)(1)(A)-(E).

If the above-described statutory provisions are to be reconciled, they cannot all be given their full, literal effect. If section 1861 can be used to compel production of call detail records, then the prohibitions of section 2702 and 2703 must be understood to have an implicit exception for production in response to a section 1861 order. On the other hand, if sections 2702 and 2703 are understood to prohibit the use of section 1861 to compel production of call detail records, then the expansive description of tangible things obtainable under section 1861(a)(1) must be construed to exclude such records.

The apparent tension between these provisions stems from amendments enacted by Congress in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (“USA PATRIOT Act”), Public Law 107-56, October 26, 2001, 115 Stat. 272. Prior to the USA PATRIOT Act, only limited types of records, not

¹ The only express limitation on the type of tangible thing that can be subject to a section 1861 order is that the tangible thing “can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things.” Id. at § 1861(c)(2)(D). Call detail records satisfy this requirement, since they may be obtained by (among other means) a “court order for disclosure” under 18 U.S.C.A. § 2703(d). Section 2703(d) permits the government to obtain a court order for release of non-content records, or even in some cases of the contents of a communication, upon a demonstration of relevance to a criminal investigation.

including call detail records, were subject to production pursuant to FISC orders.² Section 215 of the USA PATRIOT Act replaced this prior language with the broad description of “any tangible thing” now codified at section 1861(a)(1). At the same time, the USA PATRIOT Act amended sections 2702 and 2703 in ways that seemingly re-affirmed that communications service providers could divulge records to the government only in specified circumstances,³ without expressly referencing FISC orders issued under section 1861.

The government argues that section 1861(a)(3) supports its contention that section 1861(a)(1) encompasses the records sought in this case. Under section 1861(a)(3), which Congress enacted in 2006,⁴ applications to the FISC for production of several categories of sensitive records, including “tax return records” and “educational records,” may be made only by the Director, the Deputy Director or the Executive Assistant Director for National Security of the Federal Bureau of Investigation (“FBI”). 18 U.S.C.A. § 1861(a)(3). The disclosure of tax return records⁵ and educational records⁶ is specifically regulated by other federal statutes, which do not by their own terms contemplate production pursuant to a section 1861 order. Nonetheless, Congress clearly intended that such records could be obtained under a section 1861 order, as demonstrated by their inclusion in section 1861(a)(3). But, since the records of telephone service providers are not mentioned in section 1861(a)(3), this line of reasoning is not directly on point. However, it does at least demonstrate that Congress may have intended the sweeping description of tangible items obtainable under section 1861 to encompass the records of telephone service providers, even though the specific provisions of sections 2702 and 2703 were not amended in order to make that intent unmistakably clear.

² See 50 U.S.C.A. § 1862(a) (West 2000) (applying to records of transportation carriers, storage facilities, vehicle rental facilities, and public accommodation facilities).

³ Specifically, the USA PATRIOT Act inserted the prohibition on disclosure to governmental entities now codified at 18 U.S.C.A. § 2702(a)(3), and exceptions to this prohibition now codified at 18 U.S.C.A. § 2702(c). See USA PATRIOT Act § 212(a)(1)(B)(iii) & (E). The USA PATRIOT Act also amended the text of 18 U.S.C.A. § 2703(c)(1) to state that the government may require the disclosure of such records only in circumstances specified therein. See USA PATRIOT Act § 212(b)(1)(C)(i).

⁴ See Public Law 109-177 § 106(a)(2) (2006).

⁵ See 26 U.S.C.A. § 6103(a) (West Supp. 2008), amended by Public Law 110-328 § 3(b)(1) (2008).

⁶ See 20 U.S.C.A. § 1232g(b) (West 2000 & Supp. 2008).

The Court finds more instructive a separate provision of the USA PATRIOT Act, which also pertains to governmental access to non-content records from communications service providers. Section 505(a) of the USA PATRIOT Act amended provisions, codified at 18 U.S.C.A. § 2709 (West 2000 & Supp. 2008), enabling the FBI, without prior judicial review, to compel a telephone service provider to produce “subscriber information and toll billing records information.” 18 U.S.C.A. § 2709(a).⁷ Most pertinently, section 505(a)(3)(B) of the USA PATRIOT Act lowered the predicate required for obtaining such information to a certification submitted by designated FBI officials asserting its relevance to an authorized foreign intelligence investigation.⁸

Indisputably, section 2709 provides a means for the government to obtain non-content information in a manner consistent with the text of sections 2702-2703.⁹ Yet section 2709 merely requires an FBI official to provide a certification of relevance. In comparison, section 1861 requires the government to provide to the FISC a “statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant” to a foreign intelligence investigation,¹⁰ and the FISC to determine that the application satisfies this

⁷ This process involves service of a type of administrative subpoena, commonly known as a “national security letter.” David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 19:2 (2007).

⁸ Specifically, a designated FBI official must certify that the information or records sought are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.” 18 U.S.C.A. § 2709(b)(1)-(2) (West Supp. 2008). Prior to the USA PATRIOT Act, the required predicate for obtaining “local and long distance toll billing records of a person or entity” was “specific and articulable facts giving reason to believe that the person or entity . . . is a foreign power or an agent of a foreign power.” See 18 U.S.C.A. § 2709(b)(1)(B) (West 2000).

⁹ Section 2703(c)(2) permits the government to use “an administrative subpoena” to obtain certain categories of non-content information from a provider, and section 2709 concerns use of an administrative subpoena. See note 7 supra.

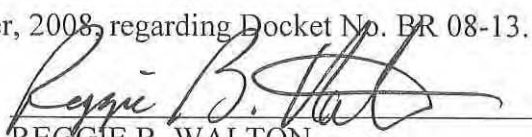
¹⁰ 50 U.S.C.A. § 1861(b)(2)(A). More precisely, the investigation must be “an authorized investigation (other than a threat assessment) . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities,” id., “provided that such investigation of a United States
(continued...)

requirement, see 50 U.S.C.A. § 1861(c)(1), before records are ordered produced. It would have been anomalous for Congress, in enacting the USA PATRIOT Act, to have deemed the FBI's application of a "relevance" standard, without prior judicial review, sufficient to obtain records subject to sections 2702-2703, but to have deemed the FISC's application of a closely similar "relevance" standard insufficient for the same purpose. This anomaly is avoided by interpreting sections 2702-2703 as implicitly permitting the production of records pursuant to a FISC order issued under section 1861.

It is the Court's responsibility to attempt to interpret a statute "as a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into an harmonious whole." Food & Drug Admin. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000) (internal quotations and citations omitted). For the foregoing reasons, the Court is persuaded that this objective is better served by the interpretation that the records sought in this case are obtainable pursuant to a section 1861 order.

However, to the extent that any ambiguity may remain, it should be noted that the legislative history of the USA PATRIOT Act is consistent with this expansive interpretation of section 1861(a)(1). See 147 Cong. Rec. 20,703 (2001) (statement of Sen. Feingold) (section 215 of USA PATRIOT Act "permits the Government . . . to compel the production of records from any business regarding any person if that information is sought in connection with an investigation of terrorism or espionage;" "all business records can be compelled, including those containing sensitive personal information, such as medical records from hospitals or doctors, or educational records, or records of what books somebody has taken out from the library") (emphasis added). In this regard, it is significant that Senator Feingold introduced an amendment to limit the scope of section 1861 orders to records "not protected by any Federal or State law governing access to the records for intelligence or law enforcement purposes," but this limitation was not adopted. See 147 Cong. Rec. 19,530 (2001).

ENTERED this 12th day of December, 2008, regarding Docket No. BR 08-13.


REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

¹⁰(...continued)

person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Id. § 1861(a)(1). The application must also include minimization procedures in conformance with statutory requirements, which must also be reviewed by the FISC. Id. § 1861(b)(2)(B), (c)(1), & (g).

~~TOP SECRET//COMINT//NOFORN~~

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



:

: Docket Number:



:

:

ORDER

On April 3, 2007, I entered an Order and Memorandum Opinion in the above-captioned docket number (April 3 Order), in response to the first application filed in the above-captioned docket number on March 21, 2007. The April 3 Order held that the proposed electronic surveillance was directed at individual telephone numbers and e-mail addresses, rather than the facilities

identified by the Government. *Id.* at 6-16. It also granted a motion by the Government for leave to file for an extension of the prior order, in Docket No. under which this surveillance was previously authorized. *Id.* at 20-21. Leave to

~~TOP SECRET//COMINT//NOFORN~~

Derived from: Application to the USFISC in the
Docket Number captioned above

~~TOP SECRET//COMINT//NOFORN~~

seek an extension was granted in order to "give the government a reasonable amount of time to work in good faith toward the preparation and submission of a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion." *Id.* at 21.

On April 5, 2007, the Government obtained from another judge of this Court an extension of the order in Docket No. [REDACTED]. Under that extension, current surveillance authorities expire at 5:00 p.m. on May 31, 2007.

The April 3 Order also required the Government to submit periodic reports regarding its efforts to prepare and submit a revised and supplemented application. In its report submitted on April 20, 2007, the Government articulated a new legal theory, under which it proposed that the Court would make probable cause findings for each telephone number and e-mail address identified at the time of the application as one at which surveillance would be directed, but that the Government could initiate electronic surveillance of later-discovered numbers and addresses, subject to reporting to the Court under 50 U.S.C. § 1805(c)(3).

On May 24, 2007, the Government filed a revised and supplemented application that seeks, *inter alia*, authority to conduct electronic surveillance of more than [REDACTED] identified telephone numbers and e-mail addresses and to initiate electronic

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

surveillance of later-discovered numbers and addresses on the theory noted above. On May 30, 2007, the Government submitted a Supplemental Declaration of Lieutenant General Keith B. Alexander, U.S. Army, Director of the National Security Agency (NSA), as well as a Declaration of (b)(3); (b)(6), NSA. Both the revised and supplemented application and the Supplemental Declaration filed on May 30 contain individual statements of the Government's factual basis for asserting probable cause to believe that each identified telephone number and e-mail address is being used, or about to be used, by one of the targeted foreign powers. I have reviewed each of these statements of facts, which were provided on a rolling basis prior to their formal submission. This Order addresses the revised and supplemented application, as further supplemented by the declarations filed on May 30, 2007, and by the Notice of Withdrawal, in Part, of Application for an Order Authorizing Electronic Surveillance filed on May 31, 2007 (the application). The Court continues to exercise jurisdiction over this matter for the reasons stated in the April 3 Order at page 8 n.12.

Having given full consideration to the matters set forth in the Government's application and all of the Government's other filings in this docket, as well as the hearings I have conducted with the Government, I find as follows:

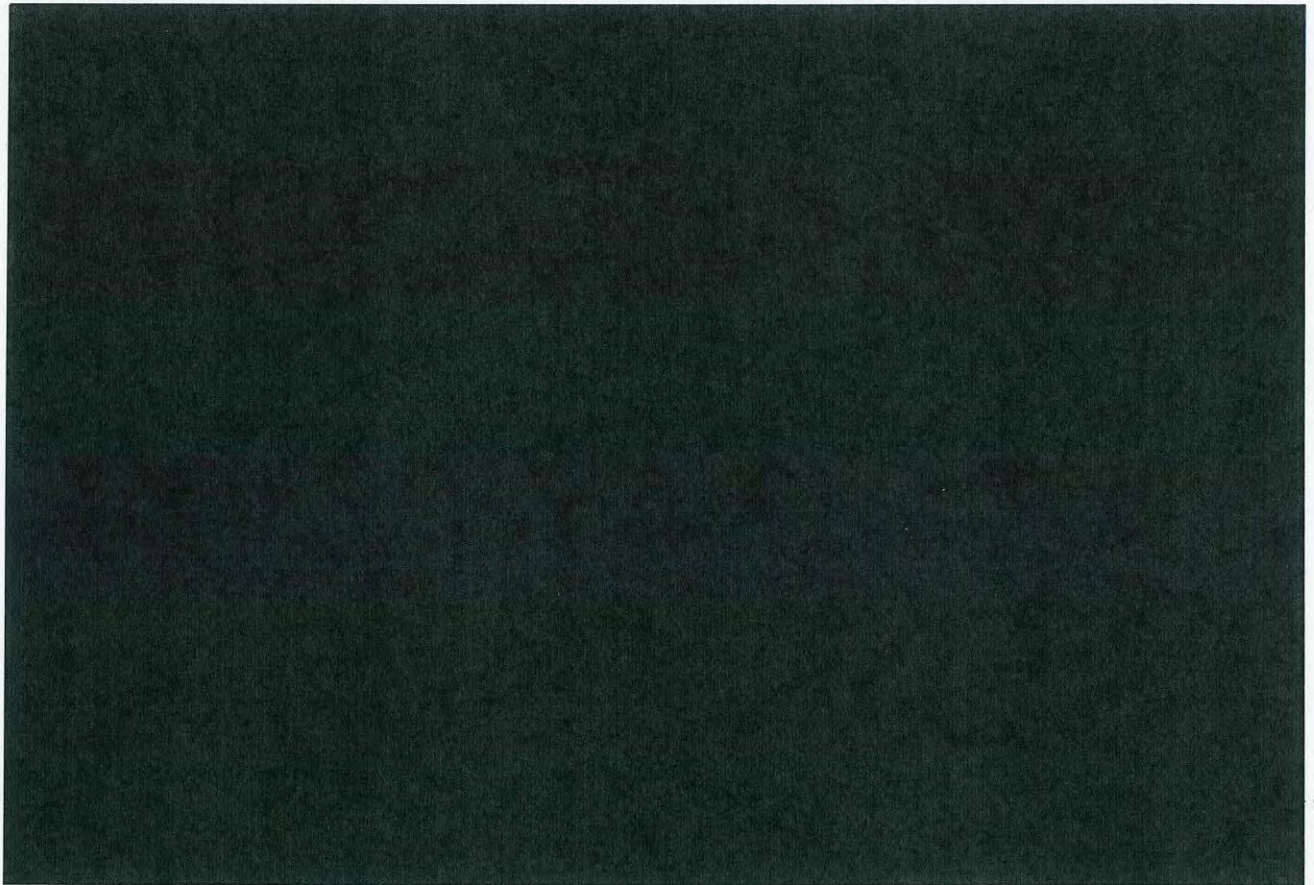
~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

1. The President has authorized the Attorney General of the United States to approve applications for electronic surveillance for foreign intelligence information [50 U.S.C. § 1805(a)(1)];

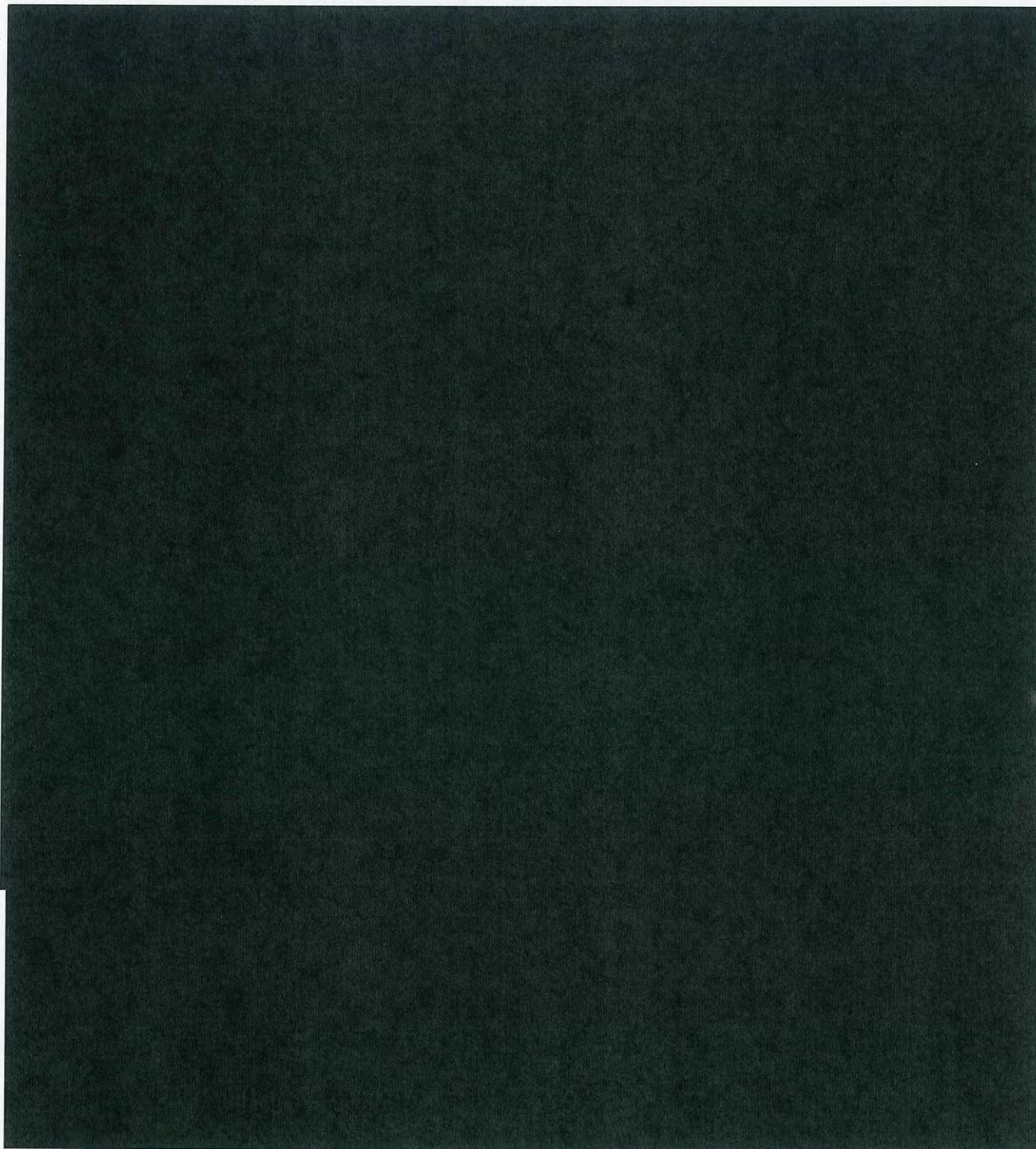
2. The application has been made by a Federal officer and approved by the Attorney General [50 U.S.C. § 1805(a)(2)];

3. On the basis of the facts submitted by the applicant, there is probable cause to believe that [50 U.S.C. § 1805(a)(3)];



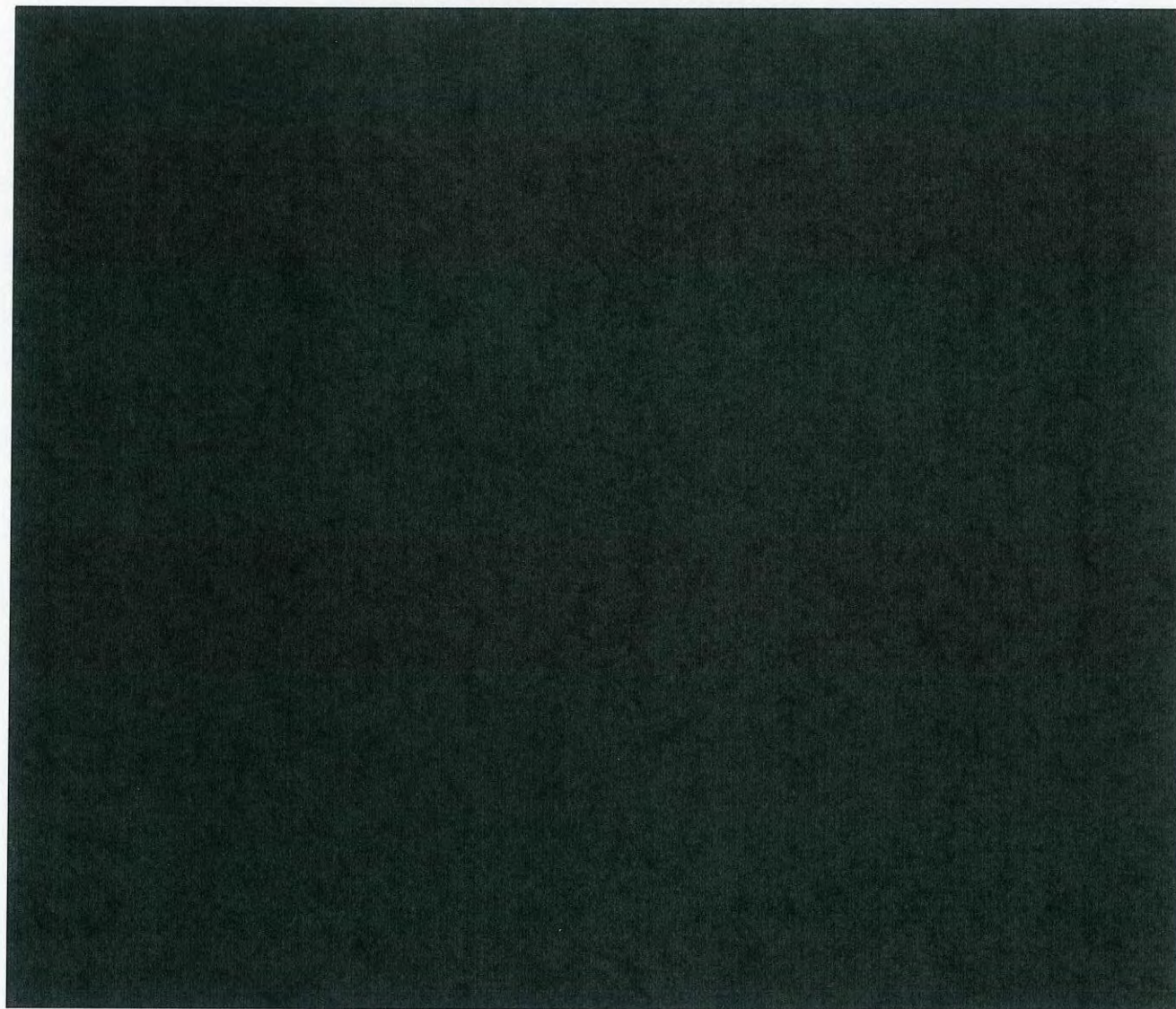
~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~



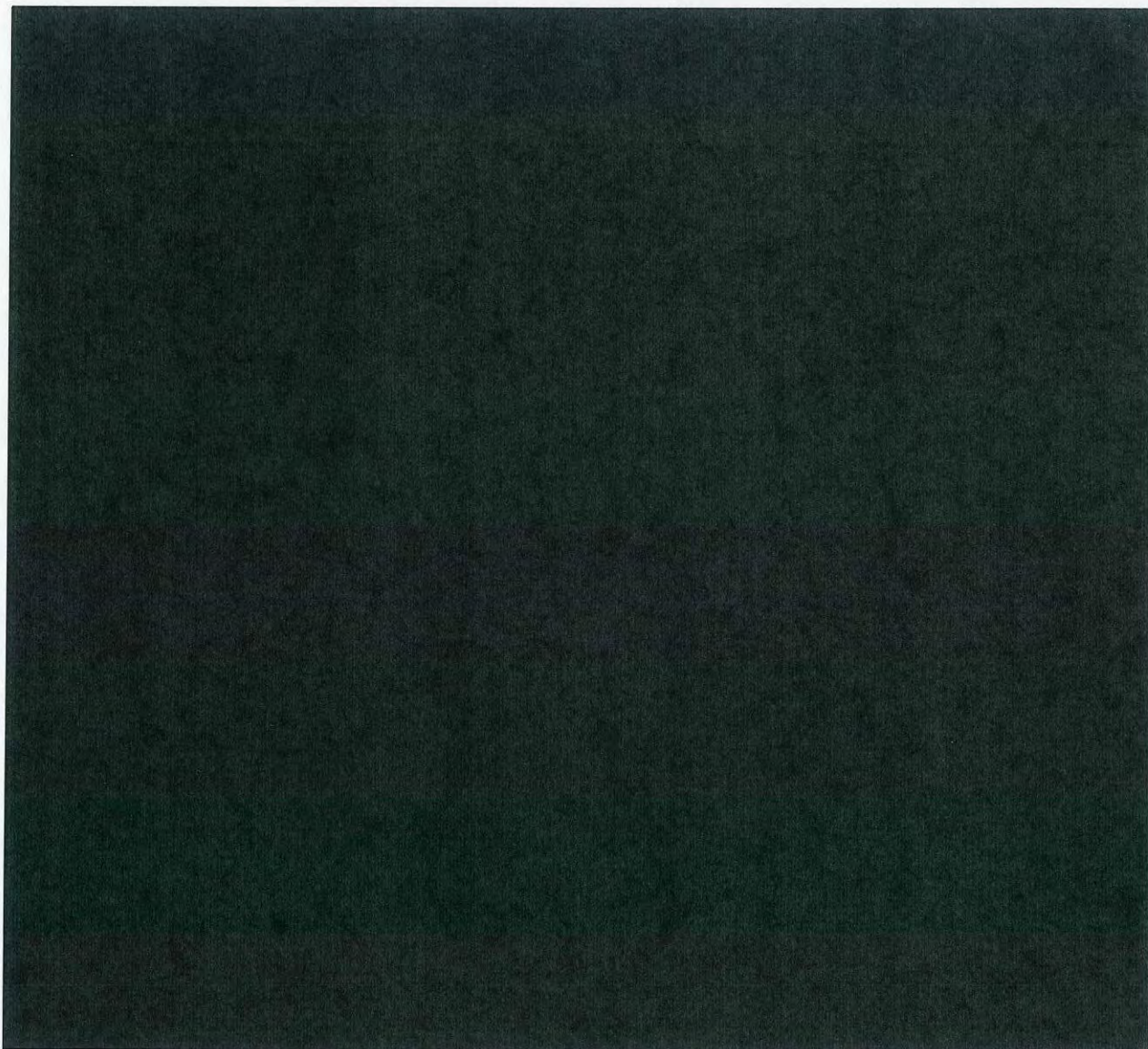
~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~



2



~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

(c) each of the facilities identified in Attachments A and B to Exhibit B in the revised and supplemented application, filed on May 24, 2007, and in Attachments A and B to the Supplemental Declaration of General Alexander, filed on May 30, 2007, but excluding the facilities identified in the Notice of Withdrawal filed on May 31, 2007, at which the electronic surveillance is directed, is being used or is about to be used by these foreign powers, and electronic surveillance is authorized, using for each particular facility only such means as are identified in paragraph II. below [50 U.S.C. § 1805(a)(3)(B)];

4. The minimization procedures proposed in the application have been adopted by the Attorney General and, as modified herein, meet the definition of minimization procedures under 50 U.S.C. § 1801(h). [50 U.S.C. § 1805(a)(4)]; and

5. The application contains all statements and certifications required by 50 U.S.C. § 1804, and the certification is not clearly erroneous on the basis of the statements made under 50 U.S.C. § 1804(a)(7)(E), and any other information furnished under 50 U.S.C. § 1804(d). [50 U.S.C. § 1805(a)(5)].





~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

WHEREFORE, IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application of the United States to conduct electronic surveillance, as described in the application, is GRANTED, and it is FURTHER ORDERED, as follows [50 U.S.C. § 1805(c)-(e)]:

I. The United States is authorized to conduct electronic surveillance to acquire foreign intelligence information as defined by 50 U.S.C. § 1801(e)(1)(A) and (B), including the incidental acquisition of other foreign intelligence information as defined by 50 U.S.C. § 1801(e)(1)(C) and (2) at the facilities described below, subject to the minimization procedures specified in paragraph 4 above and specifically detailed in paragraph IV below, for a period of ninety days, unless otherwise ordered by the Court.

(a). The facilities described in paragraph 3(c) above.

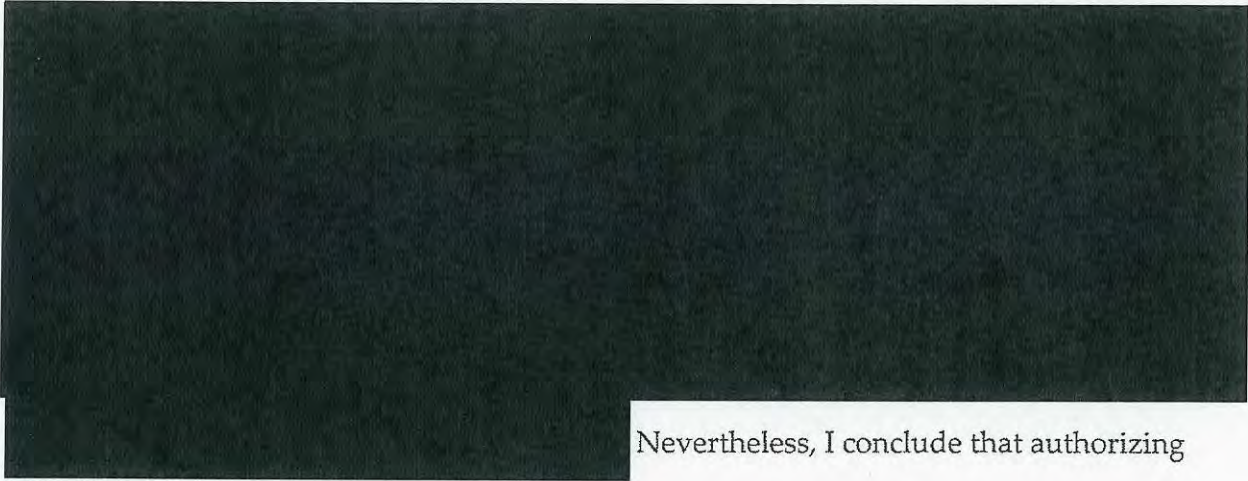
(b). It is well established that the targeted foreign powers pose a grave terrorist threat to the United States. ^{(b)(6); (b)(7)(C)} Declaration, at 10-12, 61-64. The evidence further establishes that the members and agents of the targeted foreign powers engage in a variety of activities in order to thwart or counter surveillance, 



Id., at 89, 94-98.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

While the provisions of 50 U.S.C. § 1805 are in tension with one another,³ it appears that the intent of Congress, when amending these provisions in 2001 and 2006, was to authorize multipoint or “roving” surveillance of a target that is actively avoiding surveillance, and to provide judicial oversight of such surveillance through the notice requirement in 50 U.S.C. § 1805(c)(3).⁴ This Court’s practice has generally been to



Nevertheless, I conclude that authorizing

³ On the one hand, 50 U.S.C. § 1805(a)(3)(B) requires that the judge find probable cause to believe that each of the facilities at which surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. On the other hand, 50 U.S.C. § 1805(c)(1)(B) clearly envisions cases in which the Court’s order would authorize electronic surveillance of facilities, under circumstances where the nature and location of the facilities were unknown at the time the application was approved. Similarly, the notice requirement in 50 U.S.C. § 1805(c)(3) indicates that an order can, consistent with 50 U.S.C. § 1805(c)(1)(B), authorize electronic surveillance of “any new facility or place,” and suggests that the order can authorize the government to determine whether “each new facility or place” is being used, or is about to be used, by the target of surveillance, subject to prompt notice to, and review by, this Court.

⁴ The legislative history for the USA PATRIOT Act’s amendment to § 1805(c)(2)(B) states that the new language was “included... to modify [FISA] to allow surveillance to follow a person who uses multiple communications devices or locations, a modification which conforms FISA to the parallel criminal procedures for electronic surveillance in 18 U.S.C. § 2518(1)(b).” 147 Cong. Rec. S11006 (Daily ed. Oct. 25, 2001)(section-by-section analysis of Sen. Leahy). The subsequent addition of “if known” to § 1805(c)(1)(B) was intended “to avoid any uncertainty about the kind of specification required in a multipoint wiretap case, where the facility to be monitored is typically not known in advance.” H.R. Conf. Rep. No. 107-328, at 24 (2001). The notice requirements set forth in § 1805(c)(3) were added in 2006 by section 108(b)(4) of the USA PATRIOT Improvement and Reauthorization Act, Pub. L. No. 109-177, to add “an extra layer of judicial review and to ensure that intelligence investigators will not abuse the multipoint authority.” Conf. Rep. H.R. 3199, reprinted in Cong. Rec. at H11303.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

such surveillance in this case is consistent with the provisions of 50 U.S.C. § 1805, as well as the intent of Congress, and is particularly appropriate where, as is the case here, the national security interests of the Government are great, and the impact of the surveillance on the Constitutional rights of United States persons is, or can be, minimized.

Therefore, in accordance with 50 U.S.C. § 1805(c)(1)(B) and § 1805(c)(3), the United States is authorized to conduct electronic surveillance of any other telephone numbers or e-mail [REDACTED] the nature and location of which are not specified herein because they were unknown to the NSA as of May 24, 2007 (the date the application was filed), where there is probable cause to believe that each additional telephone number or e-mail [REDACTED] is being used, or is about to be used, [REDACTED]

[REDACTED] This authority shall be limited to the surveillance of telephone numbers and e-mail [REDACTED] which the NSA reasonably believes are being used, or about to be used, by persons outside the United States and shall not include the surveillance of telephone numbers and e-mail [REDACTED] that the

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

NSA reasonably believes are being used, or about to be used, by United States persons, as defined in 50 U.S.C. § 1801(i).

(c). In this case, the Government has also asked for specific authority to acquire certain electronic communications that relate to or refer to an e-mail

[REDACTED] that is targeted for surveillance under this Order. For example, the Government argues that it should be allowed to acquire any e-mail communication that mentions a targeted e-mail [REDACTED] even though the communication is to and from other e-mail [REDACTED] not currently under electronic surveillance.⁵ After careful consideration of the Government's arguments, the Court holds that, in the limited and carefully considered circumstances described below, there is probable cause to believe that internet communications relating to a previously targeted e-mail [REDACTED] are themselves being sent and/or received by one of the targeted foreign powers, and thus those communications may be acquired by the NSA. At the same time, any e-mail facilities that were involved in sending or receiving such communications may not be further targeted absent a further examination by the NSA of the evidence supporting probable cause that involves, among other things, looking at the actual content of the

⁵ The Government identifies these as "abouts" or "referred to" communications. "For example, if an unknown [REDACTED] Memorandum of Law at 4.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

original intercepted communication which refers to the previously targeted e-mail

[REDACTED] This holding, albeit novel, is consistent with the overall statutory requirements; it requires the Government to promptly report and provide appropriate justification to the Court; and it supplies the Government with a necessary degree of agility and flexibility in tracking the targeted foreign powers. This Court will be able to ultimately determine whether the electronic surveillance was proper.

Therefore, in accordance with 50 U.S.C. § 1805(c)(1)(B) and § 1805(c)(3), the United States is further authorized to conduct electronic surveillance, as follows:

(i) by acquiring internet communications that contain a reference to an e-mail

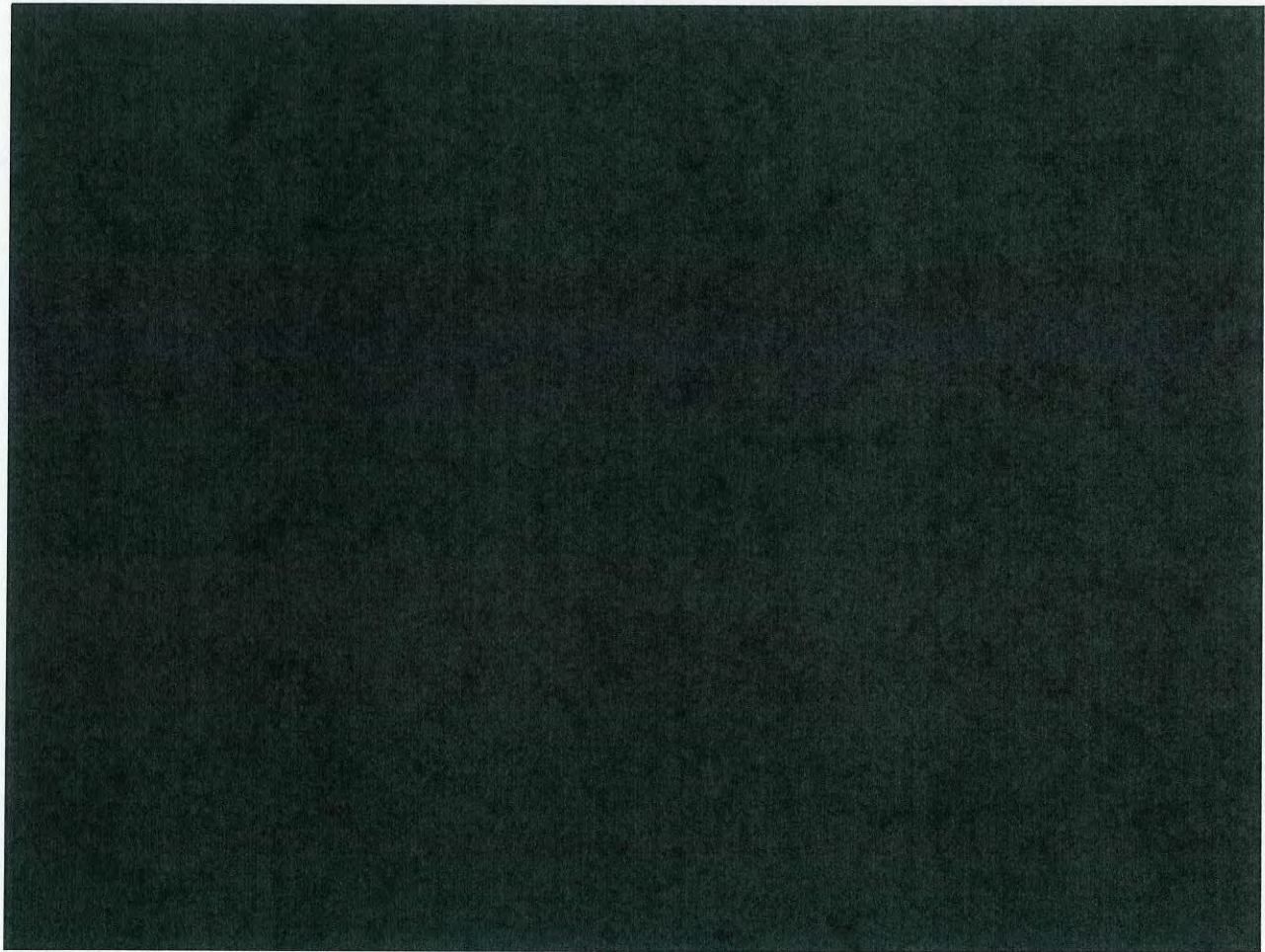
[REDACTED] that is subject to electronic surveillance under this Order at the time of acquisition (targeted [REDACTED]), under one of the following circumstances:

⁶ For example, if the user of targeted [REDACTED]

[REDACTED] account under this authority. The government's application does not ask separately for authority to initiate electronic surveillance under these circumstances, Memorandum of Law, at 2, apparently on the theory that [REDACTED] is actually electronic surveillance directed at the already targeted [REDACTED]. However, I conclude that electronic surveillance is directed at the newly identified facility in cases where that facility is separate and distinct from the already targeted [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~



[REDACTED] Therefore, separate authority is required to direct this form of electronic surveillance at a new facility, i.e., a separate [REDACTED] and I grant such authority here.

⁷ For purposes of this Order, [REDACTED]

⁸ For example, if the user [REDACTED]

[REDACTED] See Memorandum of Law, at 3. The government's application does not ask separately for authority to initiate electronic surveillance of [REDACTED] under these circumstances. *Id.*, at 2. However, for the same reasons discussed in footnote 6, it seems to me that separate authority is required to initiate electronic surveillance of a separate facility, [REDACTED] and I grant such authority here.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

I conclude and find that in each of the circumstances described [REDACTED]

[REDACTED] above, there is probable cause to believe that the facility at which electronic surveillance is directed is being used, or is about to be used, by [REDACTED]

[REDACTED] and

(ii) by targeting for collection by means of internet communications surveillance, as defined in paragraph II. below, an e-mail [REDACTED] a communication of which has been acquired pursuant to clause (i) above, only when all of the following requirements are satisfied:

(A). the NSA determines, on the basis of the contents of the acquired communication, and other reliable intelligence or publicly available information, there is still probable cause to believe that the e-mail [REDACTED] is being used, or is about to be used, by one of the targeted foreign powers;

(B). the NSA reasonably believes that the e-mail [REDACTED] is being used, or is about to be used, by persons outside the United States; and

(C). the NSA does not have reason to believe that the e-mail [REDACTED] is being used, or is about to be used, by a United States person, as defined in 50 U.S.C. § 1801(i).

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

For each new facility at which the Government directs electronic surveillance under sub-paragraphs (b) or (c)(ii) above, the Government shall provide notice to the Court in accordance with 50 U.S.C. § 1805(c)(3) within twenty-one days after the date on which such surveillance begins and in accordance with the following reporting schedule. The first such report shall be filed on Wednesday, June 13, 2007; this first report shall provide notice of newly discovered telephone numbers and e-mail [REDACTED] for which the Government initiated electronic surveillance from May 24, 2007 (i.e., the date on which this application was filed) through June 2, 2007. Subsequent reports shall be filed on a weekly basis each Wednesday (or on Tuesday if Wednesday is a national holiday), and will cover surveillance initiated during an earlier one-week period. For example, on June 20, 2007, the Government shall provide a report on surveillance initiated from June 3, 2007, through June 10, 2007; on June 27, 2007, the Government shall provide a report on surveillance initiated from June 11, 2007, through June 18, 2007; and so on. Such notice shall include:

- (A) the nature and location of each new facility or place at which electronic surveillance is directed;
- (B) the facts and circumstances relied upon by the United States to justify its belief that the new facility or place at which the electronic surveillance is directed

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

is or was being used, or is about to be used, by a target of surveillance (for surveillance conducted pursuant to paragraph I(c)(ii), the notice shall include the facts and circumstances relied upon by the United States to justify its continued surveillance of that facility);

(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and

(D) the total number of electronic surveillances that have been or are being conducted under the authority of this Order.

In accordance with 50 U.S.C. § 1805(c)(3), I find that the Government has established good cause to justify the twenty-one day period described above.

In addition, for each new facility at which the Government directs electronic surveillance under sub-paragraph (c)(i) above, the Government shall provide notice to the Court in accordance with 50 U.S.C. § 1805(c)(3) within sixty days after the date on which such surveillance begins and in accordance with the following reporting schedule. The first such report shall be filed on Wednesday, July 30, 2007; this first report shall provide notice of each new facility for which the Government initiated electronic surveillance from May 31, 2007 (i.e., the date of this Order) through July 15, 2007. The second report shall be filed fifteen days after the expiration of this Order, and shall provide notice of each new facility for which the Government initiated electronic

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

surveillance from July 16, 2007 through the expiration of the authorized surveillance.

Such notice shall include:

- (A) the nature and location of each new facility or place at which electronic surveillance is directed;
- (B) the facts and circumstances relied upon by the United States to justify its belief that the new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by a target of surveillance;
- (C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and
- (D) the total number of electronic surveillances that have been or are being conducted under the authority of this Order.

In accordance with 50 U.S.C. § 1805(c)(3), I find that the Government has established good cause to justify the sixty day period described above.

The Court may order the Government to immediately cease electronic surveillance of any facility as to which it deems the facts and circumstances relied upon by the Government to be inadequate.

In addition, the Government shall continue to file emergency FISA applications pursuant to 50 U.S.C. § 1805(f)(or alternatively, a motion to amend) if it seeks authority to conduct electronic surveillance, as described herein, of additional telephone numbers and e-mail [REDACTED] that the Government believes are being used,

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

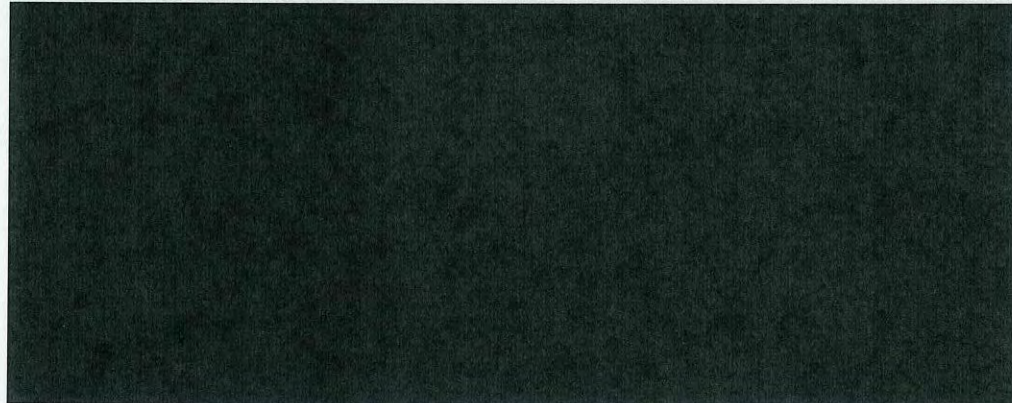
or are about to be used, by one of the targeted foreign powers and which are reasonably believed to be used by persons located outside the United States who are United States persons as defined in 50 U.S.C. § 1801(i). The Government has proposed a streamlined FISA emergency application form, attached as Exhibit G to the application, specifically for this purpose. I find that for any such application made under the above-captioned docket number the form of this proposed application is consistent with FISA.

I also hereby find that the Government has established "good cause" within the meaning of 50 U.S.C. § 1806(j) that a subject of emergency surveillance initiated by the Government during the period of this Order, but not authorized by this Court, should not be notified of the emergency employment of electronic surveillance. For any such surveillance, the requirement of notice shall be suspended for ninety days following the emergency employment of electronic surveillance, provided that on a further ex parte showing of good cause by the Government, the Court shall forego ordering the serving of the notice required under section 50 U.S.C. § 1806(j).

II. The means by which this electronic surveillance shall be effected are as follows:

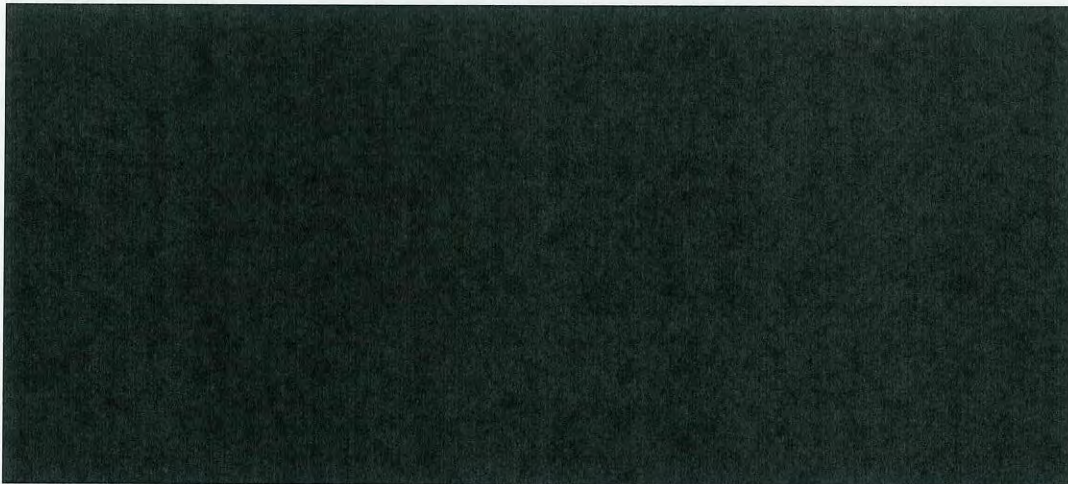
~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~

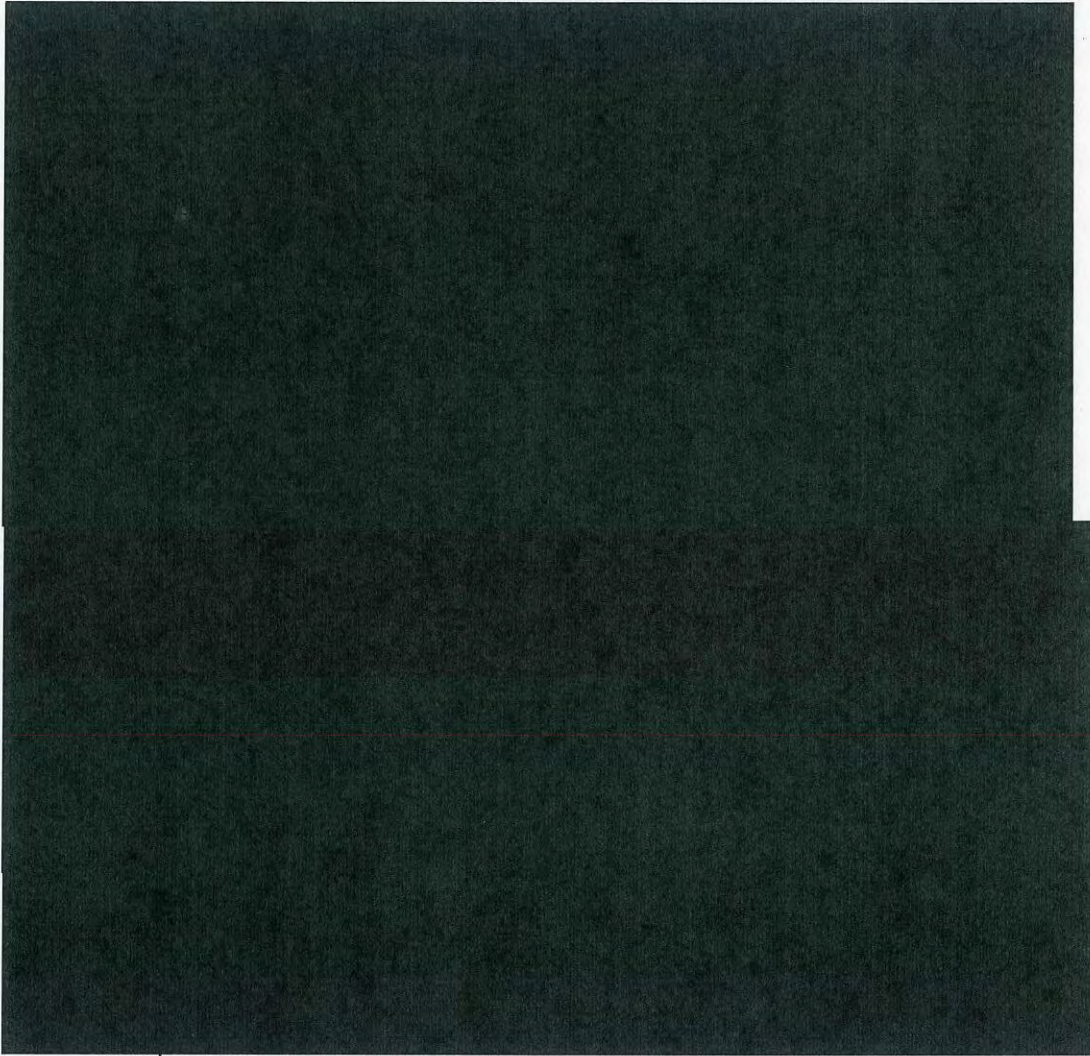
~~TOP SECRET//COMINT//NOFORN~~



¹¹ This Order is based on the principle that the NSA surveillance will be designed to acquire only international communications where a communicant is located outside the United States, but the Court understands that the communications infrastructure and the manner in which it routes communications do not permit complete assurance that no domestic communications will be acquired. In such cases, NSA shall apply its standard FISA minimization procedures, as described and modified herein, to any domestic communications it may inadvertently acquire.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~



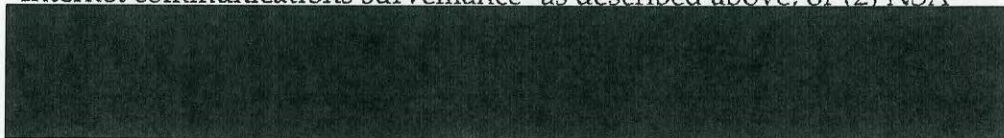
§1801(f)(4) surveillance. This surveillance will be effected by using either, or both, of two techniques, as follows: (1) The first technique constitutes



TOP SECRET//COMINT//NOFORN

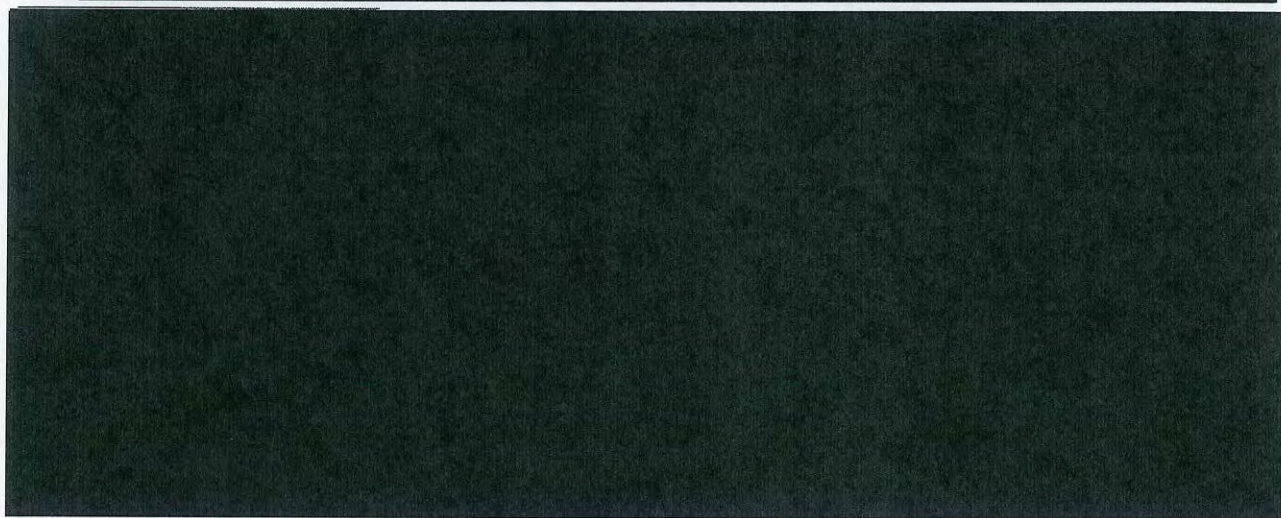
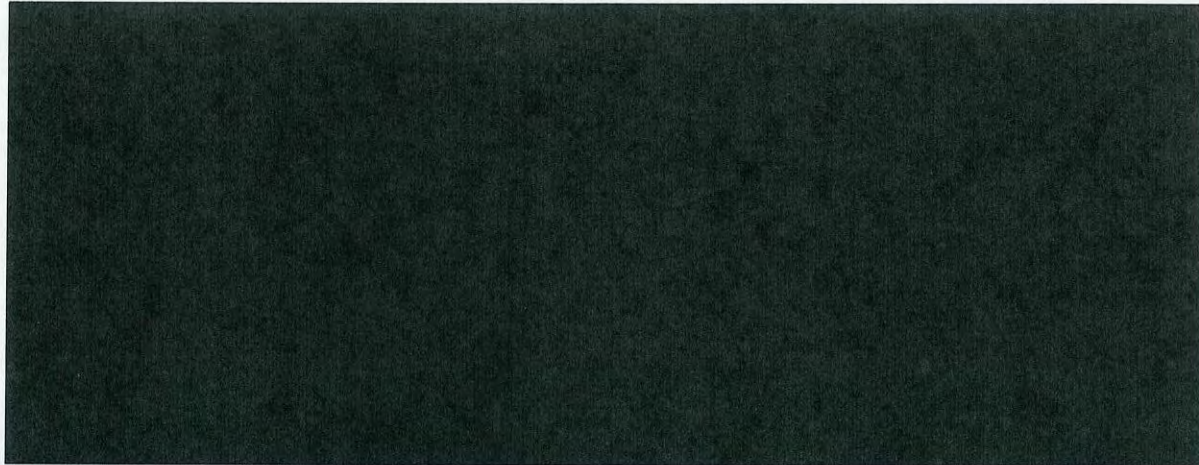
~~TOP SECRET//COMINT//NOFORN~~

"Internet communications surveillance" as described above; or (2) NSA



Unconsented physical entry is not authorized to implement the electronic surveillance approved herein.

III. The person(s) specified in the secondary orders attached hereto, specifically:



~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

including all assigns and/or other successors in interest to said specified persons with regard to the facilities and/or places targeted herein, shall:

(a) furnish the United States all information, facilities, or technical assistance necessary to effect the authorities granted herein in accordance with the orders of this Court directed to said specified person; and

(b) maintain all records concerning this matter, or the aid furnished to the United States, under the security procedures approved by the Attorney General and the Director of Central Intelligence (or the Director of National Intelligence) that have previously been or will be furnished to the specified persons and are on file with this Court,

and the United States shall compensate any such person(s) providing assistance at the prevailing rate for all assistance furnished in connection with the activities described herein [50 U.S.C. § 1805(c)(2)(B)-(D)].

IV. As to all information gathered through the authorities requested herein, the NSA shall follow:

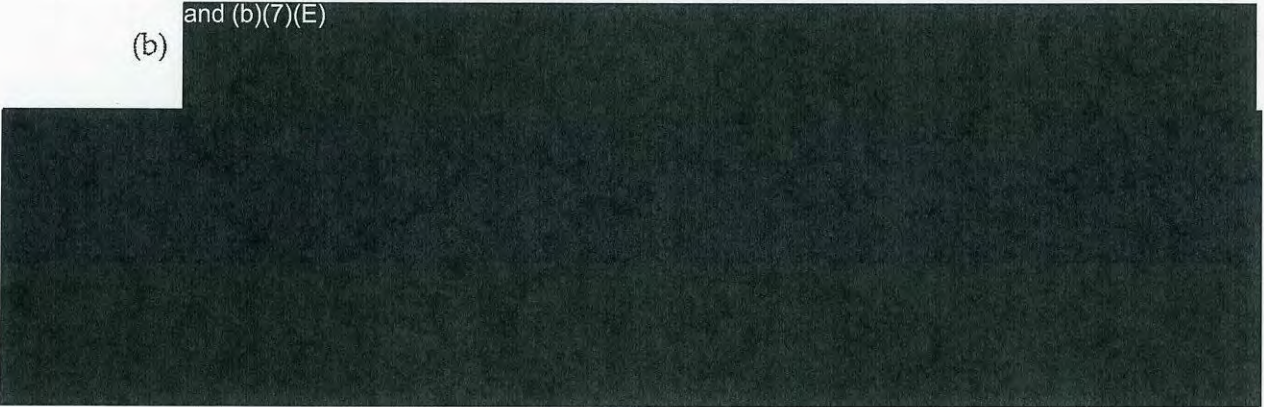
(a) The Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency (also known as Annex A to United States

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with this Court;

(b) and (b)(7)(E)



1. The following shall be added to the end of Section 3(f) of these standard NSA FISA procedures:

(7) The National Security Division of the Department of Justice shall periodically determine that information concerning communications of or concerning United States persons that is retained meets the requirements of these procedures and the Foreign Intelligence Surveillance Act.

2. The following shall be added to the end of Section 4(b) of these standard NSA FISA procedures:

With respect to any other communication where it is apparent to NSA processing personnel that the communication is between a person and the person's attorney (or someone acting on behalf of the attorney) concerning legal advice being sought by the former from the latter, such communications relating to foreign intelligence information may be retained and disseminated within the U.S. Intelligence Community if the communications are specifically labeled as being privileged. However, such communications may not be disseminated outside of

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

the U.S. Intelligence Community without the prior approval of the Assistant Attorney General for the National Security Division or his designee.

3. The following shall replace subsections (a), (b), and (c) of Section 8 of these standard NSA FISA procedures:

NSA may disseminate nonpublicly-available identity or personally identifiable information concerning United States persons to foreign governments provided that such information is foreign intelligence information and either (i) the Attorney General approves the dissemination; or (ii) NSA disseminates the information under procedures approved by the Attorney General. In addition, NSA may disseminate such foreign intelligence information, to the extent authorized by the Director of National Intelligence (DNI) and in accordance with DNI directives, subject to the following procedures:¹⁴

(1) Disseminations to [REDACTED]

[REDACTED] may be made upon the approval of any person designated for such purpose by the Director of NSA.

(2) Disseminations to [REDACTED] foreign governments may be made upon the approval of the NSA's Office of General Counsel, upon consideration of the following factors: the national security benefit the United States may reasonably expect to obtain from making the dissemination; the anticipated uses to which the foreign government will put the information; and any potential for economic injury, physical harm, or other restriction of movement to be reasonably expected from providing the information to the foreign government. If the proposed recipient(s) of the dissemination have a history of human rights abuses, that history should be considered in assessing the potential for economic injury, physical harm, or other restriction of movement, and whether the

14

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

dissemination should be made. In cases where there is a reasonable basis to anticipate that the dissemination will result in economic injury, physical harm, or other restriction of movement: (i) the approval of the NSA's Signals Intelligence Director will also be required; and (ii) if dissemination is approved, NSA will undertake reasonable steps to ensure that the disseminated information will be used in manner consistent with United States law, including Executive Order No. 12333 and applicable federal criminal statutes.

(3) NSA will make a written record of each dissemination approved pursuant to these procedures, and information regarding such disseminations and approvals shall be made available for review by the National Security Division, United States Department of Justice, on at least an annual basis.

4. Regarding dissemination of evidence of a crime, Sections 5(a)(2) and 6(b)(8) of these standard NSA FISA procedures shall be superseded by the following:

Information that is not foreign intelligence information, but reasonably appears to be evidence of a crime that has been, is being, or is about to be committed, may be disseminated (including United States person identities) to the FBI and other appropriate federal law enforcement authorities, in accordance with 50 U.S.C. § 1806(b), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 'Memorandum of Understanding: Reporting of Information Concerning Federal Crimes,' or any successor document.

5. The following shall be added to end of Section 6 of these standard NSA FISA procedures:

NSA may disseminate all communications acquired to the CIA, which shall process any such communications in accordance with minimization procedures approved by this Court.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

(c) The following additional modifications to the standard NSA FISA minimization procedures for electronic surveillance:

1. Notwithstanding sections 3(c)(2) and (e), 5(b), and 6(a) of the standard NSA FISA procedures, communications acquired under this Order may be retained for five years, unless this Court approves retention for a longer period. The communications that may be retained under this Order include electronic communications acquired because of limitations on NSA's ability to filter communications, as described in Exhibit B to the application.

2. Section 3(c)(6) of these standard NSA FISA minimization procedures is deleted and replaced with:

To the extent reasonably possible, NSA personnel with access to the data acquired pursuant to this authority shall query the data in a manner designed to minimize the review of communications of or concerning U.S. persons that do not contain foreign intelligence information or evidence of a crime.

3. Section 3(g)(1) of these standard NSA FISA minimization procedures, relating to absences "from premises under surveillance" by agents of a foreign power, shall not apply to this surveillance.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

V. The CIA shall minimize all communications received under this order as provided in Exhibit E to the application.

Signed 05-31-2007 10:15A Eastern Time
Date Time

This authorization regarding [REDACTED]

[REDACTED] expires at 5:00 p.m.

on the 24th day of August, 2007.



ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//COMINT//NOFORN~~

29

(b)(6); (b)(7)(C)

Deputy Cler.

FISC, certify that this document
is a true and correct copy of
the original (b)(6); (b)(7)(C)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE [REDACTED] :

[REDACTED] : Docket No.: (b)(7)(E)

:

:

ORDER AND MEMORANDUM OPINION

This case involves an extremely important issue regarding probable cause findings that determine what persons and what communications may be subjected to electronic surveillance pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA"), 50 U.S.C. §§ 1801-1811: Are they required to be made by a judge of this Court, through procedures specified by statute for the issuance of a FISA order under 50 U.S.C. § 1805? Or may the National Security Agency (NSA) make these probable cause findings itself, as requested in the application in this case, under an alternative mechanism adopted as "minimization procedures"?¹

I. INTRODUCTION

When the government believes that a telephone number or e-mail address is being used in furtherance of international terrorism, it will appropriately want to acquire communications relating to that number or e-mail address. Under FISA, the government may obtain an electronic surveillance order from this Court, upon a judge's finding, *inter alia*, of probable cause to believe that the telephone number or e-mail address is used by a foreign power (to include an international terrorist group) or an agent of a foreign power. § 1805(a)(3)(B). In an emergency, the government may begin the electronic surveillance before obtaining the Court order, upon the approval of the Attorney General and provided that a Court order, supported by such a judicial probable cause finding, is obtained within 72 hours thereafter. § 1805(f).

Until recently, these were the only circumstances in which the government had sought, or this Court had entered, a FISA order authorizing electronic surveillance of the telephone or e-

¹ This order and opinion rests on an assumption, rather than a holding, that the surveillance at issue is "electronic surveillance" as defined at 50 U.S.C. § 1801(f), and that the application is within the jurisdiction of this Court. See note 12 *infra*.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

mail communications of suspected international terrorists. However, on December 13, 2006, in Docket No. (b)(7)(E), the government filed an application seeking an order that would authorize electronic surveillance of telephone numbers and e-mail addresses thought to be used by international terrorists without a judge's making the probable cause findings described above, either before initiation of surveillance or within the 72 hours specified in § 1805(f). The proposed electronic surveillance targeted [REDACTED] and involved acquisition by NSA of international telephone and Internet communications [REDACTED].

That application was presented to another judge of this Court. After considering the application and supporting materials, that judge orally advised the government that he would not authorize, on the terms proposed in the application, electronic surveillance of "selector" phone numbers and e-mail addresses, as described below, believed to be used by persons in the United States. The government then filed a second application regarding surveillance of the previously identified phone numbers used by persons in the United States on January 9, 2007, in Docket No. (b)(7)(E).

On January 10, 2007, the judge entered orders in Docket No. (b)(7)(E) that granted the requested electronic surveillance authority, subject to a number of modifications, and specifically limiting the authorized surveillance to "selector" phone numbers and e-mail addresses believed to be used by persons outside the United States. Primary Order at 12. On the same date, the judge also entered orders granting the surveillance authority requested by the application in Docket No. (b)(7)(E) for the identified phone numbers believed to be used by persons in the United States.

The authorization in Docket No. (b)(7)(E) comported with the long-established probable cause determination described above, but the authorization in Docket No. (b)(7)(E) did not. The Primary Order in Docket No. (b)(7)(E) identified [REDACTED] phone numbers as the facilities at which the electronic surveillance is directed and, pursuant to § 1805(a)(3)(B), found probable cause to believe that each phone number was being used or about to be used by an agent of a foreign power. Primary Order at 4-5. This finding rested on specific facts provided in the application regarding the use of each phone number.²

² Declaration of (b)(3), (b)(6), (b)(7)(C) NSA, at 4-59 (Exhibit A to application in Docket No. [REDACTED]). In subsequent supplemental orders, the judge authorized additional phone numbers for surveillance in Docket No. [REDACTED] based on the same kind of judicial probable cause findings, for a total of [REDACTED] telephone numbers covered in Docket No. [REDACTED]. See, e.g., Amendment to Order at (continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

On the other hand, the Primary Order in Docket No. [REDACTED] did not identify, or make probable cause findings regarding, [REDACTED] phone numbers and e-mail addresses subject to surveillance under that order. Instead, that order identified [REDACTED] which the authorized electronic surveillance is directed and found probable cause to believe that [REDACTED] was being or about to be used by the targeted terrorist organizations. Docket No. [REDACTED] Primary Order at 2-5.

On March 21, 2007, the government filed the application in this case, Docket No. [REDACTED] seeking renewal of the surveillance authority granted in Docket No. [REDACTED].³ This application follows Docket No. [REDACTED] in identifying [REDACTED] which the electronic surveillance is directed for purposes of the judge's probable cause findings under § 1805(a)(3)(B).⁴

II. THE SURVEILLANCE AT ISSUE

For surveillance of international telephone communications, [REDACTED] identified in the application. Alexander Decl. at 16. The devices acquire only communications to or from the telephone numbers entered as "selectors." Alexander Decl. at 16, 20-21.

²(...continued).

2 (entered Jan. 16, 2007); Primary Order in Docket No. [REDACTED] at 2 (entered Jan. 22, 2007); Primary Order in Docket No. [REDACTED] at 2 (entered Feb. 2, 2007).

³ On March 22, 2007, in Docket No. [REDACTED], the government filed an application for renewal of the authority granted in Docket No. [REDACTED]. The renewal application identifies [REDACTED] U.S. phone numbers as the facilities at which the surveillance is directed, and requests that the Court find probable cause to believe that each of these phone numbers is being used or is about to be used by an agent of a foreign power, based on specific information set out in the application regarding the use of each number. Docket [REDACTED], proposed Order at 2-5, Declaration of [REDACTED] NSA, at 6-64 (submitted as Exhibit A to Application).

⁴ Docket No. [REDACTED], Application at 4-5; Declaration of Lt. Gen. Keith B. Alexander, Director, NSA, at 26-42 (submitted as Exhibit C to Application) (hereinafter "Alexander Decl."); proposed Order at 6.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

For Internet communications, NSA uses e-mail addresses as selectors.⁵ [REDACTED]

[REDACTED] Id. at 34-42. [REDACTED] acquire only communications that are to or from, or that contain a reference to,⁶ a selector e-mail address. Id. at 14-15, 21-23.

NSA uses telephone numbers or e-mail addresses as selectors only if "it reasonably believes [they] are being used or are about to be used by persons located overseas and . . . has determined there is probable cause to believe [they] are being used or about to be used by a member or agent of [REDACTED]"

[REDACTED] Id. at 43. The government submits that applying this standard for selectors "narrowly focus[es] NSA's collection efforts on communications" of the targeted terrorist groups, id. at 15. [REDACTED]

[REDACTED] Id. at 14. [REDACTED] overseas e-mail addresses and phone numbers have been adopted as selectors under this standard pursuant to the order in Docket No. [REDACTED] (b)(7)(E). Id. at 19.

In most relevant respects, the means of electronic surveillance at issue in this case are quite similar to how [REDACTED] FISA surveillance orders have been implemented. The means of conducting the phone surveillance is, for all relevant purposes, indistinguishable from many prior cases in which communications to or from particular phone numbers are acquired by use of [REDACTED]

[REDACTED] The e-mail surveillance is also quite similar to what has been [REDACTED]

⁵ [REDACTED]

⁶ This surveillance acquires an Internet communication containing a reference to a selector e-mail address [REDACTED]

[REDACTED] Id. at 22 n.34.

⁷ [REDACTED]

(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

authorized previously, to the extent that it acquires communications to or from selector e-mail addresses.⁸ The acquisition of e-mail communications because they refer to a selector e-mail

⁷(...continued)

[REDACTED]

In addition, the standard description of ^{b(1), b(7)(E)} ^{b(1), b(7)(E)} conducted by the FBI states that such surveillance and b(6) and b(7)(C)

[REDACTED]

⁸

[REDACTED]

and b(6), b(7)(C) and (E)

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//XI~~

address does not appear to have been authorized under FISA prior to Docket No. [REDACTED] and is discussed further below.

III. PROBABLE CAUSE FINDINGS

Under FISA, a judge of this Court may enter an electronic surveillance order only upon finding, inter alia, that

on the basis of the facts submitted by the applicant there is probable cause to believe that --

(A) the target⁹ of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.

§ 1805(a)(3) (emphasis added). FISA defines "foreign power," in relevant part, as including "a group engaged in international terrorism or activities in preparation therefor." § 1801(a)(4).

In this case, the government contends that, for purposes of § 1805(a)(3)(B) the "facilities" at which the electronic surveillance is directed are [REDACTED] E.g., Alexander Decl. at 13; Government's Memorandum of Law at 32 (attached to Application as part of Exhibit A). The government acknowledges that the telephone numbers and e-mail addresses selected for

and b(6), b(7)
(C) and (E)

[REDACTED]

⁹ The target of a surveillance "'is the individual or entity . . . about whom or from whom information is sought.'" In re Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (quoting H.R. Rep. 95-1283, pt. 1 at 73 (1978)).

~~TOP SECRET//COMINT//ORCON,NOFORN//XI~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

acquisition are [REDACTED] "facilities" [Government's Memorandum of Law at 31 n.18] [REDACTED] Simultaneously, however, the government maintains in another case that [REDACTED] resulting in an entirely different focus for the judge's assessment of probable cause under § 1805(a)(3)(B).¹⁰ Underlying the government's position, therefore, is the premise that § 1805(a)(3)(B) can be applied so variously that a FISA judge has great discretion in determining what "facilities" should be the subject of the judge's probable cause analysis.

In deciding how to apply § 1805(a)(3)(B), the Court looks first to the language of the statute. See, e.g., Engine Manufacturers Ass'n v. South Coast Air Quality Mgmt. Dist., 541 U.S. 246, 252 (2004). That statutory language specifies that a probable cause finding must be made for each facility "at which the electronic surveillance is directed." The statute provides four alternative definitions of electronic surveillance, but the one most pertinent to this case is at § 1801(f)(2).¹¹ Section 1801(f)(2) defines "electronic surveillance" as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition

¹⁰ For example, the manner of phone surveillance [REDACTED] proposed in this docket is identical to that proposed in Docket No. [REDACTED] for phone numbers used in the United States. Compare Docket No. [REDACTED] Declaration of Lt. Gen. Keith B. Alexander, Director, NSA at 3 (submitted as Attachment C to Application) (defining [REDACTED] with Alexander Decl. in this docket at 24-25 (same definition, but with references to [REDACTED] and to the "minimization probable cause standard"). [REDACTED] and b(7)(E)

[REDACTED] Proposed Order at 2-6.

¹¹ Section 1801(f)(2) provides the relevant definition of "electronic surveillance" for all of the proposed phone surveillance, as well as the proposed e-mail surveillance [REDACTED] Application at 19. In the government's view, the relevant definition for [REDACTED] See note 13 *infra* & accompanying text.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

occurs in the United States.” (Emphasis added.)¹² Thus, the electronic surveillance is the acquisition of the contents of communications.

In this case, communications will be acquired because they are to or from (or, in the case of Internet communications, refer to) a certain class of facilities - - - the telephone numbers and e-mail addresses used as selectors. NSA has no interest in acquiring the contents of [REDACTED]

Rather, it is interested in acquiring only [REDACTED] Accordingly, NSA [REDACTED] to select for acquisition communications that relate to a selector facility, and to exclude from acquisition [REDACTED]

¹² The record does not disclose to what extent the surveillance conducted under Docket No. [REDACTED] has in fact acquired communications to or from a person in the United States. See Alexander Decl. at 22 n.36 (the “volume of communications targeted for collection” in Docket No. [REDACTED] makes it “technically infeasible” to provide such information, but “a central purpose” of such surveillance “is to collect communications to or from terrorist operatives in the United States”). However, given the large number of selectors involved [REDACTED]

[REDACTED] it appears likely that this surveillance would acquire some indeterminate number of communications to or from persons in the United States. See, e.g., id. at 6-8 [REDACTED]

In view of this apparent likelihood, the government’s implicit request that the Court exercise jurisdiction over the submitted application, the Court’s prior acceptance of jurisdiction in Docket No. [REDACTED] and prior decisions of this Court that have accepted jurisdiction in similar cases [REDACTED]

[REDACTED] I assume for purposes of this order and opinion that this case does involve “electronic surveillance” as defined by FISA, such that this Court has jurisdiction. However, I believe that the jurisdictional issues regarding the application of FISA to phone numbers and e-mail addresses that are used exclusively outside the United States merit further examination. I further believe that Congress should also consider clarifying or modifying the scope of FISA and of this Court’s jurisdiction with regard to such facilities, given the large number of overseas e-mail addresses and phone numbers now identified by the government for surveillance, and the government’s assertions regarding the need for speed and agility in targeting such facilities as new ones are identified in the future. See pages 18-19 infra.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

[REDACTED] These facts strongly suggest that the acquisition of the contents of communications - - - that is, the electronic surveillance itself - - - is directed at the telephone numbers and e-mail addresses used as selectors.

In the government's view, a discrete part of the proposed e-mail surveillance, to be conducted [REDACTED] should be analyzed under the definition of "electronic surveillance" provided at § 1801(f)(4).¹³ Section 1801(f)(4) defines "electronic surveillance" to include "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication . . ." (Emphasis added.) A similar analysis applies under § 1801(f)(4): because the surveillance consists of monitoring to acquire information, and the only information to be acquired relates to the e-mail addresses used as selectors, the electronic surveillance would be directed at those e-mail addresses.

The government argues to the contrary that this surveillance is not [REDACTED]

[REDACTED] Government's Memorandum of Law at 32. But, nothing in the language of the statute identifies the facility at which the surveillance is directed [REDACTED] Congress could have used language that focused [REDACTED] but chose not to do so in § 1805(a)(3)(B). Compare § 1842(d)(2)(A)(iii) (requiring FISA pen register/trap and trace orders to specify, "if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied") (emphasis

¹³ The orders in Docket No. [REDACTED] b(7)(E) authorized surveillance [REDACTED] but NSA has not commenced such surveillance. NSA intends to do so within the next 90 days, but has not determined how such surveillance will be conducted, or even whether some part of its intended activity will involve [REDACTED] Alexander Decl. at 41 nn.49 & 52, 42 n.55.

¹⁴ Certainly the term "directed" cannot be construed to do so. See Webster's II New College Dictionary 321 (2001) (defining "direct" to mean, inter alia, "To move or guide (someone) toward a goal;" "To show or indicate the way to;" "To cause to move in or follow a direct or straight course <directed the arrow at the bull's-eye>," "To address (e.g., a letter) to a destination.")

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

added). And, the relevant provisions assign no significance to the place where communications are acquired, so long as acquisition "occurs in the United States" (as is the case here).¹⁵

The government further argues that one portion of the proposed surveillance - - - the acquisition of e-mails that contain a reference to, but are not to or from, a selector e-mail address - - - cannot be conducted [REDACTED]

[REDACTED] Government's Supplemental Memorandum of Law at 6-7 (submitted as part of Exhibit A to the Application).¹⁶ However, even for this part of the surveillance, communications [REDACTED]

[REDACTED] The surveillance functions in this way because NSA is not interested in the contents of communications [REDACTED]; rather, it is only interested in the contents of those communications (to include the e-mail addresses of the communicants) that refer to a selector e-mail address. For these reasons, I find that this aspect of the proposed surveillance is not [REDACTED], but rather at particular e-mail addresses.¹⁷

The government also cites several prior cases as precedent for the interpretation of § 1805(a)(3)(B) adopted in Docket No. [REDACTED] b(7)(E). These cases involved very different

¹⁵ § 1801(f)(2); see also § 1801(f)(4) ("installation or use of a[] . . . surveillance device in the United States . . .")

¹⁶ The government identifies [REDACTED] communications acquired by this aspect of the surveillance. Government's Supplemental Memorandum of Law at 6-7; Declaration of [REDACTED] b(3), b(6) and b(7) NSA ("[REDACTED] b(3) Decl.") at 16-18 (submitted as part of Exhibit A to the Application). [REDACTED] and b(6) and b(7) [REDACTED]

¹⁷ On the record before me, I cannot, and do not, decide exactly which particular e-mail addresses are the ones at which this type of surveillance is directed. To the extent it is concluded that surveillance is directed at e-mail addresses [REDACTED] a judge would have to find probable cause to believe that those e-mail addresses, [REDACTED] are being used or are about to be used by a foreign power or an agent of a foreign power before authorizing the surveillance proposed in the application.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

circumstances, such as surveillances that acquired

Tellingly, none

and b(6), b(7)(A), (C), and (E)

and b(6), b(7)(A), (C), and (E)

and b(6), b(7)(A), (C), and (E)

and b(6), b(7)(A), (C), and (E)

(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

of the cited cases stand for the proposition on which this application rests - - - that electronic surveillance is not "directed" at particular phone numbers and e-mail addresses. [REDACTED]

Moreover, in each of the cited cases involving surveillance under § 1805,²⁰ the judge made probable cause determinations that a single target or well-defined set of targets [REDACTED]

[REDACTED] These determinations constrained the ability of executive branch officials to direct surveillance against persons and communications of their unilateral choosing in a way that, as discussed below, the proposed probable cause findings in this case would not.

Therefore, I conclude that, under the plain meaning of §§ 1805(a)(3)(B) and 1801(f), the proposed electronic surveillance is directed at the telephone numbers and e-mail addresses used as selectors. The result of applying this plain meaning is by no means absurd.²¹ and b(7)(E) [REDACTED]

¹⁹(...continued)

and b(7)(E) [REDACTED]

²⁰ One case relied on by the government involved different statutory requirements and no probable cause finding at all. [REDACTED]

[REDACTED] Docket No. PR/TT ^{b(7)(E)} involved the use of pen registers and trap and trace devices to acquire addressing and routing information, not the full content of communications. Because issuing a FISA pen register/trap and trace order under § 1842 does not require the judge to make probable cause findings, the Opinion and Order entered on July 14, 2004, at 49 n.34, expressly disclaimed any application to full-content surveillances under § 1805.

²¹ See Laimie v. United States Trustee, 540 U.S. 526, 534 (2004) (court is to enforce plain language of a statute, "at least where the disposition required by the text is not absurd") (internal quotations omitted).

²² See notes 7 and 8 supra.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

and b(7)(E) [REDACTED] cases (other than
this case and Docket No. [REDACTED]) consistently reflect the same understanding [REDACTED]
[REDACTED]

However, even if the statutory language were as elastic as the government contends, it would still be incumbent on me to apply the language in the manner that furthers the intent of Congress. In determining what interpretation would best further congressional intent, it is appropriate to consult FISA's legislative history.²⁵ That legislative history makes clear that the

²³ See, e.g., In re [REDACTED] and b(6), b(7)(C), and (E)

and b(6), b(7)(C), and (E)

and b(6), b(7)(A), (C), and (E)

²⁵ See Train v. Colorado Public Interest Research Group, 426 U.S. 1, 10 (1976).
Moreover, if § 1805(a)(3)(B) could be applied in such widely varying ways to the same surveillance, then its terms would be sufficiently unclear that legislative history may be consulted
(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

purpose of pre-surveillance judicial review is to protect the fourth amendment rights of U.S. persons.²⁶ Congress intended the pre-surveillance "judicial warrant procedure," and particularly the judge's probable cause findings, to provide an "external check" on executive branch decisions to conduct surveillance.²⁷

Contrary to this intent of Congress, the probable cause inquiry proposed by the government could not possibly restrain executive branch decisions to direct surveillance at any particular individual, telephone number or e-mail address. Under § 1805(a)(3)(B), the government would have the Court assess [REDACTED]

[REDACTED] See Alexander Decl. at 6-8, 11-12], and make a highly abstract and generalized probable cause finding [REDACTED] However, such a probable cause finding could be made with equal validity [REDACTED]

²⁵(...continued)

to ascertain their proper meaning. See, e.g., Blum v. Stenson, 465 U.S. 886, 896 (1984).

²⁶ "A basic premise behind this bill is the presumption that whenever an electronic surveillance for foreign intelligence purposes may involve the fourth amendment rights of any U.S. person, approval for such a surveillance should come from a neutral and impartial magistrate." E.g., H. Rep. 95-1283, pt. 1, at 24-25; see also id. at 26 (purpose of extending warrant procedure to surveillances targeting non-U.S. persons "would not be primarily to protect such persons but rather to protect U.S. persons who may be involved with them"). Such protection was deemed necessary in view of prior abuses of national security wiretaps. Id. at 21 ("In the past several years, abuses of domestic national security surveillances have been disclosed. This evidence alone should demonstrate the inappropriateness of relying solely on executive branch discretion to safeguard civil liberties.").

²⁷

The bill provides external and internal checks on the executive. The external check is found in the judicial warrant procedure which requires the executive branch to secure a warrant before engaging in electronic surveillance for purposes of obtaining foreign intelligence information. . . . For such surveillance to be undertaken, a judicial warrant must be secured on the basis of a showing of "probable cause" that the target is a "foreign power" or an "agent of a foreign power." Thus the courts for the first time will ultimately rule on whether such foreign intelligence surveillance should occur.

S. Rep. 95-604, pt. 1, at 16, reprinted in 1978 U.S.C.C.A.N. 3904, 3917.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

[REDACTED] On this reading of § 1805(a)(3)(B), facts supporting or contradicting the government's belief that terrorists use the phone numbers and e-mail addresses for which information will be acquired are irrelevant to the judge's probable cause findings.²⁸

Thus, under the government's interpretation, the judge's probable cause findings have no bearing on the salient question: whether the communications to be acquired will relate to the targeted foreign powers.²⁹ As discussed below, the government would have all of the probable cause findings bearing on that question made by executive branch officials, subject to after-the-fact reporting to the Court, through processes characterized by the government as minimization. That result cannot be squared with the statutory purpose of providing a pre-surveillance "external check" on surveillance decisions, or with the expectation of Congress that the role of the FISA judge would be "the same as that of judges under existing law enforcement warrant procedures."³⁰

²⁸ The government argues that the Court has previously, and should here, apply the requirements of § 1805(a)(3) in a flexible, common-sense fashion. See, e.g., Government's Supplemental Memorandum of Law at 12-14. In some cases, the Court's probable cause findings have left the government with a degree of flexibility in precisely how the surveillance is directed

[REDACTED] But, none of the cited cases approach what the government proposes here - - - findings under § 1805(a)(3) that do nothing to limit the government's discretion regarding the persons effectively targeted for surveillance or the communications to be acquired by the surveillance.

²⁹ Judicial authorization and oversight of surveillance under FISA is analogous to the judicial role in domestic criminal surveillance under Title III. After comparing § 1805(a)(3)(B) with the requirements for a Title III wiretap, the Foreign Intelligence Surveillance Court of Review concluded: "FISA requires less of a nexus between the facilities and the pertinent communications than Title III, but more of a nexus between the target and the pertinent communications." In re Sealed Case, 310 F.3d at 740 (emphasis added). However, under the government's theory, the judge's probable cause findings have no bearing whatever on whether the communications actually acquired pertain to a target.

³⁰ H. Rep. 95-1283, pt. 1, at 25. Congress expected the judge to "assess the facts to determine whether certain of the substantive standards have been met," in "the traditional role of a judge in passing on a warrant application." Id.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

The government's proposed probable cause findings under § 1805(a)(3)(A) do not alter these conclusions. No matter how well-founded, a judge's assessment of probable cause to believe that [REDACTED] are foreign powers cannot, in the context of the government's proposal, provide any check on what or whose communications are intercepted.³¹ These foreign powers can only communicate (or otherwise act) through individual members or agents, who use particular phone numbers and e-mail addresses. Because none of the probable cause findings proposed by the government, under either prong of § 1805(a)(3), concerns these particular individuals, phone numbers, or e-mail addresses, the judge's role in making such findings cannot provide the "external check" intended by Congress.

Accordingly, I must conclude that, for purposes of § 1805(a)(3)(B), the phone numbers and e-mail addresses used as selectors are facilities at which the electronic surveillance is directed. I am unable, "on the basis of the facts submitted by the applicant," to find probable cause to believe that each of these facilities "is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* The application contains no facts that would support such a finding. Instead, it is represented that NSA will make the required probable cause finding for each such facility before commencing surveillance. Alexander Decl. at 43. The application seeks, in effect, to delegate to NSA the Court's responsibility to make such findings "based on the totality of circumstances." *See* proposed Order at 14-15.³² Obviously, this would be inconsistent with the statutory requirement and the congressional intent that the Court make such findings prior to issuing the order.³³

³¹ *See* S. Rep. 95-701 at 54, reprinted in 1978 U.S.C.C.A.N. 3973, 4023 (requirement that "the court, not the executive branch, make[] the finding of whether probable cause exists that the target of surveillance is a foreign power or its agent" is intended to be a "check[] against the possibility of arbitrary executive action").

³² *Compare, e.g.,* H. Rep. 95-1823, pt. 1, at 43 ("judge is expected to take all the known circumstances into account" in assessing probable cause to believe that an individual is an agent of an international terrorist group) (emphasis added).

³³ This analysis of congressional purpose applies equally to the aspect of the surveillance that acquires communications that refer to a selector e-mail address, and supports the conclusion that such surveillance is not [REDACTED] identified by the government. This order and opinion does not decide which e-mail addresses are facilities at which such surveillance is directed. *See* note 17 *supra*.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

IV. MINIMIZATION

Another requirement for an electronic surveillance order under § 1805 is that the Court must also find that “the proposed minimization procedures meet the definition of minimization procedures under section 1801(h).” § 1805(a)(4). That section defines minimization procedures, in pertinent part, as

specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, 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). FISA minimization procedures cannot be framed “in a way that is clearly inconsistent with the statutory purpose.” In re Sealed Case, 310 F.3d at 730. More importantly, the minimization procedures must be consistent with the statutory text. See, e.g., Laimie, 540 U.S. at 538 (stressing the “difference between filling a gap left by Congress’ silence and rewriting rules that Congress has affirmatively and specifically enacted”) (internal quotations omitted). Accordingly, proposed minimization procedures that conflict with other provisions of FISA cannot be “reasonably designed” within the meaning of § 1801(h)(1).³⁴

It follows from this principle, and from the foregoing analysis of § 1805(a)(3)(B), that the record in this case will not support the finding required by § 1805(a)(4). The minimization procedures first approved in Docket No. [REDACTED] and proposed in this matter conflict with specific provisions of FISA that govern the initiation and extension of electronic surveillance authority. For example, under the proposed procedures, NSA may initiate surveillance of a foreign phone number or e-mail address unilaterally; express judicial approval is not required,

³⁴ This conclusion holds even if the proposed procedures arguably concern the “acquisition” of information under § 1801(h)(1). All of 50 U.S.C. §§ 1801-1811 regulates the acquisition of information by electronic surveillance. The requirement to adopt and follow reasonable minimization procedures is in addition to the statute’s other requirements for authorizing electronic surveillance, including the requirement that the judge make the probable cause findings specified at § 1805(a)(3). Minimization does not provide a substitute for, or a mechanism for overriding, the other requirements of FISA.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

even after the fact.³⁵ However, § 1805(f) provides that emergency approvals can only be granted by the Attorney General,³⁶ after which an application for electronic surveillance authority must be presented to a judge of this Court within 72 hours of emergency authorization, and surveillance must terminate within 72 hours of the emergency authorization unless a Court order, supported by the necessary probable cause findings, is obtained.

The proposed minimization procedures are also inconsistent with other express statutory requirements regarding the duration and extension of surveillance authorizations. Surveillances targeting foreign powers as defined by § 1801(a)(4) may be initially authorized for up to 90 days [§ 1805(e)(1)] and “extensions may be granted . . . upon an application for an extension and new findings made in the same manner as required for an original order.” § 1805(e)(2). Such “findings” must include a judge’s finding of probable cause to believe that each phone number or e-mail address at which surveillance is directed is being used or is about to be used by a foreign power or an agent of a foreign power. However, the proposed procedures make no provision for review of probable cause at any time after the surveillance is first reported to the Court.

The clear purpose of these statutory provisions is to ensure that, as a general rule, surveillances are supported by judicial determinations of probable cause before they commence; that decisions to initiate surveillance prior to judicial review in emergency circumstances are made at politically accountable levels; that judicial review of such emergency authorizations follows swiftly; and that decisions to continue surveillance receive the same degree of scrutiny as decisions to initiate. The law does not permit me, under the rubric of minimization, to approve or authorize alternative procedures to relieve the government of burdensome safeguards expressly imposed by the statute.

The government argues that alternative, extra-statutory procedures are necessary to provide or enhance the speed and flexibility with which NSA responds to terrorist threats. Government’s Memorandum of Law at 11-12; Government’s Supplemental Memorandum of Law at 4-5. It notes that, in the time it takes to get even an Attorney General emergency

³⁵ A report “briefly summariz[ing] the basis” for NSA’s probable cause findings in support of surveillance of new phone numbers and e-mail addresses would be submitted to the Court at 30-day intervals. Application at 8-9. If the Court concluded that there is not probable cause to believe that such a phone number or e-mail address is used by a targeted foreign power, it could direct that surveillance terminate “expeditiously.” *Id.* at 9.

³⁶ “Attorney General” is defined at § 1801(g) to include also the Acting Attorney General, the Deputy Attorney General, and, “upon designation,” the Assistant Attorney General for National Security.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

authorization, vital foreign intelligence information may be lost. Government's Memorandum of Law at 11-12; Alexander Decl. at 20; [REDACTED] Decl. at 13-15. These matters concern me as well. But, these are risks that Congress weighed when it adopted FISA's procedural requirements,³⁷ over dissenting voices who raised some of the same concerns the government does now.³⁸ These requirements reflect a balance struck by Congress between procedural safeguarding of privacy interests and the need to obtain foreign intelligence information.

The procedures approved in Docket No. [REDACTED] and proposed in this application strike this balance differently for surveillance of phone numbers and e-mail addresses used overseas. However, provided that a surveillance is within the scope of FISA at all,³⁹ the statute applies the same requirements to surveillance of facilities used overseas as it does to surveillance of facilities used in the United States. Congress could well take note of the grave threats now presented by international terrorists and changes in the global communications system,⁴⁰ and conclude that FISA's current requirements are unduly burdensome for surveillances of phone numbers and e-mail addresses used overseas.⁴¹ Unless and until legislative action is taken, however, the judges of this Court must apply the procedures set out in the statute. See § 1803(a) (Court has "jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter") (emphasis added).

³⁷ See H.R. Rep. 95-1283, pt. 1, at 26 (acknowledging potential "risks of impeding or barring needed intelligence collection").

³⁸ FISA's "warrant requirement . . . would pose serious threats to the two most important elements in effective intelligence gathering: (1) speed and (2) security The real possibilities of delay . . . are risks the intelligence community should not be required to take." *Id.* at 113 (Dissenting views of Reps. Wilson, McClory, Robinson, and Ashbrook).

³⁹ This condition is assumed, but not decided, for purposes of this order and opinion. As noted elsewhere, I believe that there are jurisdictional issues regarding the application of FISA to communications that are between or among parties who are all located outside the United States. See note 12 *supra*.

⁴⁰ See, e.g., Alexander Decl. at 11 ([REDACTED])

⁴¹ *Id.* at 19 (burden of preparing FISA applications for [REDACTED]); Government's Supplemental Memorandum of Law at 4 (same); [REDACTED] Decl. at 13-14 (same).

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

Fidelity to this principle "allows both [the legislative and judicial] branches to adhere to our respected, and respective, constitutional roles." Laimie, 540 U.S. at 542.

For the foregoing reasons, I conclude that I cannot grant the application in Docket No. [REDACTED] in the form submitted. I recognize that the government maintains that the President may have "constitutional or statutory authority to conduct the electronic surveillance detailed herein without Court authorization." Application at 25 n.12; see also Alexander Decl. at 6 n.6

[REDACTED] Nothing in this order and opinion is intended to address the existence or scope of such authority, or this Court's jurisdiction over such matters.

V. REQUEST FOR LEAVE TO SEEK EXTENSION IN DOCKET NO. [REDACTED]

On March 29, 2007, I orally advised attorneys for the government that, after careful review of the application and supporting materials, I had reached the above-stated conclusion, and provided a brief summary of the reasoning more fully stated herein. I also stated that, if it chose to do so, the government could supplement the record at a formal hearing.

Based on ensuing discussions, I believe that the government may be able to submit a revised and supplemented application, on the basis of which I could grant at least a substantial portion of the surveillance authorities requested herein, consistent with this order and opinion. The government has undertaken to work toward that goal; however, it is understood that the government has not yet decided on a particular course of action and may, after further consideration, conclude that it is not viable to continue this surveillance within the legal framework stated in this order and opinion.

On April 2, 2007, the government filed in the above-captioned docket a Motion for Leave to File an Application for an Extension of the Orders Issued in Docket No. [REDACTED]. That motion requests leave to file an application for a 60-day extension of those authorities. Motion at 3. On April 3, 2007, the government informally advised that it did not wish to have a hearing on the record prior to my ruling on the motion. I have decided to grant the government leave to file such an application in Docket No. [REDACTED], subject to the requirements stated below.

The sole purpose for granting such leave is to give the government a reasonable amount of time to work in good faith toward the preparation and submission of a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion. I have concluded that an extension for this purpose is appropriate, in view of the following circumstances: that the government has commendably devoted substantial resources to bring the NSA's surveillance program, which had been conducted under the President's assertion

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

of non-FISA authorities, within the purview of FISA; that a judge of this Court previously authorized this surveillance in Docket No. (b)(7)(E), on substantially the same terms as the government now proposes; that it would be no simple matter for the government to terminate surveillance of (b)(7)(E) phone numbers and e-mail addresses under FISA authority, and to decide whether and how it should continue some or all of the surveillance under non-FISA authority; and, importantly, that within the allotted time the government may be able to submit an application that would permit me to authorize at least part of the surveillance in a manner consistent with this order and opinion.

Accordingly, it is hereby ORDERED as follows:

(1) The government may submit an application for a single extension of the authorities granted in Docket No. (b)(7)(E). Any authorities granted pursuant to such an application shall terminate no later than 5:00 p.m., Eastern Time, on May 31, 2007. There shall be no extensions beyond May 31, 2007.

(2) If an extension is obtained under paragraph (1), the government shall periodically submit written reports to me regarding its efforts to prepare and submit for my consideration a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion. The first report shall be submitted on or before April 20, 2007; the second report shall be submitted on or before May 4, 2007; and the third report shall be submitted on or before May 18, 2007.

(3) If, during the period of an extension obtained under paragraph (1), the government determines that it is not feasible or not desirable to submit a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion, it shall immediately notify me in writing of this determination. The submission of such notification shall relieve the government of the requirement to submit reports under paragraph (2). I contemplate that, upon receipt of such notification, I would enter an order formally denying the application in the above-captioned docket.

(4) If authorities obtained pursuant to any extension under paragraph (1) should expire before the government has submitted, and I have ruled on, a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion, then this order and opinion shall be deemed a denial of the above-captioned application, on the grounds stated herein.


(5) Without my prior approval, the government may not submit additional briefing on the bases for my conclusion that I cannot grant this application in its present form. However, if the government continues to seek authority for the type of surveillance discussed at note 17 supra

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

and accompanying text, its further submissions shall include an analysis of the extent to which such surveillance is directed at selector e-mail addresses, and the extent to which it is directed at e-mail addresses that send or receive communications that are acquired because they refer to a selector e-mail address.

Done and ordered this 3^d day of April, 2007 in Docket No. [REDACTED]

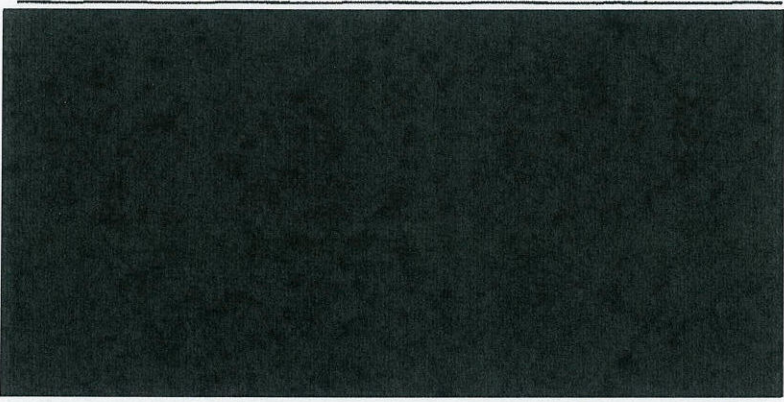

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN~~

All redacted information
exempt under b(1) and/
or b(3) except where
otherwise noted.

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




Docket Number: PR/TT



PRIMARY ORDER

A verified application having been made by a designated attorney for the Government and approved by the Attorney General of the United States for an order authorizing installation and use of pen registers and trap and trace devices pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States Code (U.S.C.), §§ 1801-1811, 1841-1846, and full consideration having been given to the matters set forth therein, the Court finds that:

~~TOP SECRET//COMINT//NOFORN~~

Derived from: Pleadings in the above-captioned docket
Declassify on: 

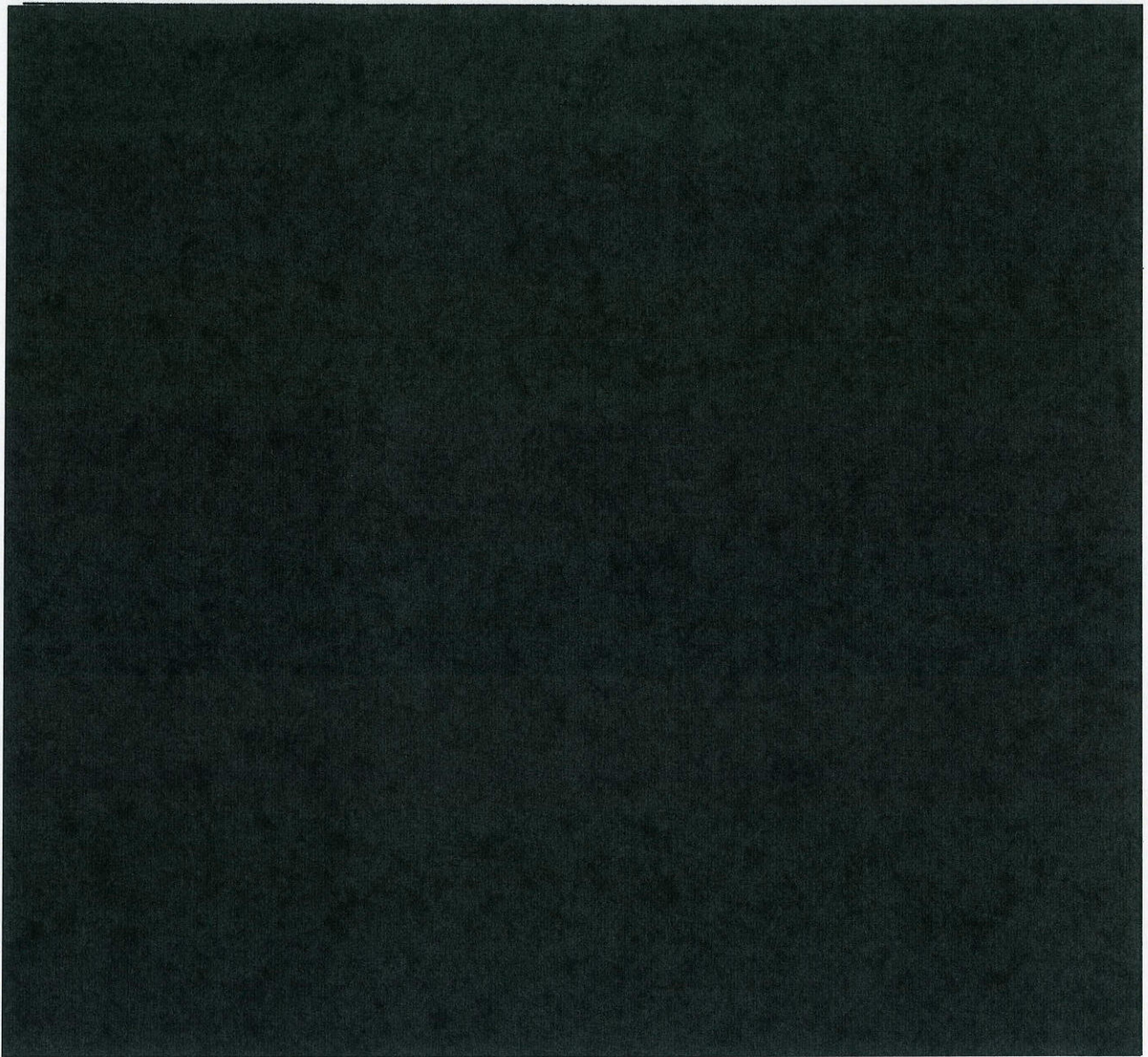
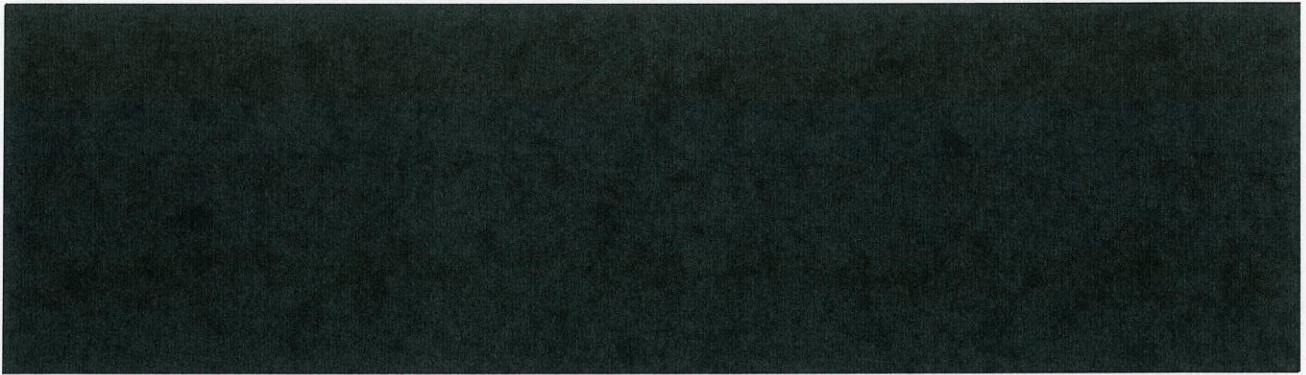
1. The Attorney General is authorized to approve applications for pen registers and trap and trace devices under the Act, and the Attorney General or a designated attorney for the Government is authorized to make such applications under the Act.

2. The applicant has certified that the information likely to be obtained from the requested pen registers and trap and trace devices is relevant to ongoing investigations to protect against international terrorism that are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

3. 



~~TOP SECRET//COMINT//NOFORN~~



~~TOP SECRET//COMINT//NOFORN~~

are the subjects of national security investigations conducted by the Federal Bureau of Investigation (FBI) under guidelines approved by the Attorney General pursuant to Executive Order 12333, as amended.

4. The pen registers and trap and trace devices shall be [REDACTED] described in Tab 1 to the Declaration of [REDACTED] Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate (SID), NSA, which is attached to the Government's Application as Exhibit A.³

WHEREFORE, relying on and adopting the conclusions and analysis set out in its July 14, 2004, Opinion and Order in docket number PR/TT [REDACTED] and the Supplemental Opinion issued on [REDACTED] in docket number PR/TT [REDACTED] which the Court finds applicable to each authorized [REDACTED] as described in Tab 1 to Exhibit A of the Application, the Court finds that the Application of the United States to install and use pen registers and trap and trace devices, as described in the

³ [REDACTED]

Application, satisfies the requirements of the Act and specifically of 50 U.S.C. § 1842 and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the Application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1) Installation and use of pen registers and trap and trace devices as requested in the Government's Application are authorized for a period of ninety days from the date of this Order, unless otherwise ordered by this Court, as follows: installation and use of pen registers and/or trap and trace devices as described above to collect all addressing and routing information reasonably likely to identify the sources or destinations of the electronic communications identified above on the [REDACTED] identified above, including the "to," "from," "cc," and "bcc" fields for those communications [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Collection of the contents of such communications as defined by 18 U.S.C. § 2510(8) is not authorized.

(2) The authority granted is within the United States.

(3) As requested in the Application, [REDACTED]

[REDACTED] (specified persons) are directed to furnish the NSA with any information, facilities, or technical assistance necessary to accomplish the installation and operation of pen registers and trap and trace devices, for purposes of targeting [REDACTED]

[REDACTED]

[REDACTED] in such a manner as will protect their secrecy and produce a minimum amount of interference with the services each specified person is providing to its subscribers. Each specified person shall not disclose the existence of the investigation or of the pen registers and trap and trace devices to any person, unless or until ordered by the Court, and shall maintain all records concerning the pen registers and trap and

trace devices, or the aid furnished to the NSA, under the security procedures approved by the Attorney General and the Director of Central Intelligence that have previously been or will be furnished to each specified person and are on file with this Court.

(4) The NSA shall compensate the specified persons referred to above for reasonable expenses incurred in providing such assistance in connection with the installation and use of the pen registers and trap and trace devices authorized herein.

(5) The NSA shall follow the following procedures and restrictions regarding the storage, accessing, and disseminating of information obtained through use of the pen registers and trap and trace devices authorized herein:

a. The NSA shall store such information in a manner that ensures that it will not be commingled with other data.⁴

b. The ability to retrieve information derived from the pen register and trap and trace devices shall be limited to [REDACTED] specially cleared analysts

⁴

and to specially cleared technical personnel.⁵ The NSA shall ensure that the mechanism for accessing such information will automatically generate a log of auditing information for each occasion when the information is accessed, to include the accessing user's login, IP address, date and time, and retrieval request.

c. Such information shall be accessed only through queries using the contact chaining [REDACTED] [REDACTED] described at page 43 of the Court's July 14, 2004, Opinion and Order in docket number PR/TT [REDACTED]. Such queries shall be performed only on the basis of a particular known [REDACTED] after the NSA has concluded, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, that there are facts giving rise to a reasonable, articulable suspicion that such [REDACTED] [REDACTED] is associated with [REDACTED] [REDACTED] [REDACTED] [REDACTED] provided, however, that

⁵ The Court understands that certain processes must be performed by NSA technical personnel in order to make the metadata collected pursuant to this Order usable by analysts. The restrictions on access contained in this Order shall not apply to those processes.

an [REDACTED] believed to be used by a U.S. person
shall not be regarded as [REDACTED]

[REDACTED]
[REDACTED] solely on the
basis of activities that are protected by the First
Amendment to the Constitution. Further, all metadata

queries shall be performed in accordance with this Court's
[REDACTED] Orders in docket numbers
PR/TT [REDACTED], PR/TT [REDACTED] and PR/TT [REDACTED]. Queries shall
only be conducted with the approval of one of the following
twenty-three NSA officials: the Chief, Special Foreign
Intelligence Surveillance Act (FISA) Oversight and
Processing, Oversight and Compliance, Signals Intelligence
Directorate (SID), NSA; the Chief or Deputy Chief, Homeland
Security Analysis Center; or one of the twenty specially-
authorized Homeland Mission Coordinators in the Analysis
and Production Directorate of the Signals Intelligence
Directorate. E-mail [REDACTED] that are the
subject of electronic surveillance and/or physical search
authorized by the Foreign Intelligence Surveillance Court
(FISC) based on the FISC's finding of probable cause to
believe that they are used by agents of [REDACTED]
[REDACTED]

[REDACTED] including those used by U.S. persons, may be deemed approved for metadata querying without approval of an NSA official. The preceding sentence is not meant to apply to e-mail [REDACTED] [REDACTED] under surveillance pursuant to any certification of the Director of National Intelligence and the Attorney General, pursuant to Section 105B of FISA as added by the Protect America Act of 2007, or Section 702 of FISA, as added by the FISA Amendments Act of 2008. Nor is it intended to apply to e-mail [REDACTED] under surveillance pursuant to an Order of this Court issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

d. The Court understands that the processes described in paragraph (c)(i) and (c)(ii) at pages 7-11 of the 90-Day Report attached to the Application at Tab B are no longer in use. The Government shall not resume use of either of those processes without obtaining prior Court approval.

e. Because the implementation of this authority involves distinctive legal considerations, NSA's Office of General Counsel shall:

i) ensure that analysts with the ability to access such information receive appropriate training

and guidance regarding the querying standard set out in paragraph c. above, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of such information;

ii) monitor the designation of individuals with access to such information under paragraph b. above and the functioning of the automatic logging of auditing information required by paragraph b. above;

iii) to ensure appropriate consideration of any First Amendment issues, review and approve proposed queries of metadata in online storage based on seed accounts used by U.S. persons;⁶ and

iv) at least twice during the 90-day authorized period of surveillance, conduct random spot checks on [REDACTED] to ensure that the collection is functioning as authorized by the Court. Such spot checks shall include an examination of a sample of the data.

⁶ The Court notes that, in conventional pen register/trap and trace surveillances, there is judicial review of the application before any particular e-mail account is targeted. In this case, the analogous decision to use a particular e-mail account as a seed account takes place without prior judicial review. In these circumstances, it shall be incumbent on NSA's Office of General Counsel to review the legal adequacy for the bases of such queries, including the First Amendment proviso, set out in paragraph c. above.

f. The NSA shall apply the Attorney General-approved guidelines in United States Signals Intelligence Directive 18 (Attachment D to the application in docket number PR/TT [REDACTED] to minimize information concerning U.S. persons obtained from the pen registers and trap and trace devices authorized herein. Prior to disseminating any U.S. person information outside of the NSA, the Chief of Information Sharing Services in the NSA's Signals Intelligence Directorate shall determine that the information is related to counterterrorism information and is necessary to understand the counterterrorism information or to assess its importance.

g. Information obtained from the authorized pen registers and trap and trace devices shall be available online for querying, as described in paragraphs b. and c. above, for four and one-half years. Metadata shall be destroyed no later than four and one-half years after its initial collection.

h. Every thirty days during the authorized period of surveillance, NSA shall file with the Court a report that includes: (i) a discussion of the queries that have been made since the prior report to the Court and the NSA's application of the standard set out in paragraph c. above

to those queries; and (ii) any changes in the description of the [REDACTED] described above [REDACTED]

[REDACTED]

i. Additional Oversight Mechanisms. In addition, the Government shall implement the following additional oversight mechanisms to ensure compliance with this Order:

i) NSA's OGC shall consult with the Department of Justice's National Security Division (NSD) on all significant legal opinions that relate to the interpretation, scope, and/or implementation of the authorizations granted by the Court in this matter. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

ii) NSA's OGC shall promptly provide NSD with copies of all formal briefing and/or training materials (including all revisions thereto) currently in use or prepared and used in the future to brief/train NSA personnel concerning the authorizations granted by this Order.

iii) At least once before the expiration of the authorities granted herein, a meeting for the purpose of assessing compliance with this Court's orders in

this matter shall be held with representatives from NSA's OGC, NSD, and appropriate individuals from NSA's SID. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authorities granted herein.

iv) At least once before the expiration of the authorities granted herein, NSD shall meet with NSA's Office of Inspector General (OIG) to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders in this matter.

v) Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC and NSD.

vi) At least once every ninety days, NSA's OGC and NSD shall review a sample of the justifications for querying the metadata, including e-mail [REDACTED] placed on an alert list.

~~TOP SECRET//COMINT//NOFORN~~

In addition, should the United States seek renewal of these authorities, at that time it shall file a report that includes:

(i) detailed information regarding any new facilities proposed to be added to such authority; and (ii) any changes in the proposed means of collection, [REDACTED]

[REDACTED] of the pen registers and/or trap and trace devices.

Signed.

Date

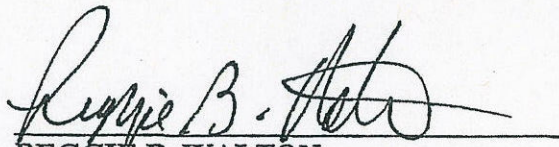
Time

[REDACTED] P04:06

E.T.

This authorization regarding [REDACTED]

[REDACTED] expires on the [REDACTED]
[REDACTED] at 5 p.m., Eastern Time.


REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

[REDACTED] TOP SECRET//COMINT//NOFORN

15

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



MEMORANDUM OPINION
and
ORDER

This matter is before the Court on the Government's Ex Parte Submission of

[REDACTED] and Related Procedures and Request for an Order Approving [REDACTED]

[REDACTED] and Procedures, filed on [REDACTED] 2009 ([REDACTED] Submission" [REDACTED]

[REDACTED] pursuant to 50 U.S.C. § 1881a(g). For the reasons stated below, the government's request for approval is granted.

I. BACKGROUND

A. [REDACTED] Certifications Submitted Under Section 1881a

The [REDACTED] Submission includes [REDACTED] filed by the government pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which was enacted as part of the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (Jul. 10, 2008)

[REDACTED]

On [REDACTED] 2009, respectively, the Director of National Intelligence and the Attorney General executed amendments to the certifications [REDACTED] [REDACTED] for the purpose of authorizing the FBI to use, under those certifications, the same revised FBI minimization procedures that were submitted to and approved by the Court in connection with [REDACTED]. See [REDACTED] 2009 Memorandum Opinion at 3. On [REDACTED] 2009, the Court issued a Memorandum Opinion and accompanying order approving the amendments. *Id.* at 6. Each of the Court's Memorandum Opinions in the Original 702 Dockets (to include the [REDACTED] 2009 Memorandum Opinion) is incorporated by reference herein.

B. The Government's Representations

On [REDACTED] 2009, following a meeting with the Court staff, the United States submitted the Government's Response to the Court's Questions Posed by the Court (the [REDACTED] Submission").¹ In that submission, the government indicates that each set of targeting and minimization procedures now before the Court is either substantively identical, or very similar, to procedures previously approved by the Court in the Original 702 Dockets.² [REDACTED]

¹ [REDACTED]

² See Procedures Used by NSA for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended ("NSA Targeting Procedures") (attached [REDACTED])

(continued...)

Submission at 13-14. Notwithstanding such similarity, the government notes a few cross-cutting changes from the earlier approved procedures. First, in the various procedures submitted [REDACTED]

[REDACTED] the government throughout uses “will” rather than “shall, which had been used in the prior sets of procedures. [REDACTED] Submission at 1.³ The government avers that this change “[is] purely stylistic and ... not intended to suggest that each agency’s obligation to comply with the requirements set forth in their respective targeting and/or minimization procedures submitted with [REDACTED] diminished in any way.” Id. Second, the government has changed the deadline for complying with various reporting requirements from “seven days” to “five business days.” Id. at 2. According to the government, this change “is intended to remove any potential ambiguity in calculating the deadline for reporting matters as required.” Id. Finally, the government has added to the NSA and CIA Minimization Procedures an emergency provision similar to that which already had

²(...continued)

[REDACTED] as Exhibit A); Procedures Used by the FBI for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended (“FBI Targeting Procedures”) (attached [REDACTED] as Exhibit C).

See Minimization Procedures Used by the NSA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended (“NSA Minimization Procedures”) (attached [REDACTED] as Exhibit B); Minimization Procedures Used by the FBI in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended (“FBI Minimization Procedures”) (attached [REDACTED] as Exhibit D); Minimization Procedures Used by the CIA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended (“CIA Minimization Procedures”) (attached [REDACTED] as Exhibit E).

³This change also is reflected in the Affidavit submitted by Lt. Gen. Keith B. Alexander, U.S. Army, Director, NSA (attached [REDACTED] at Tab 1) at 3-4.

been included in the FBI Minimization Procedures. [REDACTED] NSA Minimization Procedures at 1, CIA Minimization Procedures at 6 [REDACTED] Submission at 2.

Apart from these across-the-board changes, the government confirms that the NSA and FBI targeting procedures are virtually identical to those submitted to and approved by the Court

[REDACTED] Submission at 13. Similarly, the

government represents that the FBI Minimization Procedures now before the Court are in all

material respects identical to the FBI Minimization Procedures approved by the Court [REDACTED]

[REDACTED] and again in connection with the [REDACTED] amendments to the certifications [REDACTED]

[REDACTED] Id. at 14. Likewise, the NSA Minimization

Procedures at bar are nearly identical to the corresponding procedures approved by the Court [REDACTED]

[REDACTED] ⁴ Id. at 13-14.⁵

The CIA Minimization Procedures, while substantially similar to the procedures approved by the Court [REDACTED] include a few material

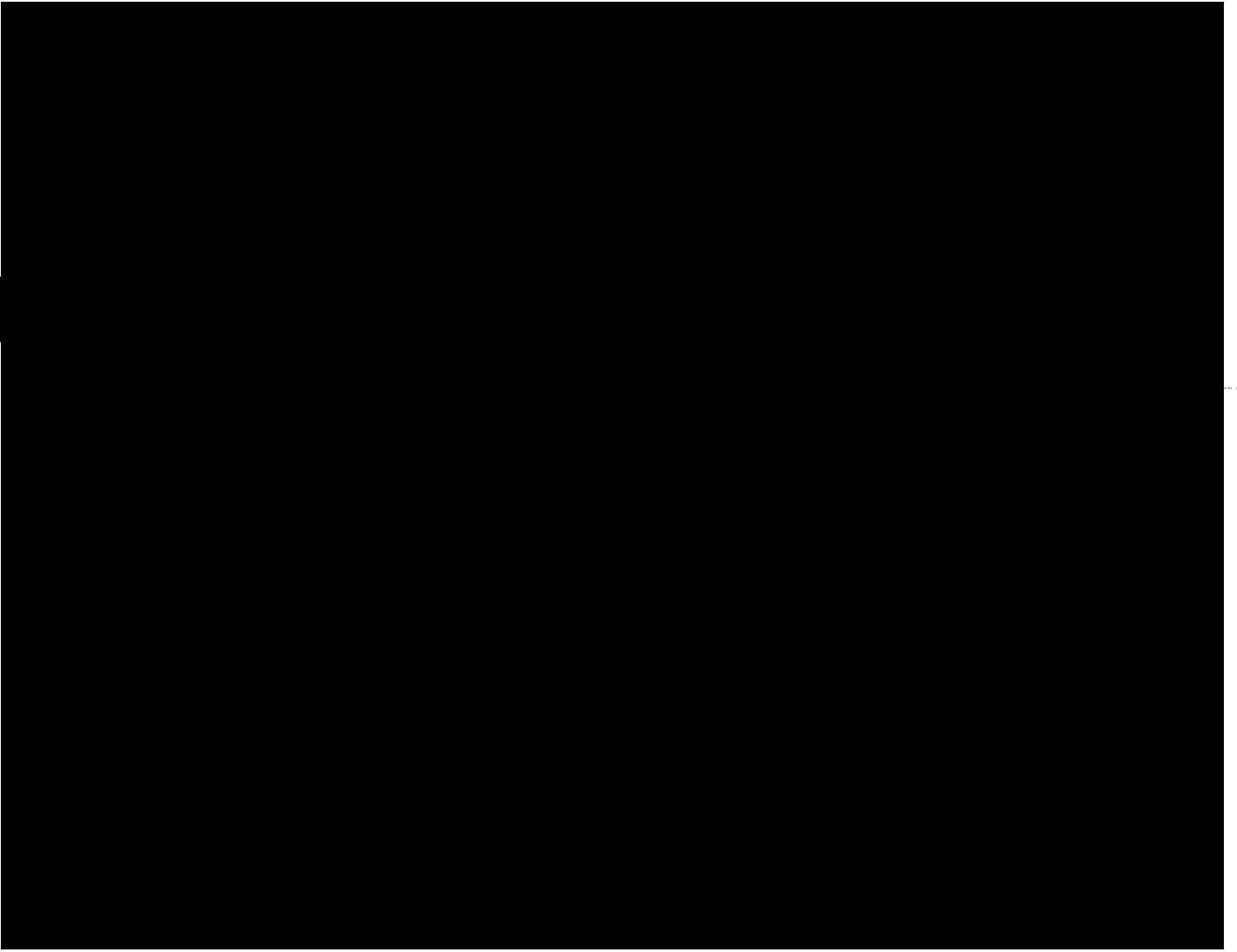
4 [REDACTED]

⁵In a departure from the previous minimization procedures, the NSA Minimization Procedures submitted in this docket do not characterize the transfer of unminimized information from NSA to the FBI and the CIA as “disseminations,” but rather as the provision of information. The government made this change “so that the description of the information-sharing regime established by the NSA minimization procedures ... is consistent with the Court’s opinion in [REDACTED]

[REDACTED] Submission at 4-5. The Court does not understand this change of wording to modify or limit the requirements governing such “provision” or “dissemination” of information.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

differences. The procedures submitted in this Docket incorporate a handful of provisions that had not been in the prior minimization procedures but are part of [REDACTED]



6

7

~~TOP SECRET//COMINT//ORCON,NOFORN~~

The Court has carefully reviewed the instant Procedures and has found that, with the exception of the above-described differences and certain non-material changes, the procedures submitted in the current Docket, as informed by the [REDACTED] Submission, mirror those submitted and approved by the Court in the Original 702 Dockets and their amendments.

II. REVIEW [REDACTED]

The Court must review a certification submitted pursuant to Section 702 of FISA “to determine whether [it] contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court’s examination [REDACTED] submitted in the above-captioned docket confirms that:

- (1) [REDACTED] been made under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), [REDACTED]
- (2) [REDACTED] each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), *id.* at 1-3;
- (3) as required by 50 U.S.C. § 1881a(g)(2)(B), [REDACTED] accompanied by the applicable targeting procedures⁸ and minimization procedures;⁹
- (4) [REDACTED] supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);¹⁰ and

⁸ See [REDACTED] NSA Targeting Procedures and FBI Targeting Procedures.

⁹ See [REDACTED] NSA Minimization Procedures, FBI Minimization Procedures, and CIA Minimization Procedures.

¹⁰ See [REDACTED] Affidavit of Lt. Gen. Keith B. Alexander, U.S. Army, Director, NSA (attached [REDACTED] at Tab 1); Affidavit of Robert S. Mueller, III, Director, (continued...)

(5) [REDACTED] an effective date for the authorization in compliance with 50 U.S.C. § 1881a(g)(2)(D). [REDACTED]

Accordingly, the Court finds that [REDACTED] submitted [REDACTED]
“contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A).

III. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is required to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). 50 U.S.C. § 1881a(i)(2)(B) and (C). Section 1881a(d)(1) provides that the targeting procedures must be “reasonably designed” to “ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States” and to “prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” Section 1881a(e)(1) requires that the “minimization procedures [] meet the definition of minimization procedures under section 1801(h) or 1821(4) of [the Act]...” In addition, the Court must determine whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A).

¹⁰(...continued)

FBI (attached [REDACTED] at Tab 2); Affidavit of Leon E. Panetta, Director, CIA (attached [REDACTED] at Tab 3).

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

Based on the Court's review of the targeting and minimization procedures in the above-captioned Docket, the representations of the government made in this matter and those carried forward from the Original 702 Dockets, and the analysis set out below and in the Memorandum Opinions of the Court in the Original 702 Dockets and their amendments, the Court finds that the targeting and minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.

As discussed above, the targeting and minimization procedures are, in substantial measure, the same as those previously found to comply with the requirements of the statute and with the Fourth Amendment to the Constitution. The few substantive changes noted do not change the Court's assessment. There is no statutory or constitutional significance to the change from a seven day reporting deadline to five business days. Nor is the Court concerned about the government's use of "will" rather than "shall," given the government's assurance that the change is merely stylistic. And, the Court is satisfied that U.S. person information will be properly protected through the processes described in the CIA Minimization Procedures, [REDACTED] [REDACTED] In fact, only two changes even have the potential to require that the Court re-assess its prior determinations.

For the first time, both NSA and CIA include a provision in their Minimization Procedures that allows the agency to act in apparent departure from the procedures to protect against an immediate threat to human life. [REDACTED] NSA Minimization Procedures at 1, CIA Minimization Procedures at 6. However, these emergency provisions are

virtually identical to a provision in the FBI Minimization Procedures that were approved [REDACTED]

[REDACTED] The government has informed the Court that the one substantive difference - the absence of a time frame by which the agency must notify the DNI and NSD of the exercise of the emergency authority - was inadvertent and that both the NSA and CIA have represented to the Department of Justice that they, like the FBI, will promptly report any emergency departure. [REDACTED]

Submission at 2.

[REDACTED]

The new standard, [REDACTED] continues to require a foreign intelligence purpose for retaining such information; the procedures only permit the retention of such [REDACTED] [REDACTED] "consistent with the need of the United States to ... produce and disseminate foreign intelligence information." 50 U.S.C. §1801(h)(1). As the Court noted in its September 4, 2008 Memorandum Opinion, procedures that meet this requirement contribute to the Court's assessment that such procedures comport with the Fourth

Amendment. Id. at 40.

In addition to the procedures themselves, however, the Court must examine the manner in which the government has implemented them. In its April 7, 2009 Memorandum Opinion, the Court acknowledged that while the potential for error was not a sufficient reason to invalidate surveillance, the existence of actual errors may “tip the scales toward prospective invalidation of the procedures under review...” Id. at 27. In its [REDACTED] Submission, the government reports on [REDACTED] compliance matters that had previously been the subjects of preliminary notices to the Court, [REDACTED] which involve NSA and one of which involves the CIA.¹² Id. at 5-11.

The NSA problems principally involve analysts improperly acquiring the communications of U.S. persons. Id. In response to these incidents, NSA’s Office of Oversight and Compliance has instituted several procedures designed to ensure more rigorous documentation of targeting decisions in order to minimize the likelihood that NSA analysts will improperly target U.S. persons or persons located within the U.S. Id. at 7, 8. In addition, NSA has conducted remedial training not only of the individual analysts who committed the errors, but the offices and management chains involved. Id. at 6-9.

The CIA problem is more discrete although arguably more troubling because it reflects a profound misunderstanding of minimization procedures, the proper application of which contribute significantly to the Court’s finding that such procedures comport with the statute and

¹²The government reports that it is aware of no new compliance incidents resulting from [REDACTED] over-collection [REDACTED]. See April 7, 2009 Memorandum Opinion at 17-27 for a full discussion [REDACTED] incident before the Court [REDACTED]

the Fourth Amendment. A [REDACTED] who no longer works with or has access to FISA information, improperly minimized at least [REDACTED] reports that were disseminated to NSA, FBI, and DOJ. [REDACTED] 2009, Preliminary Notice of Compliance Incident Regarding Collection Pursuant to Section 105B of the Protect America Act and Section 702 of the FISA, as Amended; [REDACTED] Submission at 9-11. Recognizing that if one person so significantly misunderstood the minimization regime, others might as well, the “ODNI, NSD, and CIA have been working together to implement procedures that will facilitate more comprehensive oversight of CIA’s applications of its minimization procedures in the future.” [REDACTED] Submission at 10. In addition, “CIA has made several process and training changes as a result of [this incident]. *Id.* at 11.

Given the remedial measures implemented in both agencies as a result of the compliance incidents reported to the Court, the Court is satisfied that these incidents do not preclude a finding that the targeting and minimization procedures submitted in the above-captioned docket satisfy the requirements of the FAA and the Fourth Amendment.

The Court, however, is aware that both NSA and FBI have identified additional compliance incidents that have not been reported to the Court. Through informal discussion between NSD attorneys and the Court staff, and later confirmed at a hearing held on [REDACTED] 2009 to address these matters, the Court learned that the government’s practice has been to report only certain compliance incidents to the Court: those that involve systemic or process issues, those that involve conduct contrary to a specific representation made to the Court, and those that involve the improper targeting of U.S. persons under circumstances in which the analyst knew or

should have known that the individual was a U.S. person.

Consistent with the government's practice, the Court was not notified of numerous incidents that involved the failure to de-task accounts once NSA learned that non-U.S. person targets had entered the United States. Indeed, in the [REDACTED] 2009 hearing, the government informed the Court that in addition to [REDACTED] incidents informally reported on [REDACTED], 2009 to the FISC staff, there were approximately [REDACTED] other similar incidents, all of which occurred since [REDACTED] 2008. The government reported at the hearing that while the de-tasking errors did not all stem from the same problem, NSA has instituted new [REDACTED] processes to minimize the likelihood of these types of de-tasking errors recurring. In addition, the government informed the Court that NSA's system for conducting post-targeting checks provides an effective backstop in the government's efforts to de-task accounts [REDACTED]. Finally, the government confirmed to the Court that NSA has purged from its systems all communications acquired during the period of time when these accounts should have been de-tasked. Based on these representations, the Court is satisfied that these incidents do not rise to the level of undermining the Court's assessment that the targeting and minimization procedures comport with the statute and the Fourth Amendment.

However, the Court is concerned that incidents of this sort were not reported to the Court, in apparent contravention of Rule 10(c) of Foreign Intelligence Surveillance Court Rules of Procedures.¹³ Section 702(i)(2)(B) specifically directs the Court to review the targeting

¹³The Court appreciates the assurances offered by the Department of Justice at the [REDACTED]
(continued...)

procedures “To assess whether [they] are reasonably designed to ensure that any acquisition ... is limited to targeting persons reasonably believed to be located outside the United States and 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.” Given the Court’s obligations under the statute, and consistent with 50 U.S.C. § 1803(i), the Court

HEREBY ORDERS the government, henceforth, to report to the Court in accordance with the Rule 10(c) of Foreign Intelligence Surveillance Court Rules of Procedure, every compliance incident that relates to the operation of either the targeting procedures or the minimization procedures approved herein.

IV. CONCLUSION

For the foregoing reasons, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that [REDACTED] submitted in the above-captioned docket “in accordance with [Section 1881a(g)] [REDACTED] all the required elements and that the targeting and minimization procedures adopted in accordance with [Section 1881a(d)-(e)] are consistent with the requirements of those

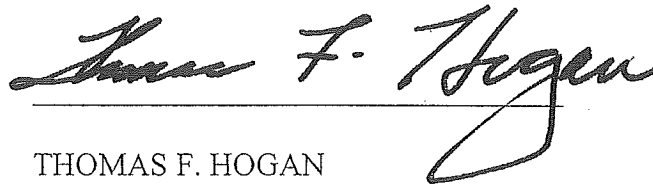
¹³(...continued)

[REDACTED] 2009 hearing that, henceforth, the government will work with the Court, through the Court’s counsel, to ensure that the government’s guidelines for notifying the Court of compliance incidents satisfy the needs of the Court to receive timely, effective notification of such incidents.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

subsections and with the fourth amendment to the Constitution of the United States.” A separate order approving [REDACTED] and the use of the procedures pursuant to Section 1881a(i)(3)(A) is being entered contemporaneously herewith.

ENTERED this [REDACTED] 2009.



THOMAS F. HOGAN
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//COMINT//ORCON,NOFORN~~

exempt under b(6)

Page 15

Deputy Clerk
This document is a copy of
the original

exempt
under b(6)

App.605

~~SECRET~~

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

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the above-captioned [REDACTED] submitted in accordance with [50 U.S.C. § 1881a(g)] [REDACTED] all the required elements and that the targeting and minimization procedures adopted in accordance with [50 U.S.C. § 1881a(d)-(e)] are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States.”

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that [REDACTED]

[REDACTED] and the use of such procedures are approved.

ENTERED this [REDACTED] 2009.



THOMAS F. HOGAN
Judge, United States Foreign
Intelligence Surveillance Court

exempt under b(6)

Deputy Clerk

This document
is a true and correct copy of
the original

exempt
under b(6)

~~SECRET~~

Docket Number: BR 09-15

On October 30, 2009, the Court authorized the acquisition by the National Security Agency (“NSA”) of the tangible things sought in the government’s application in the above-captioned docket (“BR metadata”). This supplemental opinion and order reiterates the manner in which query results may be shared within the NSA, as informed by the testimony provided by government, and elaborates on the reporting requirement imposed in the Court’s order of October 30.

Sharing of BR Metadata Query Results Within the NSA

The Court's order permits NSA analysts who are authorized to query the BR metadata to share the results of authorized queries among themselves and with other NSA personnel, "provided that all NSA personnel receiving such query results in any form (except for information properly disseminated outside NSA) shall first receive appropriate and adequate training and guidance regarding the rules and restrictions governing the use, storage, and dissemination of such information." Primary Order at 15, Docket No. BR 09-15 (October 30, 2009) ("October 30 Order"). The order further provides: "[a]ll persons authorized for access to the BR metadata and other NSA personnel who are authorized to receive query results shall receive appropriate and adequate training by NSA's [Office of General Counsel] concerning the authorization granted by this Order, the limited circumstances in which the BR metadata may be accessed, and/or other procedures and restrictions regarding the retrieval, storage, and dissemination of the metadata." *Id.* at 13. The Court's prior order in this matter contained identical provisions. Primary Order at 12, 14-15, Docket No. BR 09-13 (September 3, 2009) ("September 3 Order").

In September, 2009, the Court received oral notification that NSA analysts had, on two occasions, shared the results of queries of the BR metadata with NSA analysts involved in the [REDACTED] investigation who had not received "appropriate and adequate training and guidance" as required under the September 3 Order. Order Regarding Further Compliance Incidents at 2-3, Docket No. BR 09-13 (September 25, 2009). On September 25, 2009, the Court ordered representatives of the NSA and the National Security Division ("NSD") of the

Department of Justice to appear for a hearing in order to inform the Court more fully of the scope and circumstances of the incidents, and to allow the Court to assess whether the Court's order should be modified or rescinded and whether other remedial steps should be imposed. Id. at 4.

At the hearing, which was conducted on September 28, 2009, the government confirmed that NSA analysts authorized to query the BR metadata had sent query results to NSA personnel who had not received the training and guidance required by the Court's September 3 Order. Transcript at 6-7, Docket No. BR 09-13. Specifically, the government reported that the NSA had created an e-mail distribution list (the NSA representative referred to this list as an "alias") for the 189 NSA analysts who were working on the "[REDACTED]" threat, only 53 of whom had received the required training and guidance. Id. at 6-7, 12-13. On September 17th, an NSA analyst authorized to query the BR metadata sent an e-mail to the [REDACTED] alias that included a "general analytic summary" of the results of a query of the BR metadata. Id. at 7. After a recipient brought the e-mail to the attention of the NSA's Oversight and Compliance Office and Office of General Counsel, the Oversight and Compliance Office issued guidance on September 21st, "reemphasizing the point, no dissemination of query results in any form." Id. at 14. The NSA's Counter-terrorism organization sent a similar reminder on the morning of September 22nd, however, that afternoon, a second NSA analyst who was authorized to query the BR metadata sent a situation report to the [REDACTED] alias that contained information derived from a query of the BR metadata. Id. at 15.

The government testified at the hearing that the NSA has taken steps to ensure that any sharing of the results of queries of the BR metadata within the NSA is fully consistent with the

Court's orders. First, the NSA has issued guidance interpreting "query results in any form," to mean any information of any kind derived from the BR metadata. *Id.* at 16. Second, NSA aliases for sharing information that could include BR metadata query results, will be limited to NSA personnel who have received the necessary training and guidance to receive those query results. *Id.* at 21-22. The Court hereby affirms that the NSA may share BR metadata query results in this manner consistent with the Court's October 30 Order. The only exception to this practice is under circumstances in which the Court has expressly authorized a deviation.¹

Report on Queries Described in Footnote 6 of the Court's October 30 Order

According to the government, one advantage of the BR metadata repository is that it is historical in nature, reflecting contact activity from the past that cannot be captured in the present or prospectively. Declaration of [REDACTED] at 7, Docket No. BR 09-15. At the government's request, the Court's September 3 Order and October 30 Order both acknowledge that the government may query the BR metadata for historical purposes, using a telephone identifier that is not currently associated with one of the targeted foreign powers, but that was for a period of time in the past.²

¹ For example, pursuant to paragraph (3)J of the Court's order, NSA personnel authorized to query the BR metadata may use and share the identity of high-volume telephone identifiers and other types of identifiers not associated with specific users for purposes of metadata reduction and management, without regard to whether the recipient has received the training and guidance required for access to BR metadata query results.

² Both orders contain the following footnote: "The Court understands that from time to time the information available to designated approving officials will indicate that a telephone identifier was, but may not presently be, or is, but was not formerly, associated with [REDACTED]. In such a circumstance, so long as the designated approving official can determine that the reasonable, articulable suspicion standard can be met for a particular period of time with respect to the telephone identifier, NSA may query the BR metadata using that telephone identifier. However, analysts conducting queries using such telephone identifiers must be made aware of the time period for (continued...)"

Nevertheless, the NSA's querying of the BR metadata using telephone identifiers that do not currently satisfy the "reasonable articulable suspicion" standard has been a source of concern for the Court. Given that telephone providers regularly re-assign telephone identifiers, and in light of the fact that the NSA acquires approximately [REDACTED] call detail records per day, the vast majority of which are irrelevant to the Federal Bureau of Investigation's ("FBI") investigations and concern communications of United States persons in the United States, it would appear likely that such a query could produce results that include metadata from United States persons not under investigation by the FBI. In order to allay these concerns, the Court's September 3 Order mandated that any application to renew or reinstate the authority granted therein must include a report describing, among other things, how the NSA has conducted [these types of queries] and minimized any information obtained or derived therefrom. September 3 Order at 18.

The government's report submitted as Exhibit B to its Application in Docket Number 09-15, stated:

From time to time, NSA may have information indicating that a particular identifier was used by an individual associated with [REDACTED] only for a particular timeframe. In these circumstances, NSA would seek and grant as appropriate, RAS approval, with the understanding that contact chaining would be conducted in a manner that covered a limited timeframe that has been identified.

(...continued) which the telephone identifier has been associated with [REDACTED] in order that the analysis and minimization of the information retrieved from their queries may be informed by that fact." September 3 Order at 9, n. 5; October 30 Order at 9, n. 6.

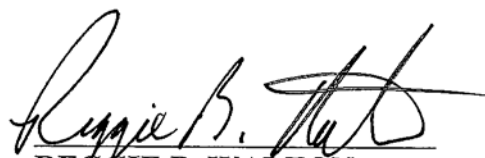
The report then provided one example of how the NSA had conducted such a query. NSA Report to the Foreign Intelligence Surveillance Court (BR 09-13) at 15-16.

This report was not sufficiently detailed to allay the Court's concerns, and the Court therefore continues to be concerned about the likelihood that these queries could reveal communications of United States person users of the telephone identifier who are not the subject of FBI investigations. As a result, the Court's October 30 Order contains the same reporting requirements as the September 3 Order. October 30 Order at 18-19. However, to assist the government in providing a report that satisfies its needs, the Court HEREBY ORDERS that any report submitted by the government pursuant to paragraph (3)S of the Court's October 30 Order shall include the following information with regard to how the NSA has conducted queries of the BR metadata using telephone identifiers determined to satisfy the reasonable articulable suspicion standard at some time in the past, but that do not currently meet the standard, and how the NSA minimized any information obtained or derived therefrom:

1. The total number of such queries run during the reporting period and what percentage those queries constitute of the total number of queries run.
2. Would the status of a telephone identifier that was approved for querying under these circumstances be changed on the Station Table to non-RAS approved once a single query using that identifier has been run? If not, does the NSA have an automated process to limit queries of that telephone identifier to the specified time frame? If not, how will an NSA analyst know that any query of that telephone identifier must be limited to the time period for which the reasonable articulable suspicion existed?

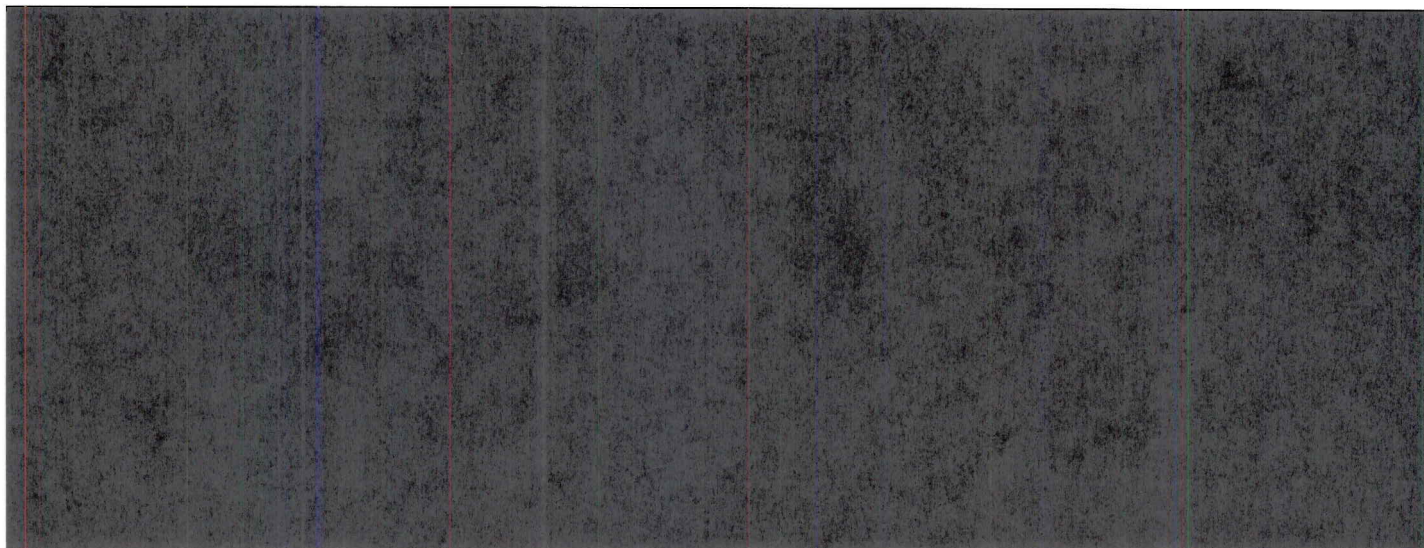
3. Are NSA analysts permitted to conduct more than one query using any telephone identifier determined to have met the reasonable articulable suspicion standard under circumstances described above, and if so, for what purpose? If query results from the first query indicated that the telephone identifier's association with the foreign power terminated earlier than the date the NSA believed the identifier no longer met the reasonable articulable suspicion, would the timeframe restriction be adjusted for any subsequent query?
4. If this type of query is run, and the NSA analyst who ran the query determines that the query results include records of communications that were made after the telephone identifier was re-assigned to a United States person who is not associated with the foreign power, must the analyst delete or otherwise mask such records prior to sharing the query results with NSA analysts authorized to receive query results pursuant to paragraph (3)I of the Court's order?

ENTERED this 5th day of November, 2009.


REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET/COMINT/OC,NF~~

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



SUPPLEMENTAL OPINION AND AMENDMENT TO PRIMARY ORDER

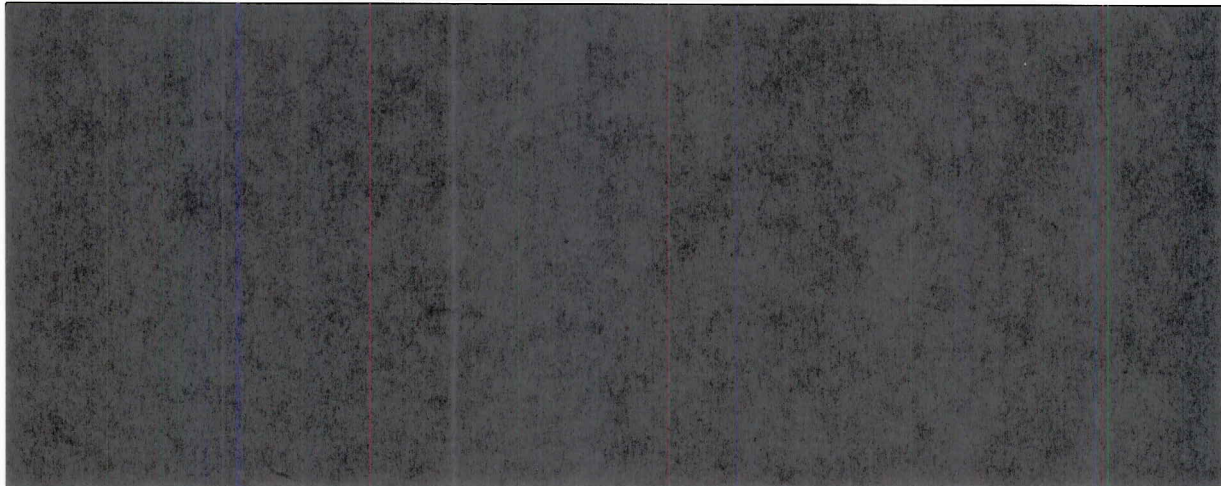
On [REDACTED] the Court issued a Primary Order in the above-captioned docket authorizing the National Security Agency (NSA) to install and use pen register/trap and trace (PR/TT) devices to engage in the bulk collection of certain forms of metadata about Internet communications. At that time, the Court also issued a Memorandum Opinion that explained, inter alia, the reasons for approving some parts of the proposed PR/TT collection, but not others. See Docket No. PR/TT [REDACTED] Memorandum Opinion issued on [REDACTED] (“Memorandum Opinion”). The Primary Order stated that “NSA shall, pursuant to this Order, collect only metadata approved for acquisition in Part II” of the Memorandum Opinion. Primary Order at 5.

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

Subsequently, the government requested clarification of certain issues addressed in the Memorandum Opinion. See Letter submitted on [REDACTED] (“[REDACTED] Letter”). The government separately submitted additional information pertaining to one of the issues for which it sought clarification. See Letter submitted on [REDACTED] (“[REDACTED] Letter”). In response to the government’s request, and in view of the importance and complexity of the issues involved, the Court is issuing this Supplemental Opinion and Amendment to Primary Order.¹ For ease of reference, the discussion below employs the government’s enumeration of the issues identified in the [REDACTED] Letter.

Issue No. 1: [REDACTED]



¹ Familiarity with the terminology and reasoning of the Memorandum Opinion is assumed. Matters discussed in the Memorandum Opinion are addressed herein only insofar as they particularly relate to a request for clarification.

² See Memorandum Opinion at 35 n.36 (“For purposes of this Opinion, the term ‘e-mail communications’ refers to e-mail messages sent between e-mail users, [REDACTED] [REDACTED]”).

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

After describing what it perceives as a potential ambiguity in the Memorandum Opinion,³ the government requests confirmation of its understanding that NSA is [REDACTED]

[REDACTED]

Letter at 2. As explained below, however, the government's formulation is an overly broad description of the authority granted by the Court.

The Memorandum Opinion largely tracks the government's application in describing [REDACTED] [REDACTED] metadata for which approval was requested. See Memorandum Opinion at 35-41. The Memorandum Opinion limits the collection authority for several of these categories. Although many of the limitations imposed by the Court mirror the government's factual description of how the PR/TT devices would operate,⁴ the government did not, for the most part, incorporate such limitations into the scope of the requested collection authority. Under the expansive interpretation of the relevant statutory provisions put forward by the government, the

³ Specifically, the government observed that its submissions had defined [REDACTED] [REDACTED] See [REDACTED] Letter at 2 (comparing Application, Exhibit D, [REDACTED] Response at 2, 8 with Memorandum Opinion at 62).

⁴ See, e.g., Application, Exhibit D, [REDACTED] Response at 1 [REDACTED] [REDACTED]; Application, Exhibit B, Memorandum of Law and Fact in Support of Application for PR/TT Devices for Foreign Intelligence Purposes at 23-24, 43 [REDACTED] [REDACTED].

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

limitations may not have been warranted. But after careful consideration, the Court adopted a less expansive interpretation of the statute, see Memorandum Opinion at 30-35, 51-62, thereby requiring a more careful examination of the circumstances of collection for some types of metadata, and particularly an assessment of [REDACTED]

See, e.g., id. at 37-38, 42-44, 51-62.

The principal limitations adopted by the Memorandum Opinion are:

[REDACTED]

[REDACTED]

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

[REDACTED]

In sum, as the Memorandum Opinion explains,

[REDACTED]

They,

therefore, may be collected only in the circumstances approved by the Court in the Memorandum Opinion.

Issue No. 2: [REDACTED]

The government seeks clarification regarding the scope of metadata it may collect from a communication [REDACTED]

See [REDACTED], Letter at 2-3. The Memorandum Opinion states:

[REDACTED]

[REDACTED]

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

[REDACTED]

Memorandum Opinion at 48 (citation omitted). After analyzing the relevant statutory provisions, the Court concluded that [REDACTED]

[REDACTED]

Id. at 62-71.

The government understands that, even in circumstances when [REDACTED]

[REDACTED]

Letter at 3. This understanding is

correct, subject to a proper understanding of what constitutes “authorized metadata” in the circumstances in question, as discussed above with respect to Issue No. 1.

Issue No. 3: [REDACTED]

[REDACTED]

Memorandum Opinion at 37. The Memorandum Opinion describes two general circumstances in

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

which the collection of [REDACTED]

See id. The government now seeks clarification regarding the scope of these circumstances. See [REDACTED] Letter at 3.

The first circumstance is [REDACTED]

[REDACTED] Memorandum Opinion at 37-38. In

such a case, the Court authorized collection of [REDACTED]

[REDACTED] Id. at 38. The government now seeks clarification that collection of [REDACTED]

[REDACTED] Letter at 3 (footnote omitted).

[REDACTED] Id. at 3 n.1.⁶

In the above-quoted example, [REDACTED]

⁶ This example is similar to one previously provided by the government to illustrate how [REDACTED]

See Application, Exhibit D, [REDACTED] Response at 2.

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

[REDACTED]

As the Memorandum Opinion stated, [REDACTED]

[REDACTED]

Memorandum

Opinion at 55 (emphasis in original). In this example, [REDACTED]

[REDACTED]

The second circumstance discussed in the Memorandum Opinion is [REDACTED]

[REDACTED]

[REDACTED] Memorandum Opinion at 37. The government understands that, in this circumstance, [REDACTED]

[REDACTED]

⁷ See Memorandum Opinion at 36-37 [REDACTED]

[REDACTED]

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

[REDACTED]

[REDACTED] Letter at 3. This understanding is correct. Footnote 37 of the Memorandum Opinion⁸ is intended to address the opposite case: [REDACTED]

Issue No. 4: [REDACTED]

The government correctly notes that some [REDACTED] approved for collection [REDACTED]. See [REDACTED] Letter at 4; Memorandum Opinion at 65. When collecting these [REDACTED]

The government requests clarification that NSA's collection process may also infer the [REDACTED]

[REDACTED] See [REDACTED] Letter at 4. For example, [REDACTED]

⁸ Footnote 37 states: [REDACTED]

[REDACTED] Memorandum Opinion at 38 n.37 (citation omitted).

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NT~~

See Memorandum Opinion at 42-43. The government requests confirmation that, in such a case,

[REDACTED]

[REDACTED] Letter at 1.

The Court concludes that [REDACTED]

[REDACTED] may be authorized as a form of PR/TT collection under the analysis adopted in the Memorandum Opinion.

[REDACTED]

[REDACTED] Memorandum Opinion

at 51-65. [REDACTED]

[REDACTED]

Cf. Memorandum Opinion at 59 [REDACTED]

[REDACTED]

Issue No. 5: [REDACTED]

As described in the Memorandum Opinion, the collection process involves [REDACTED]

[REDACTED]

[REDACTED] Memorandum Opinion at 27-28. During the

~~TOP SECRET/COMINT/OC,NT~~

~~TOP SECRET/COMINT/OC,NF~~

collection process, [REDACTED]

Id. at 27.

The government has now advised that some of this [REDACTED]

See

[REDACTED] Letter at 4. [REDACTED]

Id. [REDACTED]

Memorandum

Opinion at 27 (internal quotations omitted).

Under these circumstances, the fact that [REDACTED]

[REDACTED] poses no legal difficulty. This Court has approved other forms of PR/TT collection that involve [REDACTED] See, e.g., Docket No. PR/TT [REDACTED], Supplemental Opinion issued on [REDACTED]

In this case, [REDACTED]

Memorandum Opinion at 29 (emphasis added). Accordingly, the collection process

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

described in the Memorandum Opinion and authorized in the Primary Order may, as necessary,



* * *

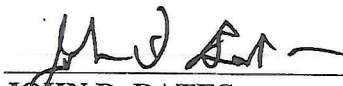
For the reasons stated above, it is permissible for NSA to collect metadata as described in Part II of the Memorandum Opinion, as supplemented herein. Accordingly, it is hereby ORDERED that the Primary Order issued on [REDACTED] in the above-captioned docket is amended as follows:

Paragraph 5(A), on page 5 of the Primary Order, is amended to read:

“(5) NSA shall implement the authority granted herein in the following manner:

A. Pursuant to this Order, NSA shall only collect metadata as approved in Part II of the [REDACTED] Memorandum Opinion, as supplemented by the Supplemental Opinion and Amendment to Primary Order issued in the above-captioned docket on [REDACTED]

Entered this [REDACTED] day of [REDACTED] in Docket No. PR/TT [REDACTED]


JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET/COMINT/OC,NF~~

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

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

IN RE PROCEEDINGS REQUIRED BY § 702(i)
OF THE FISA AMENDMENTS ACT OF 2008

Docket Number: MISC 08-01

ORDER

IT IS HEREBY ORDERED that the Motion of the American Civil Liberties Union for Leave to Participate in Proceedings Required by Section 702(i) of the FISA Amendments Act of 2008 is DENIED, for the reasons set forth in the Memorandum Opinion issued on this date.

Mary A. McLaughlin
MARY A. McLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

August 27, 2008
DATE

Beverly C. Queen Deputy Clerk
FISC, certify that this document
is a true and correct copy of
the original. *BQ*

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

IN RE PROCEEDINGS REQUIRED BY § 702(i)
OF THE FISA AMENDMENTS ACT OF 2008

Docket Number: MISC 08-01

MEMORANDUM OPINION¹

This matter comes before the Court on the "Motion for Leave to Participate in Proceedings Required by § 702(i) of the FISA Amendments Act of 2008," filed by the American Civil Liberties Union ("ACLU") on July 10, 2008 ("ACLU motion"). In accordance with a scheduling order issued on July 17, 2008, the Government filed its "Opposition to the American Civil Liberties Union's Motion for Leave to Participate in Proceedings Required by § 702(i) of the FISA Amendments Act of 2008" on July 29, 2008. The ACLU filed a "Reply Memorandum in Support of Motion for Leave to Participate in Proceedings Required by § 702(i) of the FISA Amendments Act of 2008" on August 5, 2008. For the reasons described below, the Court denies the ACLU's motion.

BACKGROUND

Section 702 of the Foreign Intelligence Surveillance Act

In its motion, the ACLU seeks information about, and the opportunity to participate in, judicial proceedings required under Section 702(i) of the Foreign Intelligence Surveillance Act ("FISA"), as most recently amended by the FISA Amendments Act of 2008 ("FAA"), Pub L.

¹ The Government's filing in this case was unclassified; this opinion does not go beyond the factual assertions that were contained in the Government's filing.

No. 110-261, 122 Stat. 2436. Section 702 of FISA (codified at 50 U.S.C. § 1881a) specifies circumstances under which the Government can authorize the targeting of non-United States persons reasonably believed to be outside the United States, to acquire foreign intelligence information. The FAA imposes several limitations upon and requirements for the exercise of this authority.

Among other requirements, the FAA provides that “[t]he Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to – (A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and (B) 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.” 50 U.S.C. § 1881a(d)(1).

The FAA further provides that the Attorney General, again in consultation with the Director of National Intelligence, “shall adopt minimization procedures that meet the definition of minimization procedures under section 1801(h) or 1821(4) . . . as appropriate, for acquisitions authorized under subsection (a).” *Id.* § 1881a(e)(1).

Finally, the Attorney General and the Director of National Intelligence are required to submit to the Foreign Intelligence Surveillance Court (“FISC”) a written certification. Among other things, this certification must attest (1) that there are procedures in place that are reasonably designed to ensure that an acquisition authorized under subsection (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; (2) that the minimization procedures to be used with respect to such an acquisition meet the definition of minimization procedures under section 1801(h) or 1821(4) of FISA, as appropriate; and (3) that both the targeting and the minimization procedures either have been approved, have been submitted for approval, or will be submitted with the certification for approval by the FISC. Id. § 1881a(g)(2)(A)(i)-(ii).

Judicial Review under Section 702(i)

The FAA provides that the FISC shall have jurisdiction to review the certification, the targeting procedures and the minimization procedures. Id. § 1881a(i)(1)(A). As the ACLU notes in its motion, however, the Court's role here is "narrowly circumscribed." ACLU Mot. at 5. With respect to the certification, the FISC is merely to "determine whether the certification contains all the required elements." Id. § 1881a(i)(2)(A). The Court is to review the targeting procedures to "assess whether the procedures are reasonably designed to – (i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and (ii) 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." Id. § 1881a(i)(2)(B). As for the minimization procedures, the Court must "assess whether such procedures meet the definition of minimization procedures under section 1801(h) or section 1821(4) of this title, as appropriate." Id. § 1881a(i)(2)(C).

The FAA further provides that the FISC shall enter an order approving the certification and the use, or continued use, of the targeting and minimization procedures if the Court finds that

the certification contains all the required elements, and that the targeting and minimization procedures are consistent with the requirements of Sections 1881a(d)(1) and 1881a(e)(1) and "with the Fourth Amendment to the Constitution of the United States." Id. § 1881a(i)(3)(A). Should the Court conclude that it cannot make these findings, the Court shall either order the Government to correct any deficiency identified by the Court or cease or not begin implementation of the authorization for which the certification was submitted. Id. § 1881a(i)(3)(B).

The ACLU's Motion

In its motion, the ACLU requests:

- (1) that it be notified of the caption and briefing schedule for any proceedings under Section 702(i) in which this Court will consider legal questions relating to the scope, meaning and constitutionality of the FAA;
- (2) that, in connection with such proceedings, the Court require the Government to file public versions of its legal briefs, with only those redactions necessary to protect information that is properly classified;
- (3) that, in connection with such proceedings, the ACLU be granted leave to file a legal brief addressing the constitutionality of the FAA and to participate in oral argument before the Court; and
- (4) that any legal opinions issued by the Court at the conclusion of such proceedings be made available to the public, with only those redactions necessary to protect information that is properly classified.

ACLU Mot. at 2. The relief sought by the ACLU can be viewed as falling into two categories, which to a certain degree overlap: (1) a request for the release of records (i.e., any legal briefs filed by the Government and legal opinions issued by the Court in connection to § 702(i) proceedings) similar to that which was considered by this court last year in In re Motion for Release of Court Records, 526 F. Supp. 2d 484 (Foreign Intel. Surv. Ct. 2007); and (2) a more general request to participate in the Court's review under § 702(i) (i.e., to be granted leave to file a legal brief and to participate in oral argument). The ACLU's request to be notified of the

caption and briefing schedule of particular proceedings under § 702(i) is a bit of a hybrid; it is in effect a request for release of records, made in order to facilitate the ACLU's participation in the matter.

1. The ACLU's Request for the Release of Records

The ACLU's request is similar to a request it made on August 9, 2007. At that time, the ACLU filed a motion with the FISC seeking the release of what it identified as court orders and Government pleadings regarding a surveillance program conducted by the National Security Agency. The court denied the motion, finding (1) that the common law provided no public right of access to the requested records; and (2) that the First Amendment provided no public right of access to the requested records. In re Motion for Release of Court Records, 526 F. Supp. 2d at 490-497. The court further declined to exercise any "residual discretion," should it exist, to release any portions of the records at issue, Id. at 497.

Although the records sought by the ACLU in the present motion are different from those it requested in 2007, this Court finds no reason to reach a different conclusion. These records also are to be maintained under the comprehensive statutory scheme described by Judge Bates in In re Motion for Release of Court Records as "designed to protect FISC records from routine public disclosure" and found to supercede any common law right of access. Id. at 491.

Nor is there a First Amendment right of access to the records. Application of the "experience and logic" tests adopted by the Supreme Court for assessing the existence of a qualified First Amendment right of access in Press-Enterprise Co. v. Superior Court, 478 U.S. 1

(1986) (Press-Enterprise II) confirms that there is no such right of access to these documents.² First, the “experience” test is not satisfied because neither the “place” nor the “process” has “historically been open to the press and general public.” Id. at 8. The FISC has no tradition of openness, either with respect to its proceedings, its orders, or to Government briefings filed with the FISC. See In re Motion for Release of Court Records, 526 F. Supp. 2d at 492. Moreover, the specific process at issue here, proceedings under Section 702(i) of the FAA, is brand-new, and therefore cannot be said to have such a tradition.

Under Press-Enterprise II, the failure to satisfy the “experience” test alone defeats a claim for a First Amendment right of access. 478 U.S. at 9. See also In Re Motion for Release of Court Records, 526 F. Supp. 2d at 493. But should the “logic” test even apply in this case, it is not satisfied because public access to these documents will not play a significant positive role in the functioning of the FISA process. The Government asserts that its certification, targeting procedures, and minimization procedures will provide the details of its sources and methods for collecting foreign intelligence information under the FAA and therefore will be classified. Gov’t. Opp’n at 8. The ACLU responds that it is not seeking access to “properly classified information,” ACLU Reply at 1, but contends that the Court should determine whether the Government’s procedures are “properly” classified. Id. at 7.

² “First, because a tradition of accessibility implies the favorable judgment of experiences, we have considered whether the place and process have historically been open to the press and general public.” Press-Enterprise II, 478 U.S. at 8 (citations and internal quotation marks omitted). “Second, in this setting the Court has traditionally considered whether public access plays a significant positive role in the functioning of the particular process in question.” Id. “If the particular proceeding in question passes these tests of experience and logic, a qualified First Amendment right of public access attaches.” Id. at 9.

Assuming, arguendo, that the Court does have the authority to undertake this type of inquiry, the "logic" test would still not be satisfied. Absent the Government's wholesale abuse of classification authority, which there is no reason to presume here, any disclosure resulting from such a review can be expected to be limited and incremental in nature. The fact that at most, only partial access to the documents could be provided undercuts the ACLU's ability to satisfy the "logic" test. As with the records at issue in In re Motion for Release of Court Records, "[t]he benefits from a partial release of declassified portions of the requested materials would be diminished, insofar as release with redactions may confuse or obscure, rather than illuminate, the decisions in question." 526 F. Supp. 2d at 495. Moreover, such a review could result in the release of information that should have remained classified.

Although it is possible to identify some benefits which might flow from public access to Government briefs and FISC orders related to Section 702(i) proceedings, the "logic" test is not satisfied because any such benefits would be outweighed by the risks to national security created by the potential exposure of the Government's targeting and minimization procedures. In short, the proceedings in Section 702(i) seem to be of the type "that would be totally frustrated if conducted openly." Press-Enterprise II, 478 U.S. at 8-9.

In the alternative, the ACLU contends that the Court should exercise its discretion to grant the relief it requests because the FAA has "sweeping implications for the rights of U.S. citizens and residents," ACLU Reply at 7, and the Section 702(i) proceedings "should be adversarial and as informed and transparent as possible," ACLU Mot. at 9. Assuming that such discretion resides with the Court, it declines to exercise that authority here. Providing the ACLU with access to the materials provided to the FISC in connection with the Section 702(i) review, and with the Court's assessment of the Government submissions, would create risks to national

security that far outweigh any potential benefit to be gained by providing the ACLU with access to the requested records.³

2. The ACLU's Request to Participate in Section 702(j) Proceedings before the FISC

The ACLU also seeks leave, in connection with proceedings under Section 702(i), to file a legal brief addressing the constitutionality of the FAA, and to participate in oral argument before the Court. The Court denies this request as well. First, the ACLU has no right to such participation. The FAA does not provide for such participation by a party other than the Government. Second, assuming that the Court has the discretion to allow such participation, it declines to do so. For the reasons described below, the ACLU's participation is unlikely to provide meaningful assistance to the Court.

First, the FAA itself does not provide for participation by a party other than the Government in the Court's review of the Government's certification and procedures. In fact, it provides that only the Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of the Court's order resulting from its review of the certification and procedures. 50 U.S.C. § 1881a(i)(4)(A). By contrast, Section 702(h) explicitly provides for the participation of parties other than the Government, in that electronic communication service providers can bring a challenge in the FISC to directives issued to them under the FAA. Id.

³ Even in a context where a criminal defendant's Sixth Amendment rights are at issue, FISA provides that materials may be disclosed to the aggrieved person "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f) (emphasis added). As Section 702(i) does not include a similar mechanism for disclosing materials when deemed necessary to the Court's review, the Court will decline to disclose such materials in this case, when it believes that disclosure is not only unnecessary to the Court's determination but also unlikely to be useful, for the reasons discussed below.

§ 1881a(h)(4). The FAA also expressly gives these providers a right to appeal. Id.

§ 1881a(h)(6).

In addition, even before the enactment of the FAA, Congress provided for the participation of parties other than the Government in the limited context of providing a right of challenge in the FISC to those receiving orders for the production of tangible things pursuant to 50 U.S.C. § 1861. Id. § 1861(f)(2). The lack of analogous provisions for proceedings under Section 702(i) strongly suggests that Congress did not contemplate the Court's review of the certification and procedures to be anything other than an ex parte proceeding.

Second, as described above, the Court's review under Section 702(i) is limited to three specific components: the certification, the targeting procedures and the minimization procedures. The Court's review of the certification is limited to determining whether the certification contains all of the elements required by the statute. As to the targeting procedures adopted by the Government, the Court must review the procedures to "assess whether the procedures are reasonably designed to – (i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and (ii) 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." 50 U.S.C. § 1881a(i)(2)(B). As to the minimization procedures, the Court must "assess whether such procedures meet the definition of minimization procedures under section 1801(h) or section 1821(4) of this title, as appropriate." Id. § 1881a(i)(2)(C). Finally, the Court must decide whether the targeting and minimization procedures are consistent with the Fourth Amendment. Id. § 1881a(i)(3)(A).

As described above, the Government states that its targeting and minimization procedures will be classified because they provide the details of its sources and methods for collecting foreign intelligence information. The ACLU, therefore, will not have access to either set of procedures. Without such access, it cannot provide meaningful input to the Court on the compliance of those procedures with the FAA or the Fourth Amendment.

The ACLU suggests that judicial review under Section 702(i) will necessarily include review of the constitutionality of the FAA, and the ACLU's input would be helpful in such a constitutional analysis. Such a generalized constitutional review, however, is not contemplated under Section 702(i). The Court is required to consider whether the targeting and minimization procedures adopted by the Government meet the requirements of the statute and whether those procedures are consistent with the Fourth Amendment. The Court is not required, in the course of this Section 702(i) review, to reach beyond the Government's procedures and conduct a facial review of the constitutionality of the statute. Accordingly, the ACLU's participation in Section 702(i) proceedings will not assist the Court.

CONCLUSION

For all the reasons set forth above, the motion of the ACLU for leave to participate in proceedings required by § 702(i) of the FISA Amendments Act of 2008 is denied. A separate order has been issued.

Mary A. McLaughlin
MARY A. McLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

August 27, 2008
DATE

Dorothy C. Queen Deputy Clerk
FISC, certify that this document
is a true and correct copy of
the original. *389*

~~SECRET//NOFORN~~

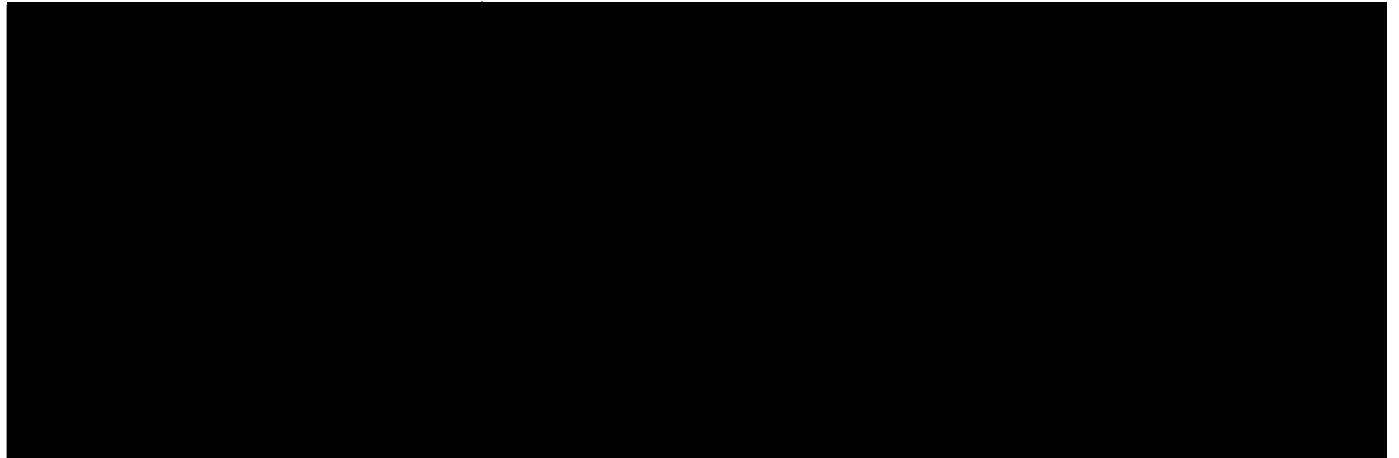
2014

UNITED STATES

U.S. Foreign Intelligence
Surveillance Court

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.



OPINION ON MOTION FOR DISCLOSURE OF PRIOR DECISIONS

On [REDACTED] 2014, [REDACTED]

“Motion for Disclosure of Prior Decisions” (“Motion for Disclosure”). The Court denied this Motion on the record at the adversary hearing held on the underlying matter on [REDACTED] 2014. It writes this Opinion to explain its reasoning.

I. BACKGROUND

This case came before the Court on the Government’s “Petition for an Order to Compel Compliance with Directives of the Director of National Intelligence and Attorney General,” submitted on [REDACTED] 2014 (“Petition”). The directives that the Government is seeking to

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

enforce were issued pursuant to Section 702(h)(1) of the Foreign Intelligence Surveillance Act, as amended (FISA)¹ and served on [REDACTED]

Pursuant to a schedule set by order of the Court on [REDACTED] 2014, [REDACTED]

[REDACTED] (“Response”) on [REDACTED] 2014, [REDACTED]

[REDACTED] (collectively

“Reply”) on [REDACTED] 2014.² In its Reply, the Government repeatedly cited and quoted two

opinions of the FISC that do not appear to have been made public in any form: one issued on

September 4, 2008, [REDACTED] and the other issued on August 26, 2014, [REDACTED]

[REDACTED] (hereinafter “the Requested Opinions”).

Both of the Requested Opinions resulted from the FISC’s ex parte review of certifications and attendant targeting and minimization procedures pursuant to Section 702(i). The August 26,

2014 opinion approved the certifications and procedures now in effect, and the directives [REDACTED]

[REDACTED] pursuant to those certifications. The

September 4, 2008 opinion approved [REDACTED] certifications and procedures.

¹ FISA is codified at 50 U.S.C. §§ 1801-1885c, within which Section 702 appears at § 1881a.

² [REDACTED]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

[REDACTED] Motion for Disclosure, in which it sought “immediate access to [the Requested Opinions] (in appropriately redacted form) to adequately prepare for the hearing scheduled for [REDACTED] th.” Motion for Disclosure at 1.³ Pursuant to the Court’s scheduling order of [REDACTED] 2014, the Government submitted its opposition to the Motion for Disclosure (“Opposition”) on [REDACTED] 2014.

II. DISCUSSION

As explained below, the Court concluded that neither FISA nor the Foreign Intelligence Surveillance Court (FISC) Rules of Procedure (“FISC Rules”) require, or provide for discretionary, disclosure of the Requested Opinions in the circumstances of this case. Similarly, the Due Process Clause of the Fifth Amendment does not compel the requested disclosure and, assuming that the Court has some discretion on this matter, no prudential considerations counsel otherwise.

A. FISA and the FISC Rules

The cases handled by the FISC involve classified intelligence gathering operations. From a security perspective, FISC operations “are governed by FISA, by Court rule,^[4] and by statutorily mandated security procedures issued by the Chief Justice of the United States.

[REDACTED] its counsel has a Top Secret security clearance [REDACTED] seeking access to the Requested Opinions with any redactions necessary to downgrade the Requested Opinions to a Top Secret, non-compartmented level.

⁴ The FISC explicitly has the authority to establish rules for its proceedings under 50 U.S.C. § 1803(g)(1).

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Together, they represent a comprehensive scheme for the safeguarding and handling of FISC proceedings and records.” In re Motion for Release of Court Records, 526 F. Supp.2d 484, 488 (FISA Ct. 2007).

Specifically applicable to this case is the requirement that, in any proceeding under Section 702, “the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.” 50 U.S.C. § 1881a(k)(2). The FISC Rules reiterate this statutory requirement and further provide: “Except as otherwise ordered, if the government files ex parte a submission that contains classified information, the government must file and serve on the non-governmental party an unclassified or redacted version. The unclassified or redacted version, at a minimum, must clearly articulate the government’s legal arguments.” FISC Rule 7(j).

FISC Rule 3 provides: “In all matters, the Court and its staff shall comply with . . . Executive Order 13526, ‘Classified National Security Information’ (or its successor).” Under that executive order, a person may be given access to classified information only if

- (1) a favorable determination of eligibility for access has been made by an agency head or the agency head’s designee;
- (2) the person has signed an approved nondisclosure agreement; and
- (3) the person has a need-to-know the information.

Executive Order 13526 § 4.1(a). “Need-to-know” is defined as “a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.” Id. § 6.1(dd) (emphasis added).

B. Analysis

The Court has reviewed the redacted copies of the Government’s Reply (to include the supporting affidavit) and finds that it clearly articulates the Government’s legal arguments.

[REDACTED] without the Requested Decisions, it “cannot adequately understand the guidance, and limitations thereof, that this Court has previously issued.” Motion for Disclosure at 1. The Government responds that the Requested Opinions do not bear on the application of its targeting and minimization procedures [REDACTED]

[REDACTED] further contends that its counsel “has a ‘need to know’ with regard to the prior relevant caselaw.” Motion for Disclosure at 1.

The government retorts [REDACTED] does not have a need-to-know more about the contents of the Requested Decisions. Opposition at 3.

The Court has carefully reviewed the Requested Opinions in the context of the issues presented by the Petition⁵ and the parties’ respective arguments on those issues and compared the citations to and quotations from the Requested Opinions that appear in the Government’s Reply to the underlying texts. In no instance does the Reply quote or reference the Requested Opinions

⁵ [REDACTED] “to comply with [each] directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of [Section 702] and is otherwise lawful.” 50 U.S.C. § 1881a(h)(5)(C).

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

in a manner that is incomplete, wrenched from necessary context or otherwise misleading with regard to the point being addressed. Based on that review, the Court finds that the Requested Opinions would be of little, if any, assistance to [REDACTED] arguments it makes on the merits.⁶

Given that FISC Rule 3 requires the Court to follow the Executive Order, the Court will not lightly second-guess the Government's need-to-know determination, which the Executive Order specifically commits to the Executive Branch. Moreover, there is no indication that the Government is exploiting the need-to-know requirement to mislead or otherwise gain a strategic advantage [REDACTED]

[REDACTED] For these reasons, the Court concludes [REDACTED] does not have the requisite need-to-know the requested information.

Other aspects of the Section 702 framework support [REDACTED] [REDACTED] not entitled to access to the Requested Opinions. The statute and the FISC Rules provide detailed guidance for the conduct of proceedings initiated by a petition to compel compliance with, or to modify or set aside, a Section 702 directive, see 50 U.S.C. § 1881a(h); FISC Rules 20-31, but they provide no mechanism for the recipient of a directive to seek discovery or disclosure of classified information. They do provide for nondisclosure in the

⁶ The Court finds that this would especially be the case once compartmented information was redacted from the Requested Opinions.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

context of the FISC's ex parte review of certifications and accompanying procedures. See 50 U.S.C. § 1881a(g)(1)(A); FISC Rule 30.⁷ In the context of a petition to compel compliance with (or to modify or set aside) a directive, in fact, FISA and Rule 7(j) provide just the opposite, i.e., they permit the Government to withhold classified information from the recipient of the directive. See 50 U.S.C. § 1881a(k)(2); FISC Rule 7(j).⁸

Finally, the statute provides a 30-day period for the completion of FISC review of the Petition in this case. See § 1881a(h)(5)(C). That 30-day period ends on [REDACTED] 2014, a deadline that is incompatible, as a practical matter, with the Government's making redactions of the Requested Opinions for disclosure [REDACTED] and

⁷ For the most part, the Requested Opinions pertain to classified material that the Government submitted under seal, as required by 50 U.S.C. § 1881a(g)(1)(A), for ex parte and in camera review under § 1881a(i). In a prior case, the FISC observed that "the Congressional judgment embodied" in a comparable statutory provision for ex parte review of procedures suggested that the FISC "should not lightly override the government's opposition to the release of" a classified FISC opinion containing classified information that "directly relates to what the government [previously] submitted for ex parte and in camera review." [REDACTED] Order issued on [REDACTED] 2008, at 2 n.2. The same logic is applicable here.

⁸ Moreover, the detailed statutory provisions regarding FISC proceedings under Section 702 do not provide for [REDACTED] disclosure of opinions arising from the Court's ex parte review of Section 702 certifications and procedures. Section 702 makes clear that, in the ordinary course, the FISC will have reviewed and approved a certification and accompanying procedures prior to the issuance of a directive pursuant to that certification. See 50 U.S.C. § 1881a(a), (g)(1)(A), (h)(1), (i)(3). If Congress had thought access to such prior FISC opinions were necessary for the recipient of a directive to challenge its lawfulness, it could have provided for such access.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

consideration of whatever additional argument such counsel would make after reviewing the Requested Opinions.⁹

C. Due Process

In its Motion for Disclosure [REDACTED]

presents no argument and cites no authority for its suggestion that due process requires the requested disclosure. Motion for Disclosure at 1-2. The weight of authority indicates otherwise. For example, with respect to challenges to the lawfulness of electronic surveillance brought by an aggrieved person,¹⁰ the district court is required to review the application, order, and other materials relating to the electronic surveillance in camera and ex parte if “the Attorney General files an affidavit under oath that disclosure . . . would harm the national security.” 50 U.S.C. § 1806(f). Such materials bear directly on any claim that a surveillance was unlawful; nevertheless, disclosure may only occur – even a partial disclosure “under appropriate security procedures and protective orders” – “where such disclosure is necessary to make an accurate

⁹ The Court may extend that 30-day period “as necessary for good cause and in a manner consistent with national security,” § 1881a(j)(2), but [REDACTED] not shown good cause to delay the proceeding to accommodate the requested disclosure. Moreover, [REDACTED]

[REDACTED] it is doubtful that delaying resolution of the lawfulness of the Directives would be consistent with national security.

¹⁰ “Aggrieved person” is defined as “a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” 50 U.S.C. § 1801(k).

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

determination of the legality of the surveillance,” when the court has found that the surveillance was unlawful or “to the extent that due process requires discovery or disclosure.” § 1806(f), (g). Courts have found non-disclosure of surveillance materials under these provisions to comport with due process, see, e.g., United States v. El-Mezain, 664 F.3d 467, 567-68 (5th Cir. 2011); United States v. Abu-Jihaad, 630 F.3d 102, 129 (2d Cir. 2010); United States v. Damrah, 412 F.3d 618, 623-24 (6th Cir. 2005), even when the attorneys seeking access have security clearances. See United States v. Ott, 827 F.2d 473, 476-77 (9th Cir. 1987). [REDACTED] presented no reason to reach a different conclusion here.

Beyond what is compelled by the Due Process Clause, the Court is satisfied that withholding the Requested Opinions does not violate common-sense fairness. As stated above, each quotation or reference to the Requested Opinions in the Government’s Reply fairly represents what those opinions say on the discrete point addressed. And the Government properly adduced each of those points in reply to [REDACTED] Response. In these circumstances, the Court would decline to compel disclosure of the Requested Opinions as a matter of discretion, assuming for the sake of argument that indeed the Court would have discretion to compel disclosure in a proper case.

//

//

//

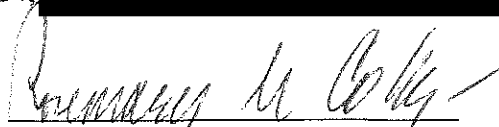
//

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

* * *

[REDACTED] Motion for Disclosure was DENIED.¹¹
ISSUED this [REDACTED] 2014, [REDACTED]


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

¹¹ Because the Court finds no basis to conclude that the Government is improperly withholding the Requested Decisions, [REDACTED] “to ask the government to show cause why these decisions should not be provided” and to “strike any portions of pleadings that refer to materials that have not been provided [REDACTED] in appropriately redacted form,” see Motion for Disclosure at 1 n.2, is also denied.

~~SECRET//NOFORN~~

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

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

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Docket Number: BR 14-96

MEMORANDUM OPINION

The Court has today issued the Primary Order appended hereto granting the
"Application of the Federal Bureau of Investigation for an Order Requiring the

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

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

Production of Tangible Things" ("Application" or "the instant Application"), which was submitted to the Court on June 19, 2014, by the Federal Bureau of Investigation ("FBI"). The Application requested the issuance of orders pursuant to 50 U.S.C. §1861, as amended (also known as Section 215 of the USA PATRIOT Act), requiring the ongoing daily production to the National Security Agency ("NSA") of certain telephone call detail records in bulk ("bulk telephony metadata").

On August 29, 2013, Judge Claire V. Eagan of this Court issued an Amended Memorandum Opinion in Docket Number BR 13-109, offering sound reasons for authorizing an application for orders requiring the production of bulk telephony metadata ("August 29 Opinion"). On September 17, 2013, following a declassification review by the Executive Branch, the Court published its redacted August 29 Opinion and the Primary Order issued in Docket Number BR 13-109. On October 11, 2013, Judge Mary A. McLaughlin of this Court granted the FBI's application to renew the authorities approved in Docket Number BR 13-109, issued a Memorandum adopting Judge Eagan's statutory and constitutional analyses, and provided additional analysis on whether the production of bulk telephony metadata violates the Fourth Amendment ("October 11 Opinion"). Both judges of this Court held that the compelled production of such records does not constitute a search under the Fourth Amendment. Judge

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

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

McLaughlin further found that the Supreme Court's decision in United v. Jones, __ U.S. __, 132 S. Ct. 945 (2012) neither mandates nor supports a different conclusion.

Following a declassification review by the Executive Branch, the Court published the October 11 Opinion and the Primary Order issued in Docket Number BR 13-158 in redacted form a week later on October 18, 2013. Since the date of Judge McLaughlin's re-authorization of the bulk telephony metadata collection in Docket Number BR 13-158, the government has sought on three occasions renewed authority for this collection. The Court has approved those applications in Docket Numbers BR 14-01 (on January 3, 2014), BR 14-67 (on March 28, 2014), and the instant Application.

In approving the instant Application, I fully agree with and adopt the constitutional and statutory analyses contained in the August 29 Opinion and the October 11 Memorandum. In particular, with respect to the constitutional analysis, I concur with Judges Eagan and McLaughlin that under the controlling precedent of *Smith v. Maryland*, 442 U.S. 735 (1979), the production of call detail records in this matter does not constitute a search under the Fourth Amendment. With respect to the statutory requirements for the issuance of orders for the collection of bulk telephony metadata, I adopt the analysis put forth by Judge Eagan in her August 29 Opinion, and in particular, I note her discussion on the issue of relevance:

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

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

The government must demonstrate "facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." 50 U.S.C. 1861(b)(2)(A). The fact that international terrorist operatives are using telephone communications, and that it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, is sufficient to meet the low statutory hurdle set out in Section 215 to obtain a production of records. Furthermore, it is important to remember that the relevance finding is only one part of a whole protective statutory scheme. Within the whole of this particular statutory scheme, the low relevance standard is counter-balanced by significant post-production minimization procedures that must accompany such an authorization and an available mechanism for an adversarial challenge in this Court by the record holder. [...] Without the minimization procedures set out in detail in this Court's Primary Order, for example, no Orders for production would issue from this Court. See Primary Ord. at 4-17. Taken together, the Section 215 provisions are designed to permit the government wide latitude to seek the information it needs to meet its national security responsibilities, but only in combination with specific procedures for the protection of U.S. person information that are tailored to the production and with an opportunity for the authorization to be challenged. The Application before this Court fits comfortably within this statutory framework.

August 29 Opinion at 22-23.

Since the issuance of the August 29 Opinion and October 11 Memorandum, there have been changes to the minimization procedures applied to the bulk telephony metadata collection. These were requested by the government and approved by this Court. Moreover, the legality of the bulk telephony metadata collection has been challenged in litigation throughout the country and considered by four U.S. District

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

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

Court judges. Lastly, on December 18, 2013, in an order entered in BR 13-158, Judge McLaughlin granted leave to the Center for National Security Studies ("the Center") to file an *amicus curiae* brief on why 50 U.S.C. §1861 does not authorize the collection of telephony metadata records in bulk. The Center filed its *amicus* brief on April 3, 2014, after the most recent authorization of this collection in Docket Number BR 14-67. Prior to making a decision to grant the instant Application, I considered each of these developments, which I briefly note below.

Changes to Minimization Procedures

Pursuant to 50 U.S.C. §1861(g), the bulk telephony metadata collected pursuant to orders granting the instant Application, as well as all predecessor applications, are subject to minimization procedures. The statutory requirements for minimization procedures under 50 U.S.C. §1861(g) are discussed in the August 29 Opinion. August 29 Opinion at 11. On February 5, 2014, the Court granted the government's Motion for Amendment to Primary Order in Docket Number BR 14-01, which amended the minimization procedures required by the Primary Order in that case in two significant respects. First, the amended procedures preclude the government (except in emergency circumstances) from querying the bulk telephony metadata without first having

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

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

obtained, by motion, a determination from this Court that reasonable, articulable suspicion (RAS) exists to believe that the selection term (e.g., a telephone number) to be used for querying is associated with an international terrorist organization named in the Primary Order requiring the production of the bulk telephony metadata.¹ Second, the amended procedures require that queries of the bulk telephony metadata be limited so as to identify only that metadata found within two "hops" of an approved selection term.² The government has requested, and the Court has approved, the same limitations in orders accompanying the two subsequent applications for this collection filed with this Court (i.e., Docket Number BR 14-67 and the instant Application).

On February 25, 2014, the government filed a Motion for Second Amendment to Primary Order in Docket Number BR 14-01, through which it sought further to modify the minimization procedures ("February 25 Motion"). Specifically, the government sought relief from the requirement that it destroy bulk telephony metadata after five

¹ Previously, the minimization procedures allowed for this RAS determination to be made by one of a limited set of high-ranking NSA personnel.

² The first "hop" would include metadata associated with the set of numbers directly in contact with the approved selection term, and the second "hop" would include metadata associated with the set of numbers directly in contact with the first "hop" numbers. Previously, the minimization procedures allowed the government to query the bulk telephony metadata to identify metadata within three "hops" of an approved selection term.

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

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

years, based on the government's common law preservation obligations in pending civil litigation. In seeking relief from the five-year destruction requirement, the government proposed a number of additional restrictions on access to and use of the data, all designed to ensure that collected metadata that was more than five years old could only be used for the relevant civil litigation purposes. Although this Court initially denied the February 25 Motion without prejudice, the Court granted a second motion for the same relief on March 12, 2014 ("March 12 Order and Opinion"), that the government sought in order to comply with a preservation order that had been issued by the U.S. District Court for the Northern District of California after this Court's denial of the February 25 Motion. The March 12 Order and Opinion required that the bulk telephony metadata otherwise required to be destroyed under the five year limitation on retention be preserved and/or stored "[p]ending resolution of the preservation issues raised . . . before the United States District Court for the Northern District of California[.]" March 12 Opinion and Order at 6. The March 12 Order and Opinion prohibited NSA intelligence analysts from accessing or using such data for any purpose; permitted NSA personnel to access the data only for the purpose of ensuring continued compliance with the government's preservation obligations; and prohibited any further accesses of BR metadata for civil litigation purposes without prior written notice to this Court. *Id.*

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

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

at 6-7. Finally, the March 12 Opinion and Order required the government promptly to notify this Court of any additional material developments in civil litigation pertaining to the BR metadata, including the resolution of the preservation issues in the proceedings in the Northern District of California. *Id.* at 7. The preservation issues raised in the Northern District of California have not yet been resolved. As a result, the government has requested and the Court has approved the same exemption from the five year limitation on retention, subject to the same restrictions on access and use, in Docket Number BR 14-67 and the instant Application.

Prior to deciding whether to re-authorize the bulk telephony metadata collection through the appended Primary Order, I considered with care the stated changes to the minimization procedures. As described, the first set of changes approved in the February 5 Order provide enhanced protections for the bulk telephony metadata. While the March 12 Opinion and Order allows the government to retain bulk telephony metadata beyond five years, it allows the government to do so for the sole purpose of meeting preservation obligations in civil litigation pending against it.

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

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

U.S. District Court Cases

In recent months, the legality of the bulk telephony metadata collection has been challenged on both statutory and constitutional grounds in proceedings throughout the country, and four U.S. District Court judges have issued opinions on these challenges.

Smith v. Obama, No. 2:13-CV-257-BLW, 2014 WL 2506421 (D. Idaho June 3, 2014);

A.C.L.U. v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); *Klayman v. Obama*, 957 F. Supp.

2d 1 (D.D.C. 2013); and *U.S. v. Moalin*, No. 10cr4246 JM, 2013 WL 6079518 (S.D. Cal.

November 18, 2013). In three of the four cases in which judges have issued opinions (i.e., all but the *Klayman* case), they have rejected plaintiffs' challenges to this collection.

In particular, with respect to Fourth Amendment challenges raised by plaintiffs, the judges in *Smith*, *Clapper* and *Moalin* recognized that the Supreme Court's decision in

Smith v. Maryland is controlling and does not support a finding that the bulk telephony metadata collection is a violation of the Fourth Amendment.

In *Klayman*, Judge Richard J. Leon of the U.S. District Court for the District of Columbia alone held that the plaintiffs were likely to succeed on their claim that the bulk telephony metadata collection was an unreasonable search under the Fourth Amendment. *Klayman*, 957 F. Supp. 2d at 41. Judge Leon ordered the government to

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

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

cease collection of any telephony metadata associated with [the plaintiffs'] personal Verizon accounts" and destroy any such metadata in its possession, but he stayed the order pending appeal. *Id.* at 43.

On January 22, 2014, a recipient of a production order in Docket Number BR 14-01 filed a Petition ("January 22 Petition") pursuant to 50 U.S.C. § 1861(f)(2)(A) and Rule 33 of the Foreign Intelligence Surveillance Court ("FISC") Rules of Procedure, asking this Court "to vacate, modify, or reaffirm" the production order issued to it.³ According to the Petitioner, the Petition arose "entirely from the effect on [the recipient] of Judge Leon's Memorandum [Opinion]," and specifically, that Judge's conclusion that the Supreme Court's decision in *Smith v. Maryland* is "inapplicable to the specific activities mandated by the [Section] 1861 order at issue in the *Klayman* litigation." January 22 Petition at 3-4. Pursuant to the requirements of 50 U.S.C. § 1861(f), Judge Rosemary M. Collyer of this Court issued an Opinion and Order on March 20, 2014 ("March 20 Opinion and Order"), finding that the Petition provided no basis for vacating or

³ Following a declassification review by the Executive Branch, the Court published the January 22 Petition filed in Docket Number BR 14-01 in redacted form on April 25, 2014.

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

modifying the relevant production order issued in Docket Number BR 14-01.⁴ In her March 20 Opinion and Order, Judge Collyer engaged in an extensive analysis of Judge Leon's opinion in *Klayman*, ultimately disagreeing with his conclusion that *Smith v. Maryland* is inapplicable to the collection of bulk telephony metadata.

In issuing the Primary Order appended hereto which re-authorizes the bulk telephony metadata collection, I have carefully examined the noted U.S. District Court opinions, and I agree with Judge Collyer's analysis and opinion of the *Klayman* holding.

Amicus Curiae Brief

On April 3, 2014, the Center for National Security Studies filed an *amicus curiae* brief explaining why it believes that 50 U.S.C. §1861 does not authorize the collection of bulk telephony metadata. The *amicus* brief made a number of thoughtful points, the merits of which I have analyzed. Notwithstanding the Center's arguments, I find the authority requested by the FBI through the instant Application meets the requirements of the statute, and that the collection of bulk telephony metadata may be authorized under the terms of the statute.

⁴ Following a declassification review by the Executive Branch, the Court published the March 20 Opinion and Order issued in Docket Number BR 14-01 in redacted form on April 25, 2014.

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

Conclusion

The unauthorized disclosure of the bulk telephony metadata collection more than a year ago led to many written and oral expressions of opinions about the legality of collecting telephony metadata. Congress is well aware that this Court has interpreted the provisions of 50 U.S.C. § 1861 to permit this particular collection, and diverse views about the collection have been expressed by individual members of Congress. In recent months, Congress has contemplated a number of changes to the Foreign Intelligence Surveillance Act, a few of which would specifically prohibit this collection. Congress could enact statutory changes that would prohibit this collection going forward, but under the existing statutory framework, I find that the requested authority for the collection of bulk telephony metadata should be granted. Courts must follow the law as it stands until the Congress or the Supreme Court changes it.

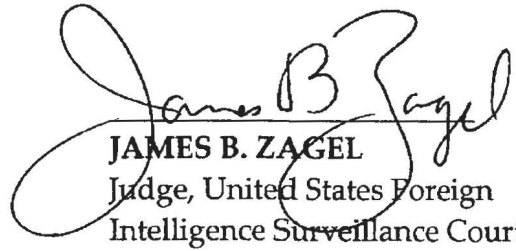
In light of the public interest in this particular collection and the government's declassification of related materials, including substantial portions of Judge Eagan's August 29 Opinion, Judge McLaughlin's October 11 Memorandum, and Judge Collyer's March 20 Opinion and Order, I request pursuant to FISC Rule 62 that this Memorandum Opinion and Accompanying Primary Order also be published, and I

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

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

direct such request to the Presiding Judge as required by the Rule.

ENTERED this 19th day of June, 2014.


JAMES B. ZAGEL
Judge, United States Foreign
Intelligence Surveillance Court

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

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

amended, requiring the production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:¹

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or

¹ The Honorable Rosemary M. Collyer issued an Opinion and Order finding that, under *Smith v. Maryland*, 442 U.S. 735 (1979), this bulk production of non-content call detail records does not involve a search or seizure under the Fourth Amendment. See FISC docket no. BR 14-01, Opinion and Order issued on March 20, 2014 (under seal and pending consideration for unsealing, declassification, and release). This authorization relies on that analysis of the Fourth Amendment issue. In addition, the Court has carefully considered opinions issued by Judges Eagan and McLaughlin in docket numbers BR 13-109 and BR 13-158, respectively, as well as the decision in *Smith v. Obama*, No. 2:13-CV-257-BLW, 2014 WL 2506421 (D. Idaho June 3, 2014), *American Civil Liberties Union v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. Dec. 27, 2013), *Klayman v. Obama*, 957 F.Supp.2d 1 (D.D.C. 2013), *U.S. v. Moalin*, No. 10cr4246 JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013), and the Brief of Amicus Curiae for Center for National Security Studies on the Lack of Statutory Authority for this Court's Bulk Telephony Metadata Orders, Misc. 14-01 (FISC filed Apr. 3, 2014), available at <http://www.fisc.uscourts.gov/sites/default/files/Misc%2014-01%20Brief-1.pdf>.

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

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

tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number BR 14-67 and its predecessors. [50 U.S.C. § 1861(c)(1)]

Accordingly, and as further explained in the accompanying Memorandum Opinion, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"² created by [REDACTED].

² For purposes of this Order "telephony metadata" includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI))

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

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

B. The Custodian of Records of [REDACTED]

[REDACTED]
[REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by [REDACTED] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [REDACTED]
[REDACTED]
[REDACTED]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives or has received as a result of this Order or predecessor Orders of this Court requiring the production to NSA of

number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer. Furthermore, this Order does not authorize the production of cell site location information (CSLI).

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

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

telephony metadata pursuant to 50 U.S.C. § 1861, NSA shall strictly adhere to the minimization procedures set out at subparagraphs A. through G. below; provided, however, that the Government may take such actions as are permitted by the Opinion and Order of this Court issued on March 12, 2014, in docket number BR 14-01, subject to the conditions and requirements stated therein, including the requirement to notify this Court promptly of any material developments in civil litigation pertaining to such telephony metadata.

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.³ The BR metadata shall carry unique markings such that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to

³ The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

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

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

authorized personnel who have received appropriate and adequate training.⁴

Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms⁵ that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes, but the results of any such queries will not be used for intelligence analysis purposes.

An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with

⁴ The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.

⁵



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

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

authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. The government may request, by motion and on a case-by-case basis, permission from the Court for NSA⁶ to use specific selection terms that satisfy the reasonable articulable suspicion (RAS) standard⁷ as "seeds" to query the BR metadata

⁶ For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.


⁷ The reasonable articulable suspicion standard is met when, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [REDACTED]

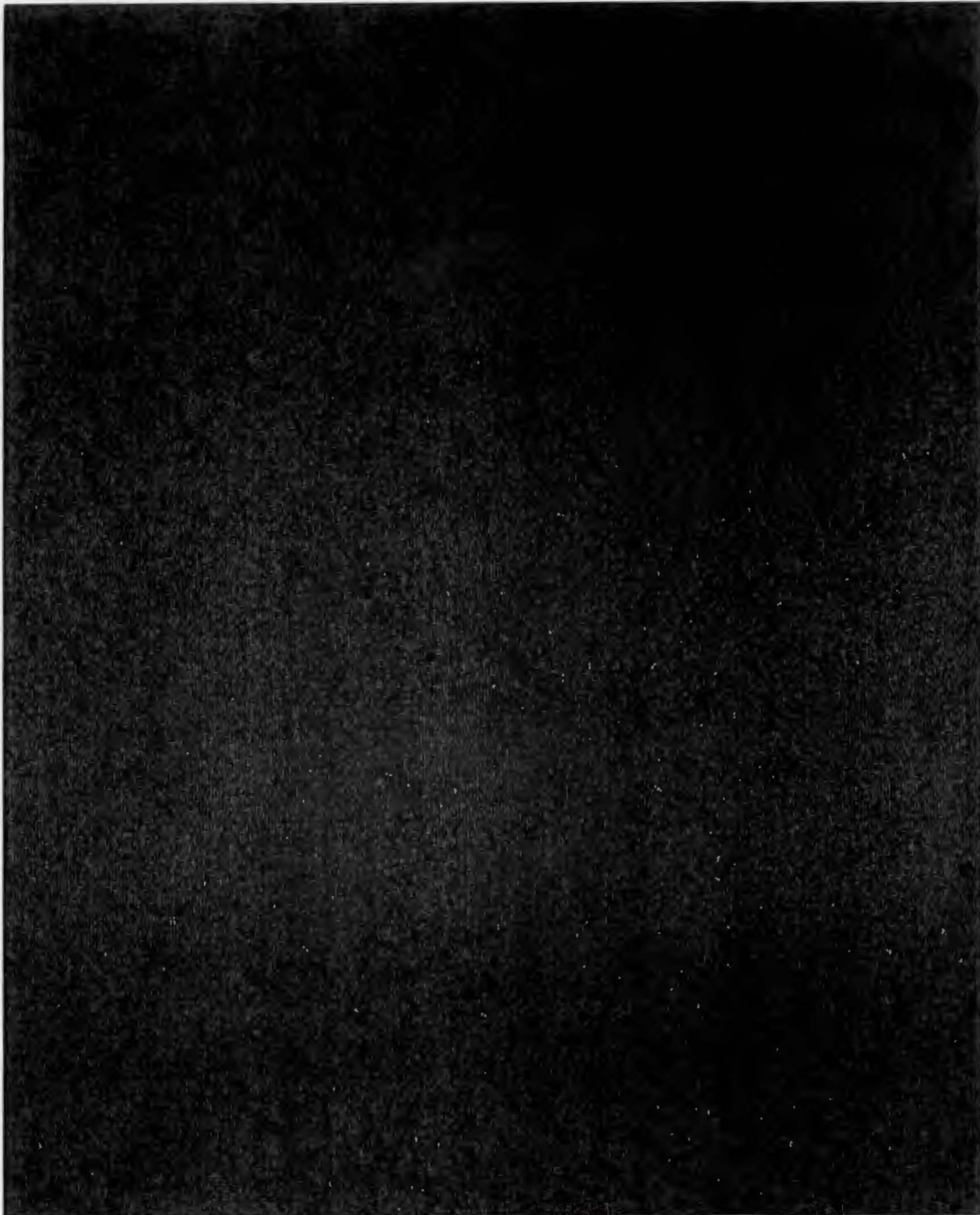
[REDACTED] provided, however, that any selection term reasonably believed to be used by a United States (U.S.) person shall not be regarded as associated with [REDACTED]

[REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution. In the event the emergency provisions the Court's Primary Order are invoked by the Director or Acting Director, NSA's Office of General Counsel (OGC), in consultation with the Director or Acting Director will first confirm that any selection term reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [REDACTED]

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

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

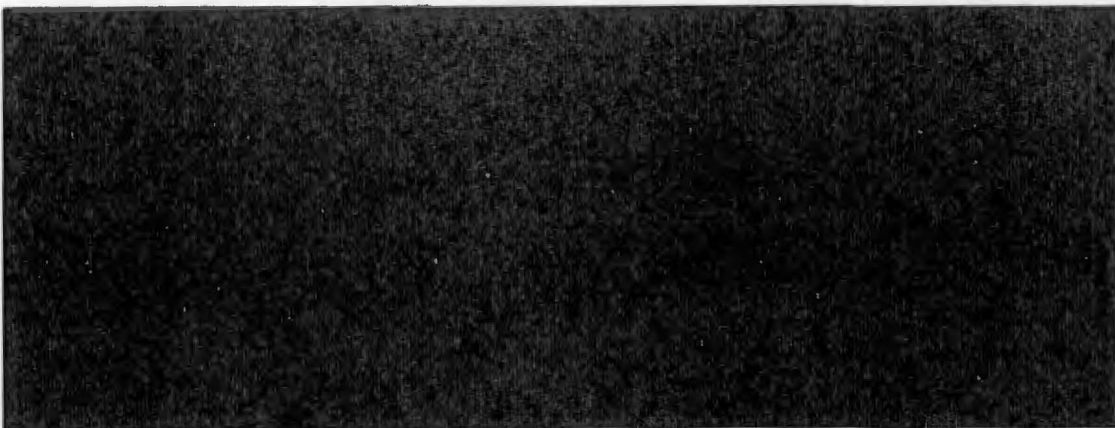
 solely on the basis of activities that are protected by the First Amendment to the Constitution.



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

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

to obtain contact chaining information, within two hops of an approved "seed", for purposes of obtaining foreign intelligence information. In addition, the Director or Acting Director of NSA may authorize the emergency querying of the BR metadata with a selection term for purposes of obtaining foreign intelligence information, within two hops of a "seed", if: (1) the Director or Acting Director of NSA reasonably determines that an emergency situation exists with respect to the conduct of such querying before an order authorizing such use of a selection term can with due diligence be obtained; and (2) the Director or Acting Director of NSA reasonably determines that the RAS standard has been met with respect to the selection term. In any case in which this emergency authority is exercised, the government shall make a motion in accordance with the Primary Order to the Court as soon as practicable, but



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

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

not later than 7 days after the Director or Acting Director of NSA authorizes such query.⁸

(i) Any submission to the Court under this paragraph shall, at a minimum, specify the selection term for which query authorization is sought or was granted, provide the factual basis for the NSA's belief that the reasonable articulable suspicion standard has been met with regard to that selection term and, if such query has already taken place, a statement of the emergency necessitating such query.⁹

(ii) NSA shall ensure, through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved.¹⁰ Whenever

⁸ In the event the Court denies such motion, the government shall take appropriate remedial steps, including any steps the Court may direct.

⁹ For any selection term that is subject to ongoing Court-authorized electronic surveillance, pursuant to 50 U.S.C. § 1805, based on this Court's finding of probable cause to believe that the selection term is being used or is about to be used by agents of [REDACTED] including those used by U.S. persons, the government may use such selection terms as "seeds" during any period of ongoing Court-authorized electronic surveillance without first seeking authorization from this Court as described herein. Except in the case of an emergency, NSA shall first notify the Department of Justice, National Security Division of its proposed use as a seed any selection term subject to ongoing Court-authorized electronic surveillance.

¹⁰ NSA has implemented technical controls, which preclude any query for intelligence analysis purposes with a non-RAS-approved seed.

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

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

the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.¹¹

(iii) The Court's finding that a selection term is associated with [REDACTED]

[REDACTED] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.^{12,13}

(iv) Queries of the BR metadata using RAS-approved selection terms for purposes of obtaining foreign intelligence information may occur by manual analyst

¹¹ This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

¹² The Court understands that from time to time the information available to NSA will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, the government's submission shall specify the time frame for which the selection term is or was associated with [REDACTED]

[REDACTED] In the event that the RAS standard is met, analysts conducting manual queries using that selection term shall properly minimize information that may be returned within query results that fall outside of that timeframe.

¹³ The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to this Order, [REDACTED]

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

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

query only. Queries of the BR metadata to obtain foreign intelligence information shall return only that metadata within two "hops" of an approved seed.¹⁴

D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.¹⁵ NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center)

¹⁴ The first "hop" from a seed returns results including all identifiers (and their associated metadata) with a contact and/or connection with the seed. The second "hop" returns results that include all identifiers (and their associated metadata) with a contact and/or connection with an identifier revealed by the first "hop."

¹⁵ In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

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

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

must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.¹⁶ Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions. Notwithstanding the above requirements, NSA may share the results from intelligence analysis queries of the BR metadata, including United States person information, with Legislative Branch personnel to facilitate lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

¹⁶ In the event the government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

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

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

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.¹⁷ OGC shall provide NSD/DoJ with copies of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this

¹⁷ The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

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

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

authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

(vi) Prior to implementation of any automated query processes, such processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA, other than

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

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

Executive Branch or Legislative Branch personnel receiving such results for their purposes that are exempted from the dissemination requirements of paragraph (3)D above. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

- Remainder of this page intentionally left blank -

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

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

This authorization regarding [REDACTED]

[REDACTED]


[REDACTED]

[REDACTED]

[REDACTED] expires on the 12th day

of September, 2014, at 5:00 p.m., Eastern Time.

Signed 19 June 2014 16:35 Eastern Time
Date Time


JAMES B. ZAGEL
Judge, United States Foreign
Intelligence Surveillance Court

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

[REDACTED]

~~TOP SECRET/COMINT/NOFORN~~

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]
[REDACTED]
[REDACTED]
[REDACTED]

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

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

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]

[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]

4 [REDACTED]

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

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] [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

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

(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.”).

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

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.

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

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

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

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,

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

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]

[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 th 13 day of May, 2011, in Docket Nos. [REDACTED]

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

~~TOP SECRET/COMINT/NOFORN~~