All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE [redacted] :

[redacted] : Docket No.: [redacted]

:

:

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.

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

mail communications of suspected international terrorists. However, on December 13, 2006, in Docket No. [redacted], 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. [redacted].

On January 10, 2007, the judge entered orders in Docket No. [redacted] 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. [redacted] for the identified phone numbers believed to be used by persons in the United States.

The authorization in Docket No. [redacted] comported with the long-established probable cause determination described above, but the authorization in Docket No. [redacted] did not. The Primary Order in Docket No. [redacted] 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 [redacted] 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...)

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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

For Internet communications, NSA uses e-mail addresses as selectors.[5] Id. at 34-42. 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 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. Id. at 14. overseas e-mail addresses and phone numbers have been adopted as selectors under this standard pursuant to the order in Docket No. [redacted]. Id. at 19.

In most relevant respects, the means of electronic surveillance at issue in this case are quite similar to how 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 The e-mail surveillance is also quite similar to what has been

---

[5] [redacted]

[6] This surveillance acquires an Internet communication containing a reference to a selector e-mail address Id. at 22 n.34.

[7] [redacted]

(continued...)

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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 [redacted] conducted by the FBI states that such surveillance [redacted]

[redacted]

[8] [redacted]

[redacted]

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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 target[9] 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

---

[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)).

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

acquisition are "facilities" [Government's Memorandum of Law at 31 n.18] Simultaneously, however, the government maintains in another case that 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 proposed in this docket is identical to that proposed in Docket No. for phone numbers used in the United States. Compare Docket No. Declaration of Lt. Gen. Keith B. Alexander, Director, NSA at 3 (submitted as Attachment C to Application) (defining with Alexander Decl. in this docket at 24-25 (same definition, but with references to and to the "minimization probable cause standard"). 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 Application at 19. In the government's view, the relevant definition for See note 13 infra & accompanying text.

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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. b(7)(E) 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. b(7)(E) 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] 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. b(7)(E) and prior decisions of this Court that have accepted jurisdiction in similar cases b(7)(E) [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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

[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] 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] 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.")

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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] 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] 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] 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] NSA ("[redacted] Decl.") at 16-18 (submitted as part of Exhibit A to the Application). [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.

circumstances, such as surveillances that acquired [redacted] Tellingly, none

---

and b(6), b(7)(A), (C), and (E) [redacted]

and b(6), b(7)(A), (C), and (E) [redacted]

and b(6), b(7)(A), (C), and (E) [redacted]

and b(6), b(7)(A), (C), and (E) [redacted]

(continued...)

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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] 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] [redacted]

[19](...continued) [redacted]

[20] One case relied on by the government involved different statutory requirements and no probable cause finding at all. [redacted] Docket No. PR/TT [redacted] 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.

and b(7)(E) cases (other than this case and Docket No. [redacted]) consistently reflect the same understanding [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 and b(6), b(7)(C), and (E) [redacted]

and b(6), b(7)(C), and (E) [redacted]

and b(6), b(7)(A), (C), and (E) [redacted]

[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...)

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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] 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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

[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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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.

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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.

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

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).

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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

All withheld information exempt under b(1) and b(3) except where otherwise noted.

APPROVED FOR PUBLIC RELEASE

of non-FISA authorities, within the purview of FISA; that a judge of this Court previously authorized this surveillance in Docket No [redacted], on substantially the same terms as the government now proposes; that it would be no simple matter for the government to terminate surveillance of [redacted] 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. [redacted] 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

All withheld information exempt under b(1) and b(3) except where otherwise noted. APPROVED FOR PUBLIC RELEASE

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 3d day of April, 2007 in Docket No. [redacted]

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

[redacted] Clerk,
I, Fl[redacted] that this document
is a true and correct copy
of the origina[redacted]