

NYT-Savage-FOIA-FISC-May-August-2007-Orders

35 Pages - Contributed by Charles Savage, The New York Times - Jan 27, 2015

Probable cause approved on long list of selectors (p. 6)

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)]:

The intent of the roving wiretap provision (p. 12)

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

NSA can go up on new foreign phone numbers and e-mail accounts without prior approval (p. 13)

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

"about the target" e-mail surveillance approved without advance review, too (p. 14)

(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

NSA has to read the "about the target" email before targeting sender/recipient, too (p. 14)

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]

"This holding, albeit novel..." (p. 15)

[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.

NSA to notify court weekly who it newly started targeting and why (p. 18)

Subsequent reports shall be filed on a weekly basis each

"streamlined" emergency application forms okay (p. 21)

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.

Some purely domestic communications may be picked up - that's okay (p. 23)

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.

Changes to NSA FISA procedures start here (p. 27)

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

NSA FISA procedures:

CIA gets raw take (p. 29)

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.

querying storehouse of data for US persons for info re intel or crime (p. 30)

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.

Did NSA know about the # or email address earlier? (p. 33)

Upon reviewing these reports, several judges of this Court have ordered supplementation with regard to whether NSA had knowledge prior to May 24, 2007, that would call into question whether it properly invoked the above-quoted provision of the May 31 Order.¹ The pending motion

Concerns by Judges Kazen, Bates, Benson, Scullin, Kollar-Kotelly (p. 33)

¹ See No. [REDACTED] Orders Dated June 22, 2007 (J. Kazen); July 6, 2007 (J. Bates); July 6, 2007 (J. Benson); July 13, 2007 (J. Scullin); July 20, 2007 (J. Kollar-Kotelly). For a number of

granting the govt as much latitude as the statute can be construed to permit (p. 34)

States, on behalf of one of the targeted foreign powers – it is appropriate to grant the government as much latitude in initiating surveillance as the statute can reasonably be construed to permit.

analysis may be based on prior info, so long as completed after (p. 35) first results in such probable cause assessment was completed

Judge Gorton (p. 35)

In his order in this docket entered on July 27, 2007, Judge Nathaniel M. Gorton noted the:



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*86 Chambers Street
New York, New York 10007*

January 26, 2015

By Electronic Mail

David E. McCraw, Esq.
Jeremy A. Kutner, Esq.
The New York Times Company
620 Eighth Avenue
New York, NY 10018
E-mail: [REDACTED]@nytimes.com

Re: *The New York Times Co. v. U.S. Department of Justice*, 14 Civ. 3948 (VSB)

Dear David and Jeremy:

This Office represents the United States Department of Justice (“DOJ”), the defendant in the above-referenced matter. In accordance with the schedule set forth in the parties’ joint submission on October 9, 2014, *see* Dkt. No. 11, as modified by the Court’s December 8, 2014, order, *see* Dkt. No. 13, DOJ is releasing the enclosed documents in partial response to the Freedom of Information Act (“FOIA”) request that is the subject of this litigation. Information has been redacted from these documents pursuant to 5 U.S.C. §§ 552(b)(1), (b)(3), (b)(6), (b)(7)(C), and (b)(7)(E). Each redacted document being released has been marked with the applicable FOIA exemption or exemptions.

These documents also are being made available to the public on the Director of National Intelligence’s website, “IC on the Record,” at <http://icontherecord.tumblr.com/>, as well as at www.dni.gov.

If you have any questions, please do not hesitate to contact us.

Sincerely,

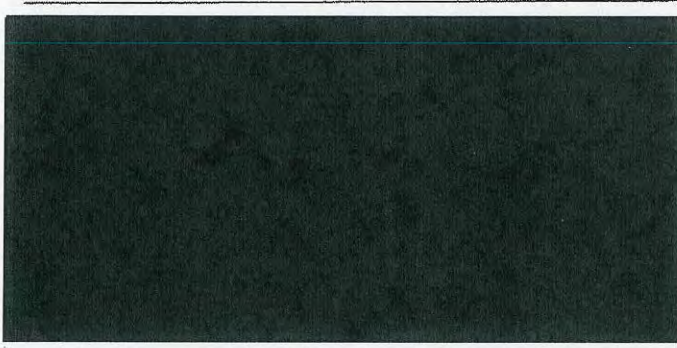
PREET BHARARA
United States Attorney for the
Southern District of New York

By: /s/ John Clopper
JOHN D. CLOPPER
EMILY E. DAUGHTRY
ANDREW E. KRAUSE
Assistant United States Attorneys
Telephone: (212) [REDACTED]
Facsimile: (212) 6 [REDACTED]
E-mail: [REDACTED]@usdoj.gov
[REDACTED]@usdoj.gov
[REDACTED]@usdoj.gov

Enclosures

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

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



:
:
:
:

: Docket Number: [redacted]

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 [redacted] facilities [redacted] [redacted] 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. [redacted] [redacted] 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:

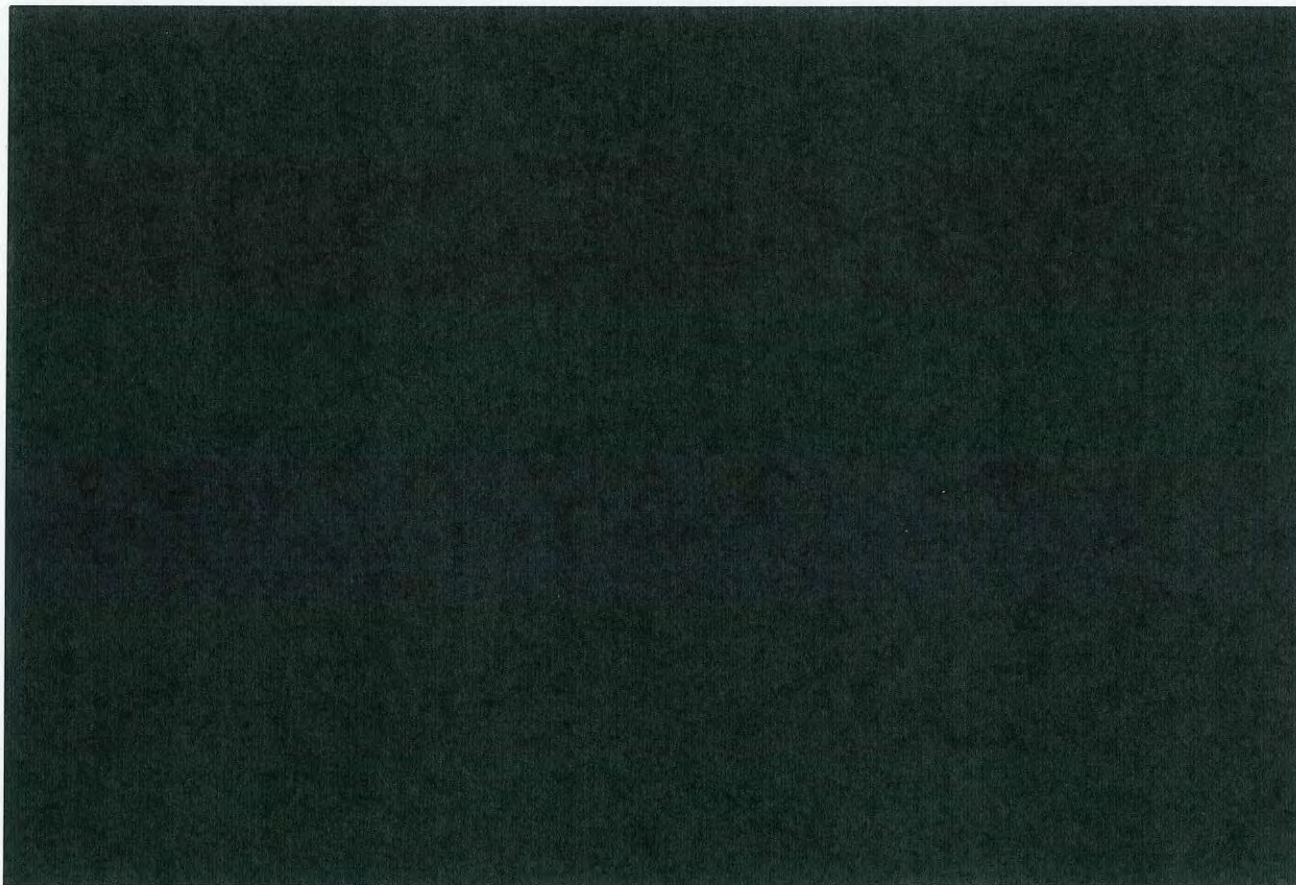
~~TOP SECRET//COMINT//NOFORN~~

~~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)];

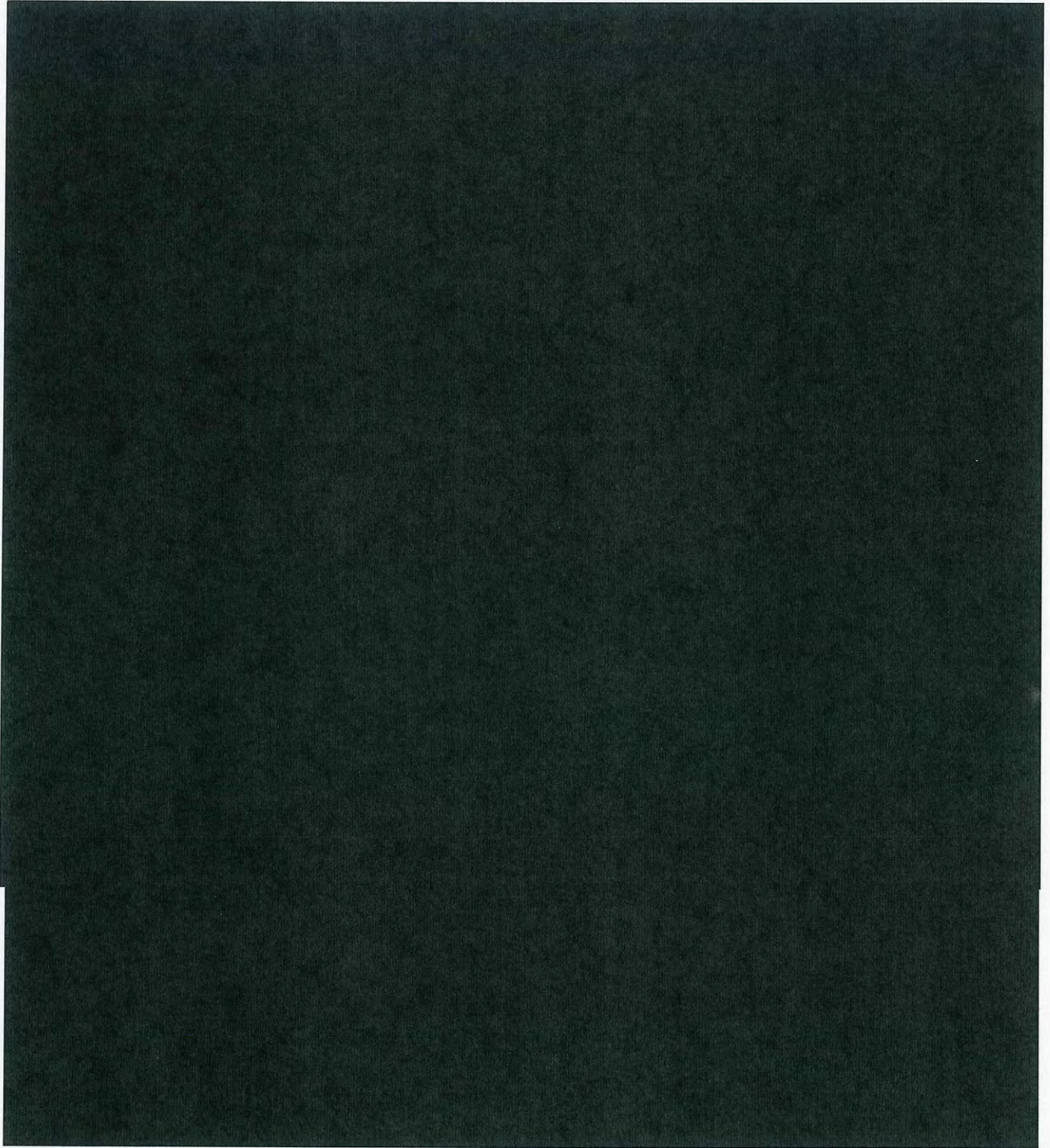
2. The application has been made by a Federal officer and approved by the Attorney General [50 U.S.C. § 1805(a)(2)];

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)];



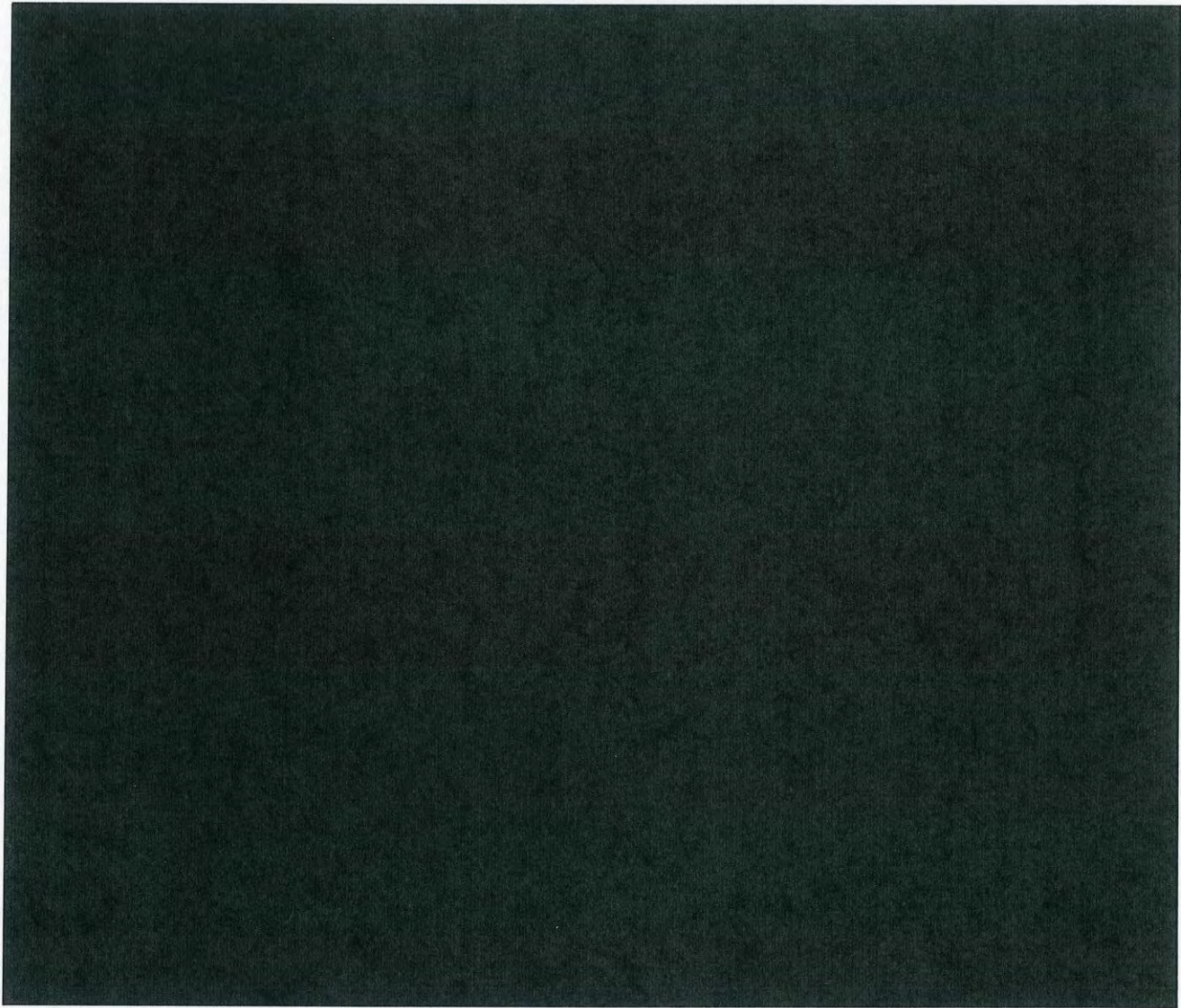
~~TOP SECRET//COMINT//NOFORN~~

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



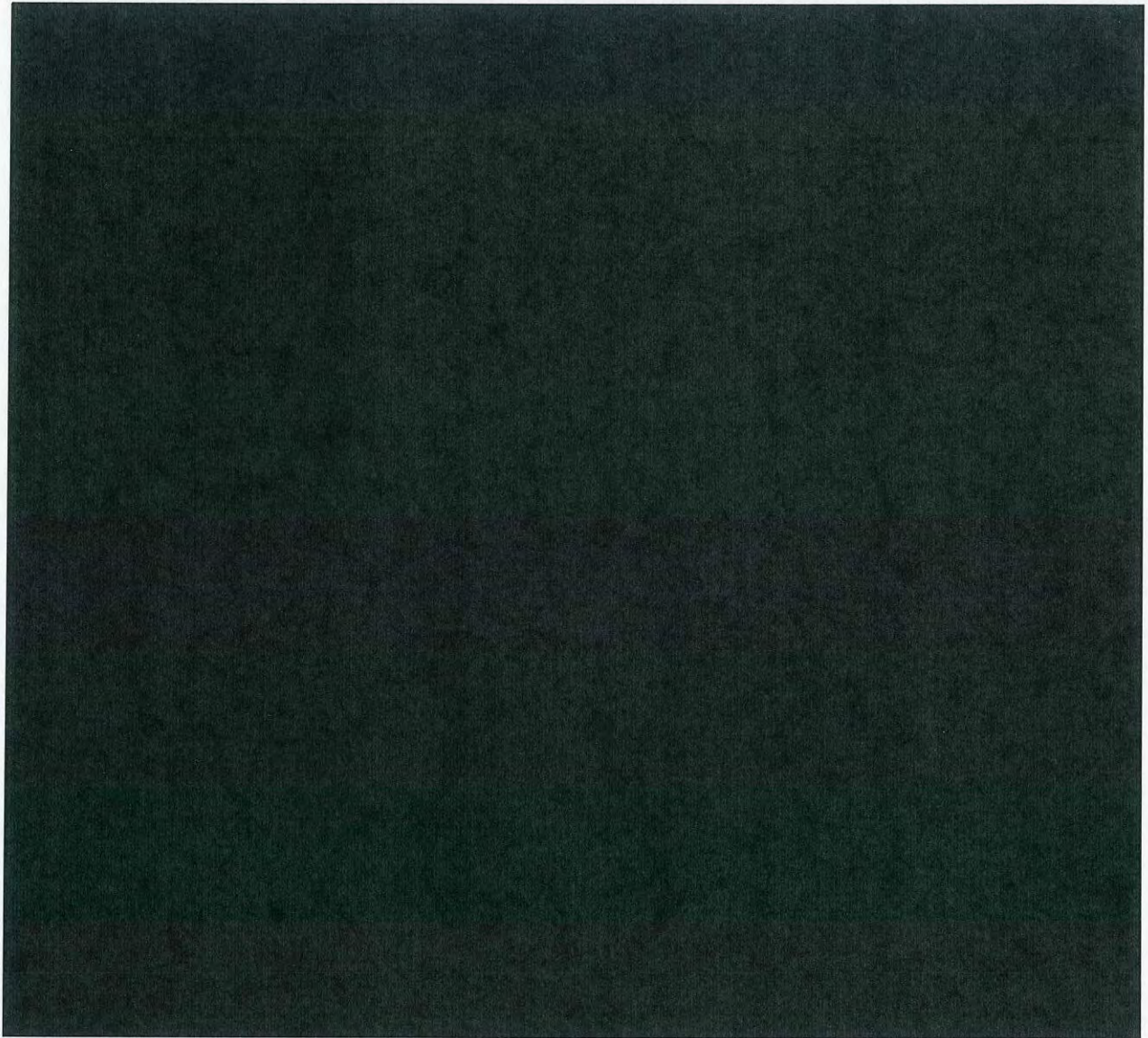
~~TOP SECRET//COMINT//NOFORN~~

~~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.

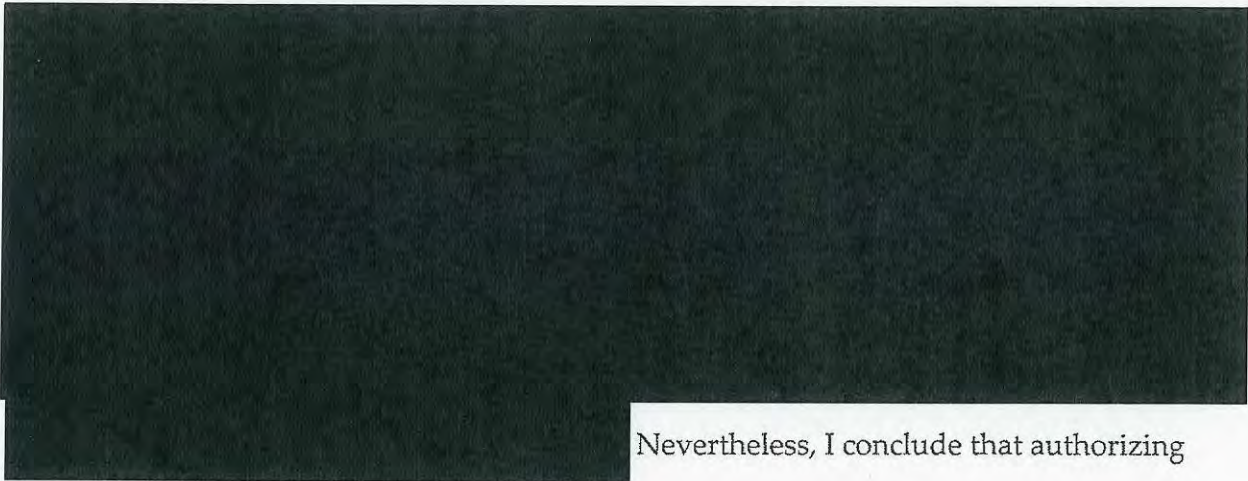
(b). It is well established that the targeted foreign powers pose a grave terrorist threat to the United States. ^{(b)(6); (b)(7)(C)} Declaration, at 10-12, 61-64. The evidence further establishes that the members and agents of the targeted foreign powers engage in a variety of activities in order to 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(11)(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

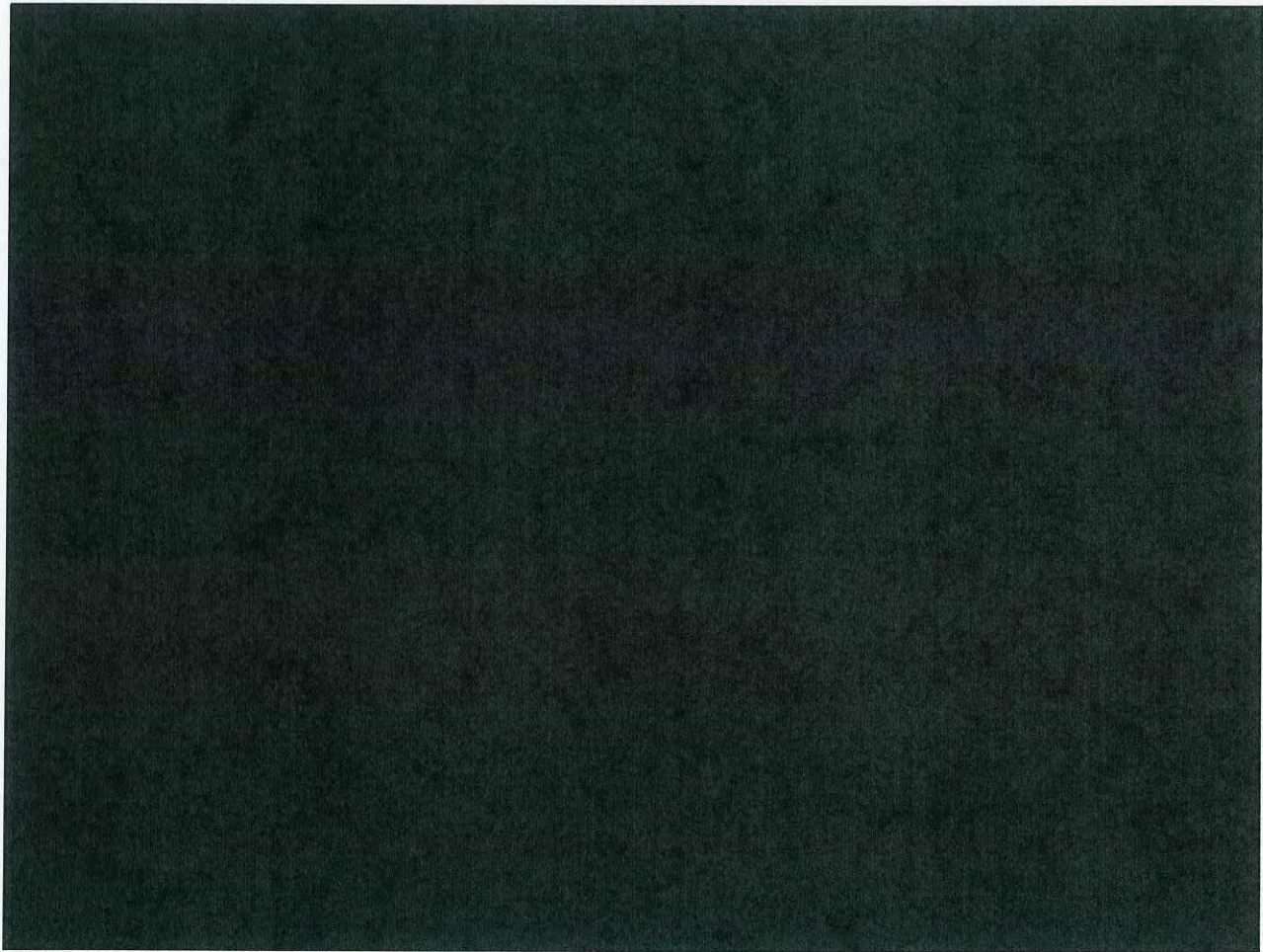
[REDACTED] that is subject to electronic surveillance under this Order at the time of acquisition (targeted [REDACTED]), under one of the following circumstances:

[REDACTED]

⁶ For example, if the user of targeted [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

~~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.

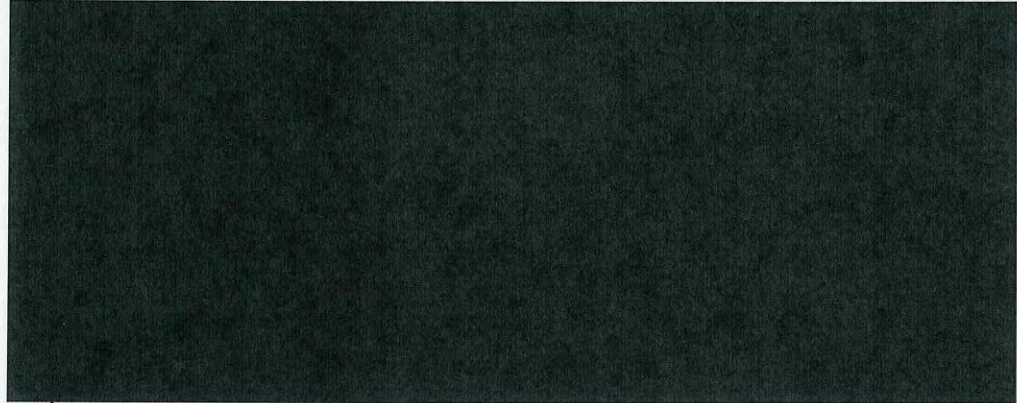
I also hereby find that the Government has established "good cause" within the meaning of 50 U.S.C. § 1806(j) that a subject of emergency surveillance initiated by the Government during the period of this Order, but not authorized by this Court, should not be notified of the emergency employment of electronic 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:



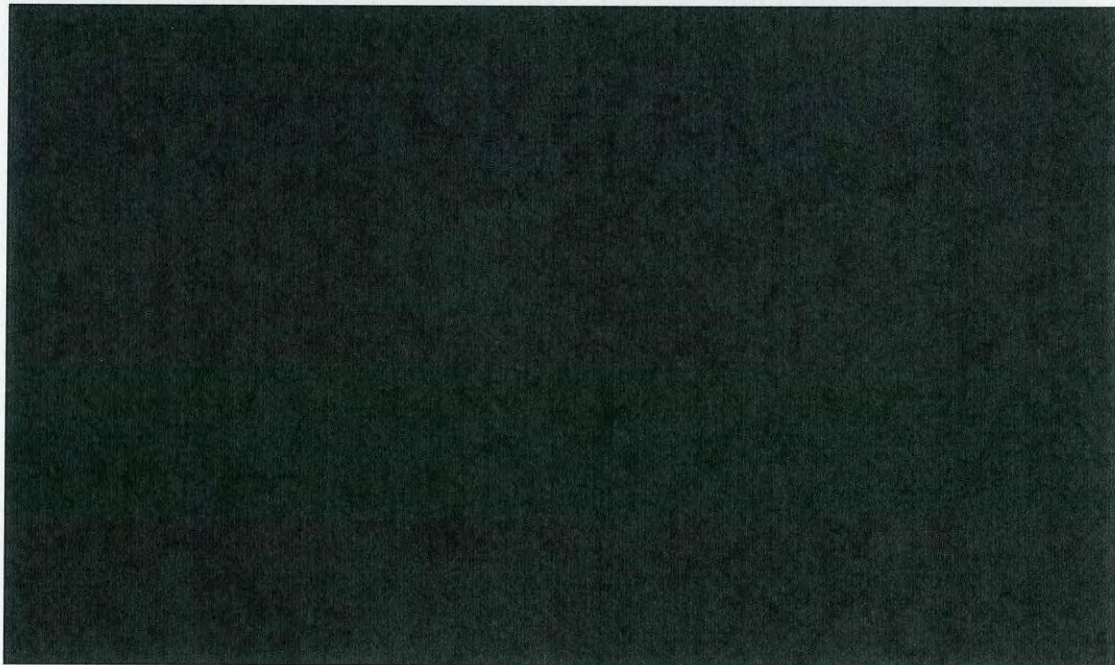
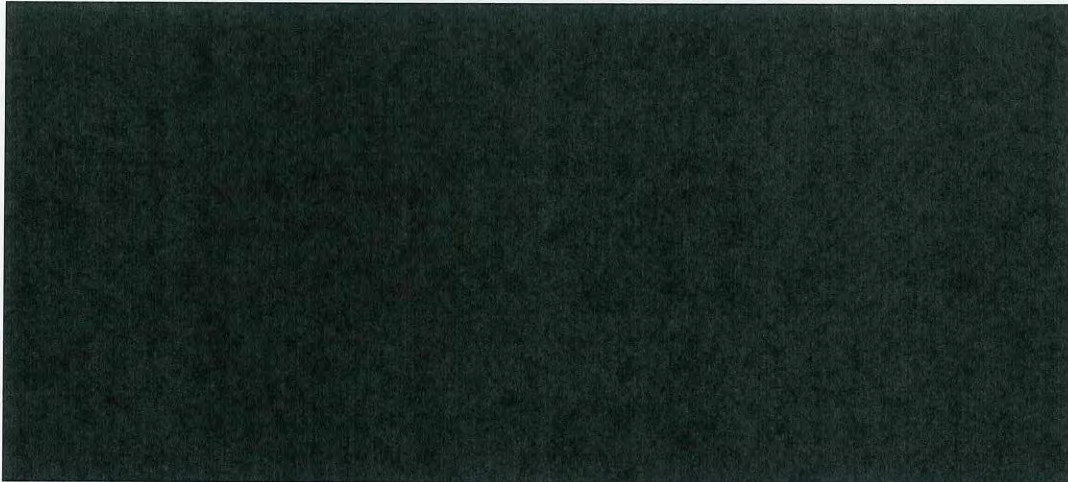
~~TOP SECRET//COMINT//NOFORN~~

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



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

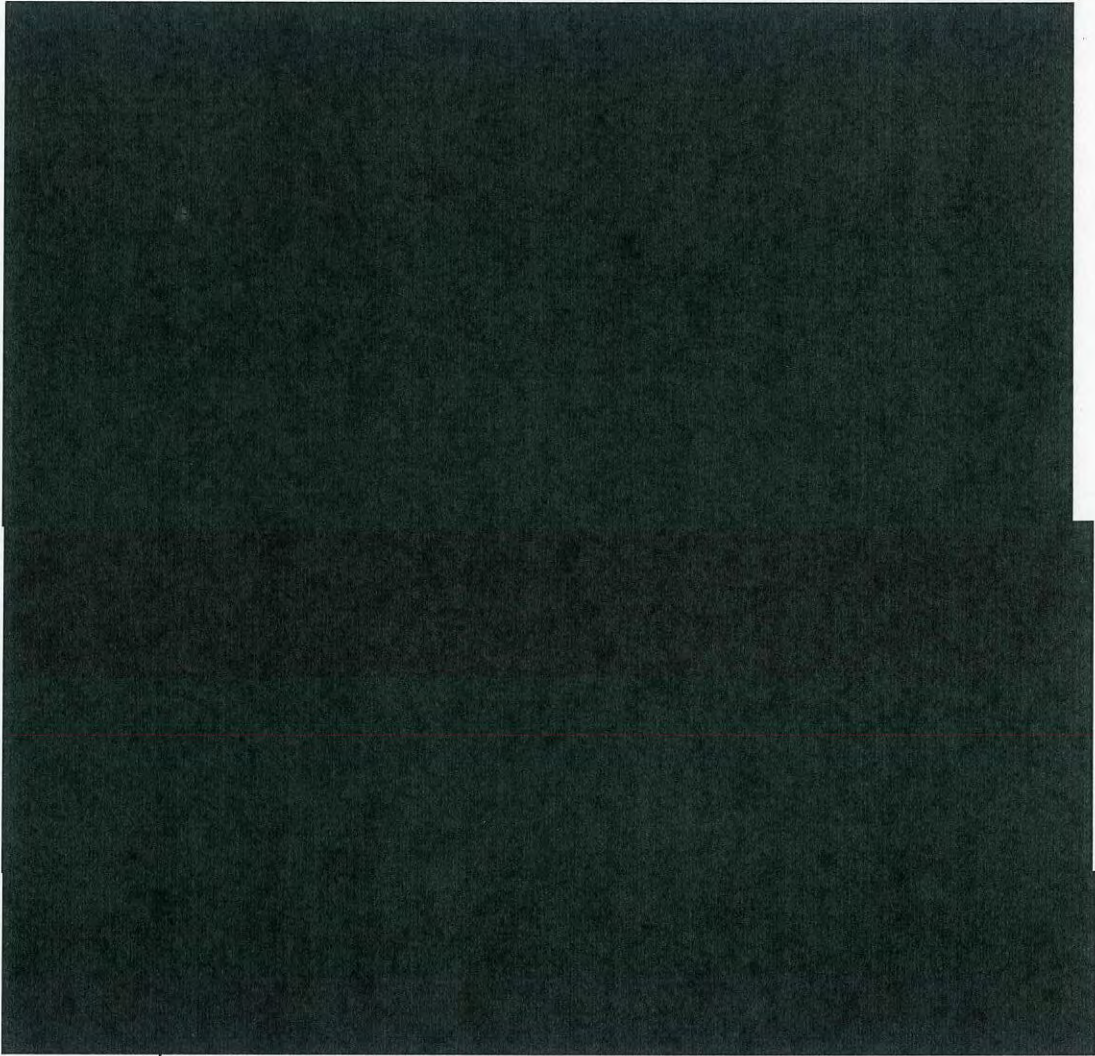
~~TOP SECRET//COMINT//NOFORN~~



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

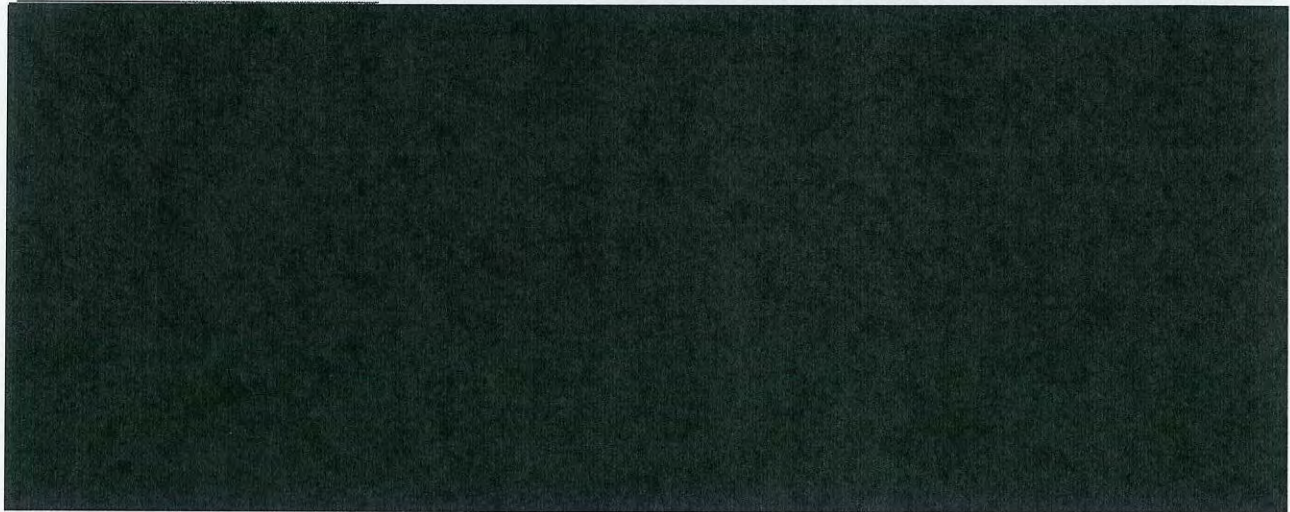
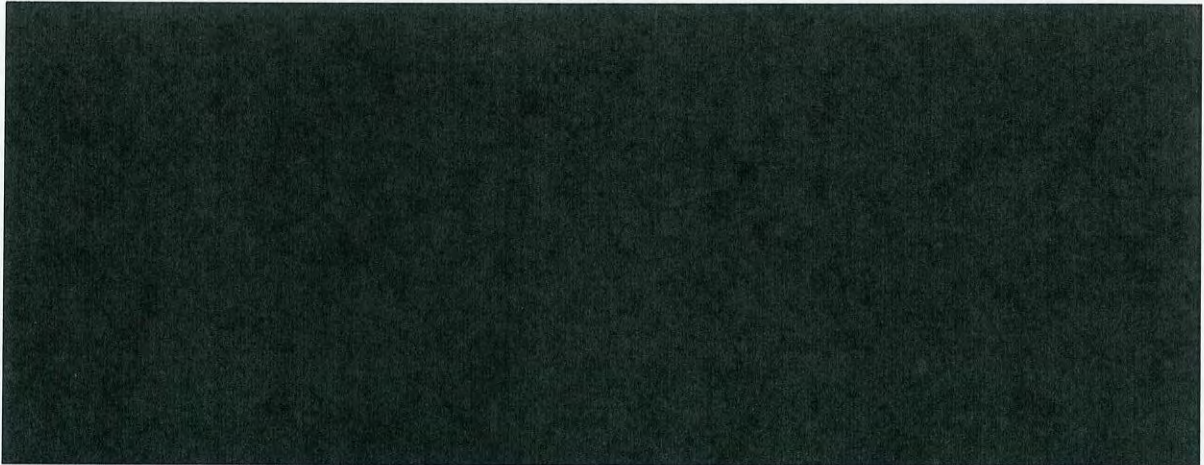
~~TOP SECRET//COMINT//NOFORN~~

"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] 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 _____ Eastern Time
Date Time

05-31-2007 10:15:4

This authorization regarding



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~~

(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)

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

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT



:
:
:
:

Docket No.:



ORDER AND MEMORANDUM OPINION

This matter is before the Court on the Motion to Amend filed by the government in the above-captioned docket on July 27, 2007.

This motion concerns just one of the difficult issues presented by this effort to apply FISA to a complex, large-scale surveillance program. This case has required, and continues to require, an extraordinary expenditure of time and effort by NSA, the Department of Justice, and this Court, notwithstanding that it concerns electronic surveillance that is overwhelmingly directed at non-U.S. persons operating outside of the United States. In my view (a view I believe to be shared by all of the judges of this Court), legislative action is urgently needed to refocus the FISA process on surveillances that – unlike this one – significantly involve interests protected by the Fourth Amendment.

Background

This order is intended to clarify and supplement the earlier orders entered in this docket on April 3, 2007, and May 31, 2007. The May 31 order authorized electronic surveillance of particular, identified telephone numbers and e-mail addresses, on the basis of my finding probable cause to believe that such numbers and addresses were being or about to be used by one of the targets. May 31, 2007 Order at 8-9. It established procedures that were novel and were designed to meet the complex requirements of insuring that the requested surveillance by the NSA complied with the statutory provisions of FISA. That order also provided for adding additional numbers or addresses:

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

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

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

about to be used, by [one of the targeted foreign powers]. 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 of the United States and shall not include the surveillance of telephone numbers and e-mail [REDACTED] that the NSA reasonably believes are being used, or about to be used, by U.S. persons, as defined in 50 U.S.C. § 1801(i).

Id. at 11-12 (emphasis added). That order also established a schedule for the government to submit, pursuant to 50 U.S.C. § 1805(c)(3), weekly reports on the initiation of electronic surveillance of such additional facilities. *Id.* at 16-17.

Upon reviewing these reports, several judges of this Court have ordered supplementation with regard to whether NSA had knowledge prior to May 24, 2007, that would call into question whether it properly invoked the above-quoted provision of the May 31 Order.¹ The pending motion seeks clarification of what it means, under that provision, for the “nature and location” of a facility to have been “unknown to the NSA as of May 24, 2007.” I conducted a hearing on this motion on the record on August 2, 2007.

Discussion

With the benefit of some two months of implementation, it can be seen that this provision of the May 31 Order requires clarification. As stated in the motion, and further addressed at the hearing, NSA has encountered different situations in which it has found the proper interpretation of this provision to be uncertain. The following hypothetical examples illustrate some of these concerns:

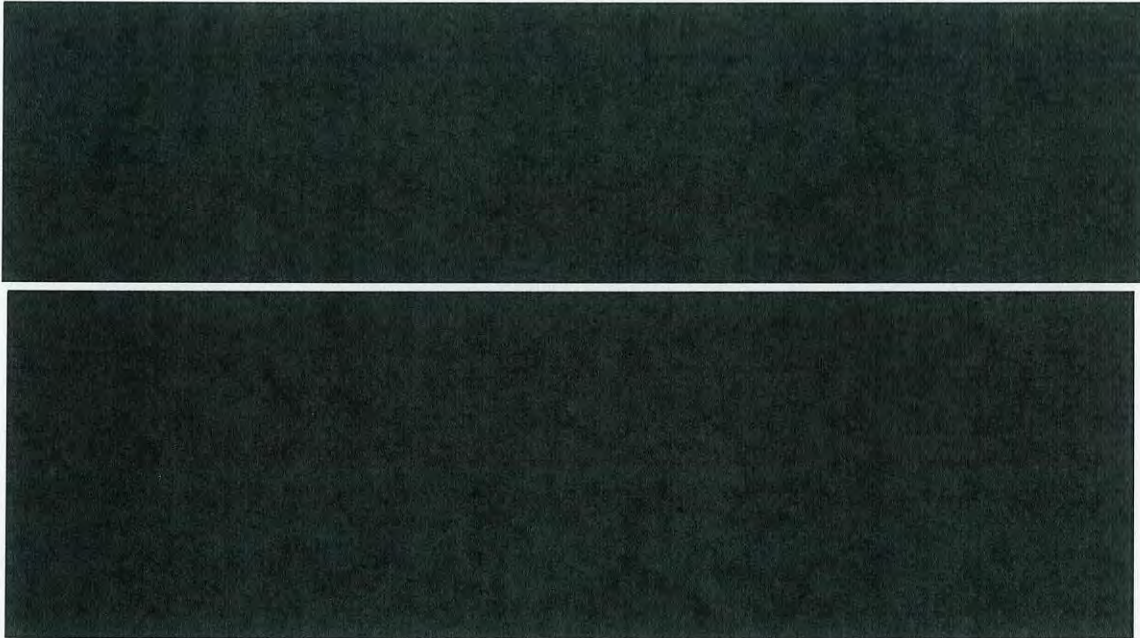


¹ See No. [REDACTED] Orders Dated June 22, 2007 (J. Kazen); July 6, 2007 (J. Bates); July 6, 2007 (J. Benson); July 13, 2007 (J. Scullin); July 20, 2007 (J. Kollar-Kotelly). For a number of reported facilities, the government was also ordered to supplement the stated basis for finding probable cause to believe that a targeted foreign power was using or about to use the facility. The adequacy of the probable cause statements is not presented by the instant motion.

² For example, (b)(3); (b)(6) [REDACTED] an NSA official, testified at the hearing that NSA maintains (continued...)

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

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



I am persuaded that, in all three of these scenarios, NSA could properly initiate surveillance under the above-quoted authority for “later-identified” facilities. For purposes of this provision of the May 31 Order, NSA obtains knowledge of the “nature and location” of a facility when it first assesses that there is probable cause to believe that the facility is being used or about to be used by a targeted foreign power. Thus, “known” in this context applies to both the fact that the target has been found or identified, and a “connecting-the-dots” or understanding of that fact’s significance. A more limited interpretation of this provision would preclude NSA from initiating surveillance under this authority for a facility that, even with the exercise of due diligence, it could not have presented in the original application. I conclude that, under the limited circumstances where this authority applies – only to facilities reasonably believed to be used by non-U.S. persons outside of the United States, on behalf of one of the targeted foreign powers – it is appropriate to grant the government as much latitude in initiating surveillance as the statute can reasonably be construed to permit.

²(...continued)
databases [REDACTED]

³ At the hearing, (b)(3); (b)(6) testified that, since February 2007, NSA had tasked approximately [REDACTED] e-mail addresses and phone numbers for non-FISA collection under Executive Order No. 12333 because they were associated with one of the targeted foreign powers – [REDACTED] than the total number of facilities targeted for surveillance under the probable cause standards of the May 31 Order.

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


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

However, I am not able to grant the government the precise relief that its motion requests. The motion proposes that a facility should be eligible for this "later-identified" authority if it had not been the subject of a FISA application or emergency authorization prior to May 24, 2007, or tasked for collection under the authority granted in Docket No. [REDACTED], or under the Terrorist Surveillance Program as of December 31, 2006. Motion at 4-5. These criteria, by their terms, would not preclude the strategic withholding from pre-surveillance judicial review of facilities that were already intended to be subjected to the FISA surveillance at the time the application was submitted. There is no reason to believe that the government has engaged, or would engage, in this practice. However, I conclude that the statute does not permit such an unlimited grant of authority that would, by its terms, allow the initiation of surveillance in those circumstances. The motion is GRANTED only to the extent set out herein.

Accordingly, it is hereby ORDERED that, for purposes of the authority granted pursuant to 50 U.S.C. § 1805(c)(1)(B) and § 1805(c)(3) on pages 11 and 12 of the May 31 Order, NSA shall be deemed to obtain knowledge of the nature and location of a facility when NSA first is able to determine that there is probable cause to believe that the facility is being used or about to be used by a targeted foreign power. Such determination may be made on the basis, in whole or in part, of analysis of information acquired by NSA on or before May 24, 2007, so long as the analysis that first results in such probable cause assessment was completed after May 24, 2007.

In his order in this docket entered on July 27, 2007, Judge Nathaniel M. Gorton noted the pendency of this motion as a reason for not requiring supplementation of the report filed by the government on July 18, 2007, regarding compliance with this requirement. Accordingly, it is hereby ORDERED that, by August 10, 2007, the government shall supplement that report by providing a statement whether, for each of the reported facilities, NSA was first able to determine that there was probable cause to believe that the facility was being used or about to be used by a targeted foreign power based on an analytical assessment NSA completed subsequent to May 24, 2007. In my view, an affirmative statement in this form should generally suffice to show that this requirement was satisfied. Similar supplementation may be sufficient with respect to the reports required by Judges Kazen, Bates, Benson, Scullin, and Kollar-Kotelly, see footnote 1 above, but I do not decide those issues now.

Done and ordered this 2nd day of August, 2007, in Docket No. [REDACTED]


ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

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