

~~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 as modified herein, and it is

FURTHER ORDERED, as follows [50 U.S.C. § 1805(c)-(e)]:

(1) 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 or places described in paragraph 3(c) above, subject to the minimization procedures specified in paragraph 4 above, including the application of the "minimization probable cause standard" specified below, for a period of **ninety days**, unless otherwise ordered by the Court, as follows:

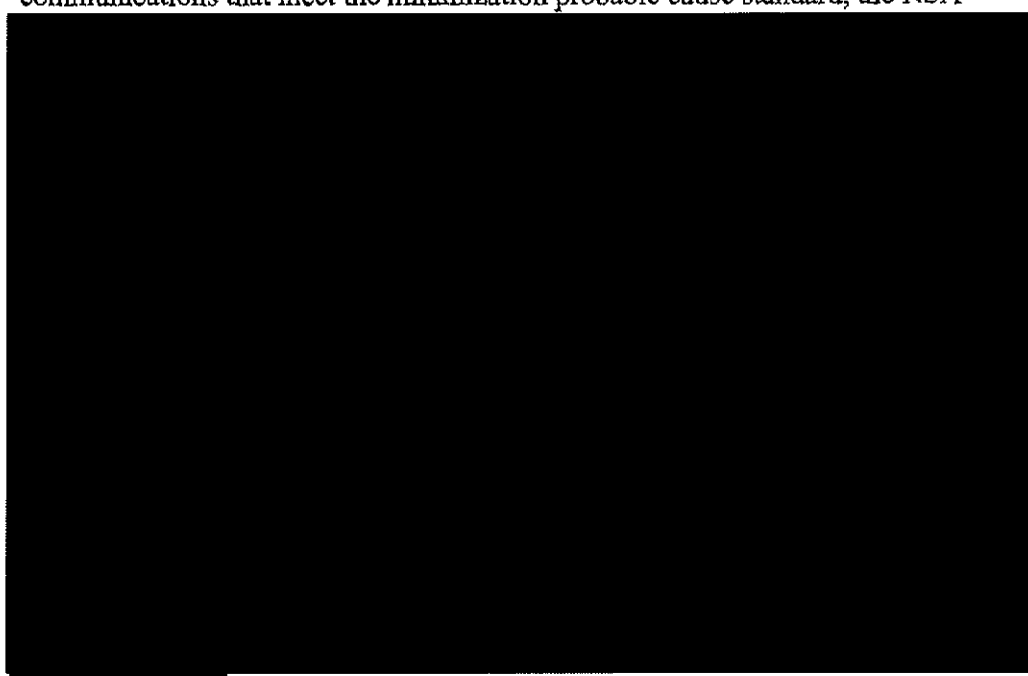


4

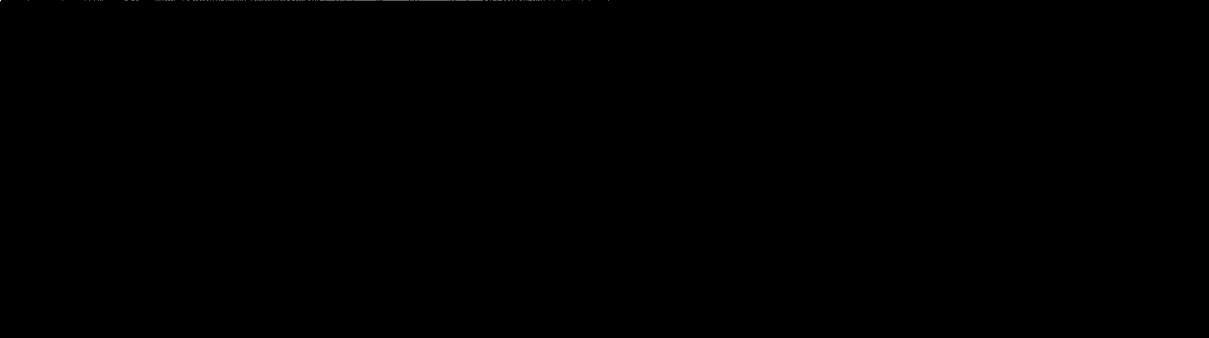
~~TOP SECRET//COMINT//NOFORN~~

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

 NSA shall collect only communications that meet the minimization probable cause standard. In addition, with respect to communications that meet the minimization probable cause standard, the NSA



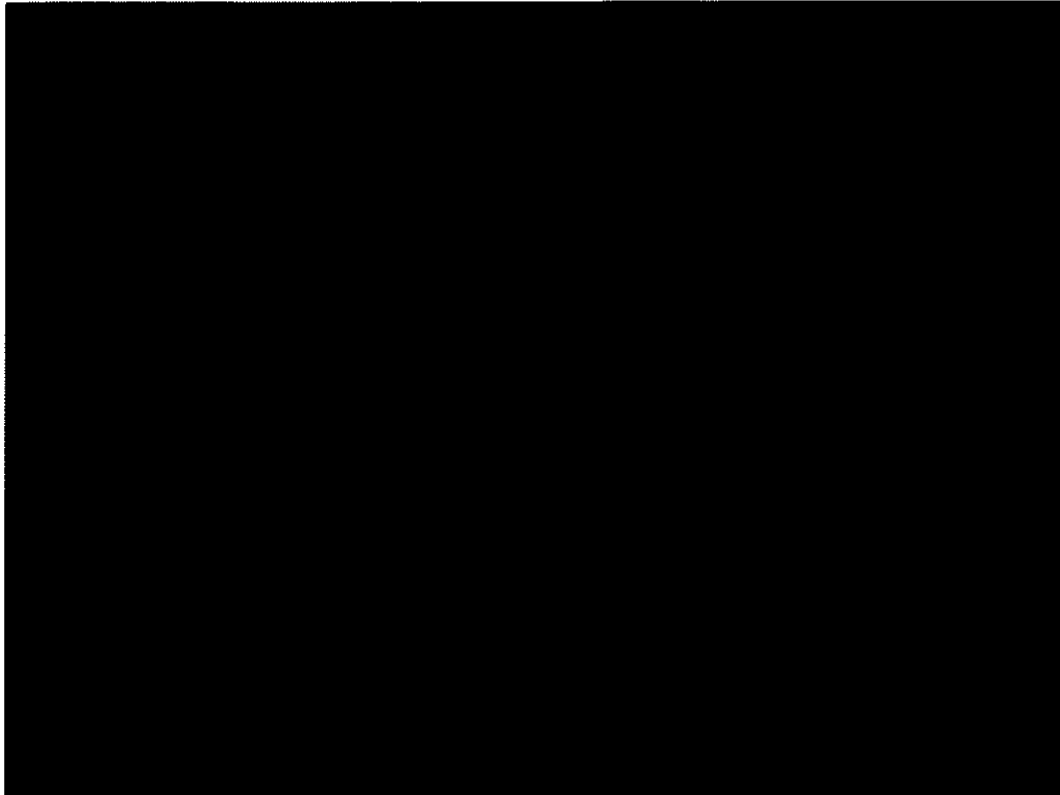
NSA shall collect only communications that meet the minimization probable cause standard. In addition, with respect to communications that meet the minimization probable cause standard, the NSA



⁵ Although the NSA surveillance will be designed to acquire only international communications where one communicant is outside the United States, the Court understands that the communications infrastructure and the manner in which it routes communications do not

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

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



permit complete assurance that this will be the case. In such cases, NSA shall apply its standard FISA minimization procedures, as described and modified herein, to any domestic communications it may inadvertently acquire.

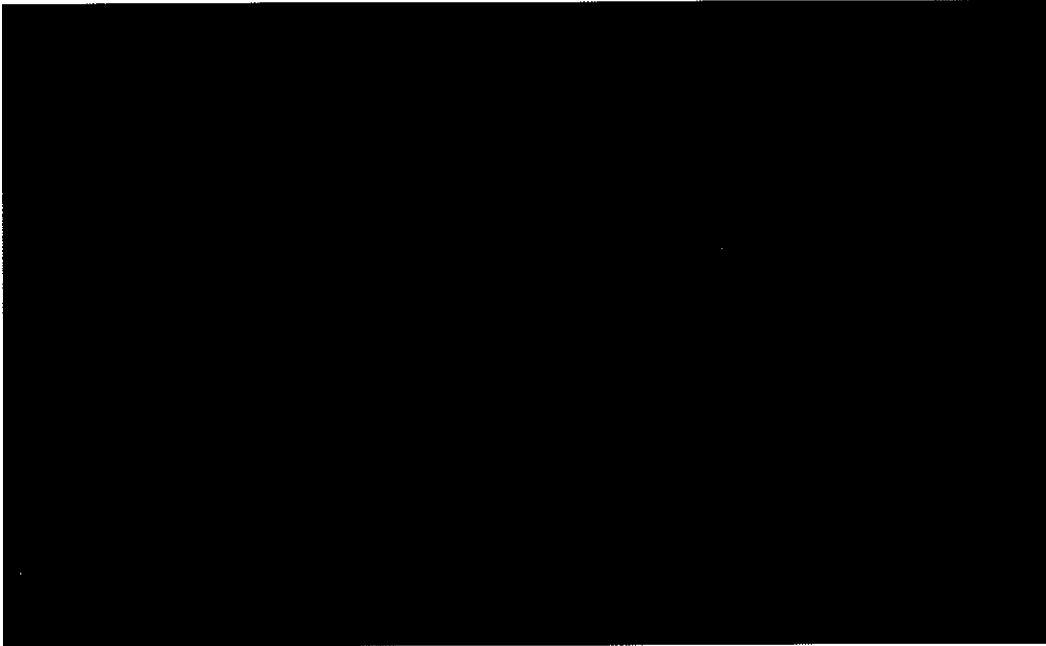
⁶ The Court understands that the system will select for delivery to NSA not only international Internet communications to and from agents or members of [REDACTED]

[REDACTED] but also Internet communications in which e-mail addresses [REDACTED] of such agents or members are mentioned in the Internet communication.

⁷ [REDACTED]

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

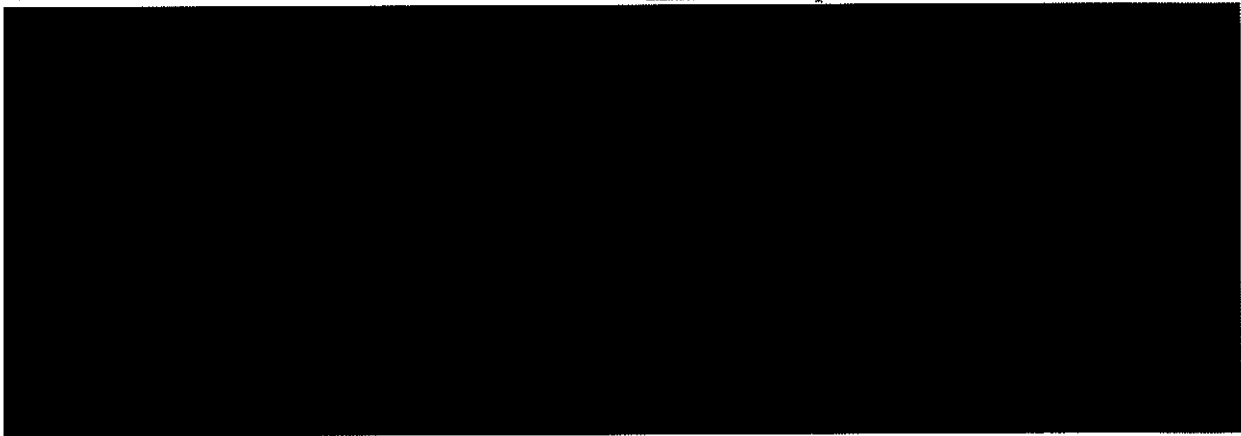
~~TOP SECRET//COMINT//NOFORN~~



8

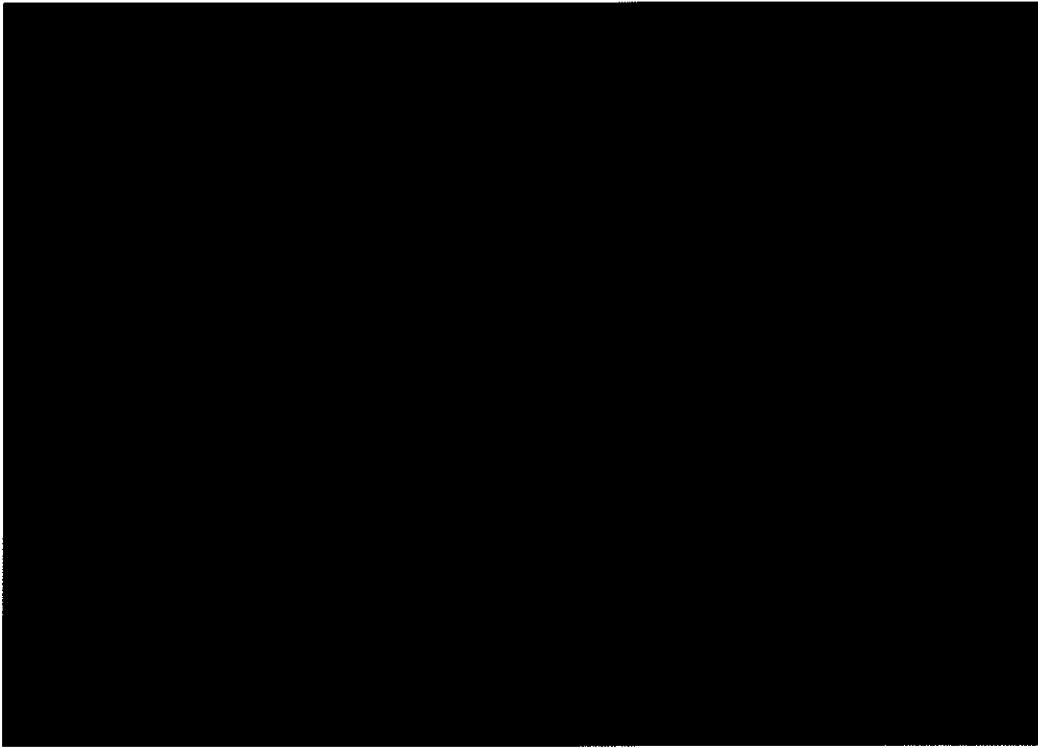


⁹ The Court understands that "selectors" as used herein to discuss the collection of Internet communications refers to e-mail addresses. 

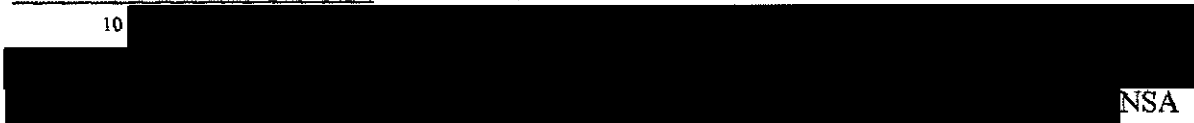


~~TOP SECRET//COMINT//NOFORN~~

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



10



NSA

shall handle non-target communications acquired as a result of this technical limitation in accordance with its standard FISA minimization procedures, as modified herein.

11

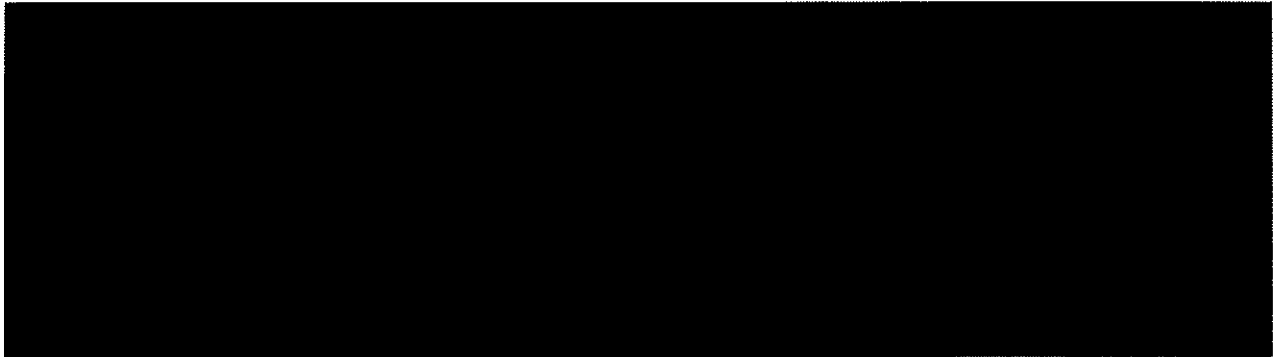


~~TOP SECRET//COMINT//NOFORN~~

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

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

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



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, and/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)].

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

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

(3) As to all information gathered through the authorities requested herein, the NSA shall follow the minimization probable cause procedure set forth below:

Minimization Probable Cause Standard. NSA shall apply two criteria in selecting communications to target for collection, both of which shall apply in each instance. First, NSA shall compile and update a list of telephone numbers and e-mail addresses (together, "selectors") for which it has determined, based on the totality of circumstances, there is probable cause to believe that the particular selector is used by [REDACTED]

[REDACTED]

Second, NSA shall acquire only communications for which there is probable cause to believe that at least one of the communicants is outside the United States. Together, these two criteria constitute the "minimization probable cause standard."

Use of Foreign Selectors. All selectors shall be telephone numbers or e-mail addresses that NSA reasonably believes are being used by persons outside the United States.¹²

¹² The Court understands that a selector that NSA reasonably believes is being used outside the United States may on occasion be used in the United States. If NSA discovers that it has acquired communications from a selector while that selector was being used inside the United States, NSA shall handle any such inadvertently acquired communications as provided in the minimization procedures described in this Order.

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

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

NSA Process for Determining that the Minimization Probable Cause Standard Has Been Met. All telephone numbers and e-mail addresses NSA analysts seek to use as a basis for acquiring communications [REDACTED]

[REDACTED] to the application shall be entered into a database that will show the telephone number or e-mail address the analyst has probable cause to believe is used by a member or agent of [REDACTED]

[REDACTED] and a statement of the reasons for such a belief. [REDACTED] as

described in Exhibit C to the application. The proposed number or e-mail address and supporting documentation shall be reviewed by officials from the [REDACTED]

[REDACTED] Branch within NSA.¹³ Prior to initiating acquisition of communications to or from a telephone number or to, from, or concerning an e-mail address [REDACTED] NSA officials from the [REDACTED]

[REDACTED] Branch shall confirm that documentation regarding the first prong of the minimization probable cause standard is present in the file. If the reviewing officials find that the standard has not been documented appropriately, the telephone

¹³ The Court understands that NSA is considering assigning this duty to another NSA component. If such a change in the assignment of this duty occurs and if different officials will determine whether proper documentation exists to support the determination that specific telephone numbers, e-mail addresses [REDACTED] meet the minimization probable cause standard, the Government shall inform the Court in the next application for a renewal of the Court's authorization.

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

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

number or e-mail address will remain in the database, but shall be ineligible for tasking and will be designated as such.

Additional Oversight. The NSA shall apply the following additional oversight. The NSA's Inspector General (IG), General Counsel (GC), and the Signals Intelligence Directorate's Office of Oversight and Compliance shall each periodically review this program to ensure it is being carried out lawfully, and shall submit an initial report to the Director of NSA sixty (60) days after the initiation of collection to assess the adequacy of the management controls and to assure that the processing and dissemination of U.S. person information is being accomplished in accordance with the minimization procedures specified herein.

Review by the Department of Justice and Reporting to this Court:

- (i) An attorney from the National Security Division at the Department of Justice shall review the NSA's justifications for targeting selectors.
- (ii) The Government shall submit a report to the Court every thirty (30) days listing new selectors that the NSA has tasked during the previous thirty days and briefly summarizing the basis for the NSA's determination that the first prong of the minimization probable cause standard has been met for each new selector.
- (iii) At any time, if the Court finds that there is not probable cause to believe that any particular selector is used by a member or agent of [REDACTED]
[REDACTED] the Court may direct that surveillance under this Order shall cease on that selector

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

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

expeditiously. The Court may also direct that any communications acquired using that particular selector shall be segregated and/or disposed of in a manner approved by the Court.

(4) In addition to the minimization probable cause standard set forth above, as to all information gathered through the authorities requested herein, 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 Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with this Court;

(b) [REDACTED]

[REDACTED]

[REDACTED]

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

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

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

expeditiously. The Court may also direct that any communications acquired using that particular selector shall be segregated and/or disposed of in a manner approved by the Court.

(4) In addition to the minimization probable cause standard set forth above, as to all information gathered through the authorities requested herein, 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 Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with this Court;

(b) Certain of the modifications to the standard NSA FISA minimization procedures for electronic surveillance adopted by this Court in *In re Electronic Surveillance and Physical Search of International Terrorist Groups, Their Agents, and Related Targets*, Order, No. (7)(E) (May 10, 2002) ("*Raw Take Motion*"), which modifications are set forth below:

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

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

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

communications are specifically labeled as being privileged. However, such communications may not be disseminated outside of 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 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. 12,333 and applicable federal criminal statutes.

¹⁴ and b(7)(E)

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

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

(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. 12,333, 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.

(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 C to the application.

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

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

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.

(5) With each request for reauthorization, the Government shall (i) present a list of current selectors previously reported to the Court that the Government intends to continue to task for collection under the reauthorization; (ii) identify any such selectors that are reasonably believed to be used by U.S. persons outside the United States; and (iii) assess the efficacy of the surveillance described in footnote 6 above in acquiring the communications of the targeted foreign powers.

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

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

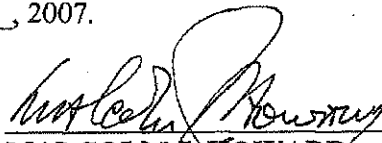
(6) The CIA shall minimize all communications received under this order as provided in Exhibit F to the application.

Signed 01-10-2007 002:18 Eastern Time
Date Time

This authorization regarding [REDACTED]

[REDACTED] expires at 3:00 pm

on the 6th day of APRIL, 2007.


MALCOLM J. HOWARD
Judge, United States Foreign
Intelligence Surveillance Court

b(6) and b(7)(C)

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

b(6) and b(7)(C)

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

IN RE VARIOUS KNOWN AND UNKNOWN :

AGENTS OF [REDACTED] :

[REDACTED] : Docket Number: [REDACTED]

PRESUMED UNITED STATES PERSONS (S) :

ORDER

The United States of America having applied, pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801-1811 ("FISA" or "the Act"), for an order for electronic surveillance targeting **Various Known and Unknown Agents of** [REDACTED] [REDACTED] presumed U.S. persons, and the Court, having given full consideration to the matters set forth in the Government's application, finds as follows:

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)];

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

Derived from: Application to the USFISC in [REDACTED]

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

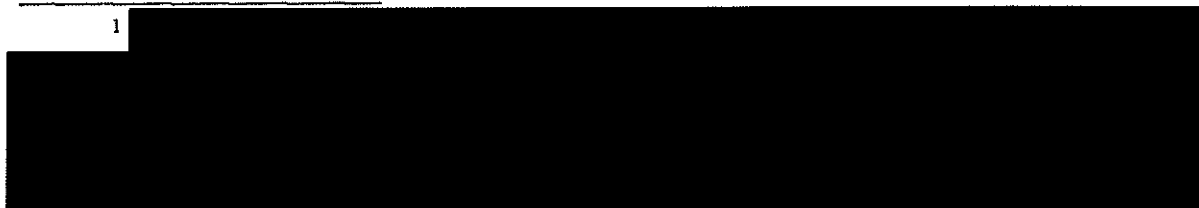
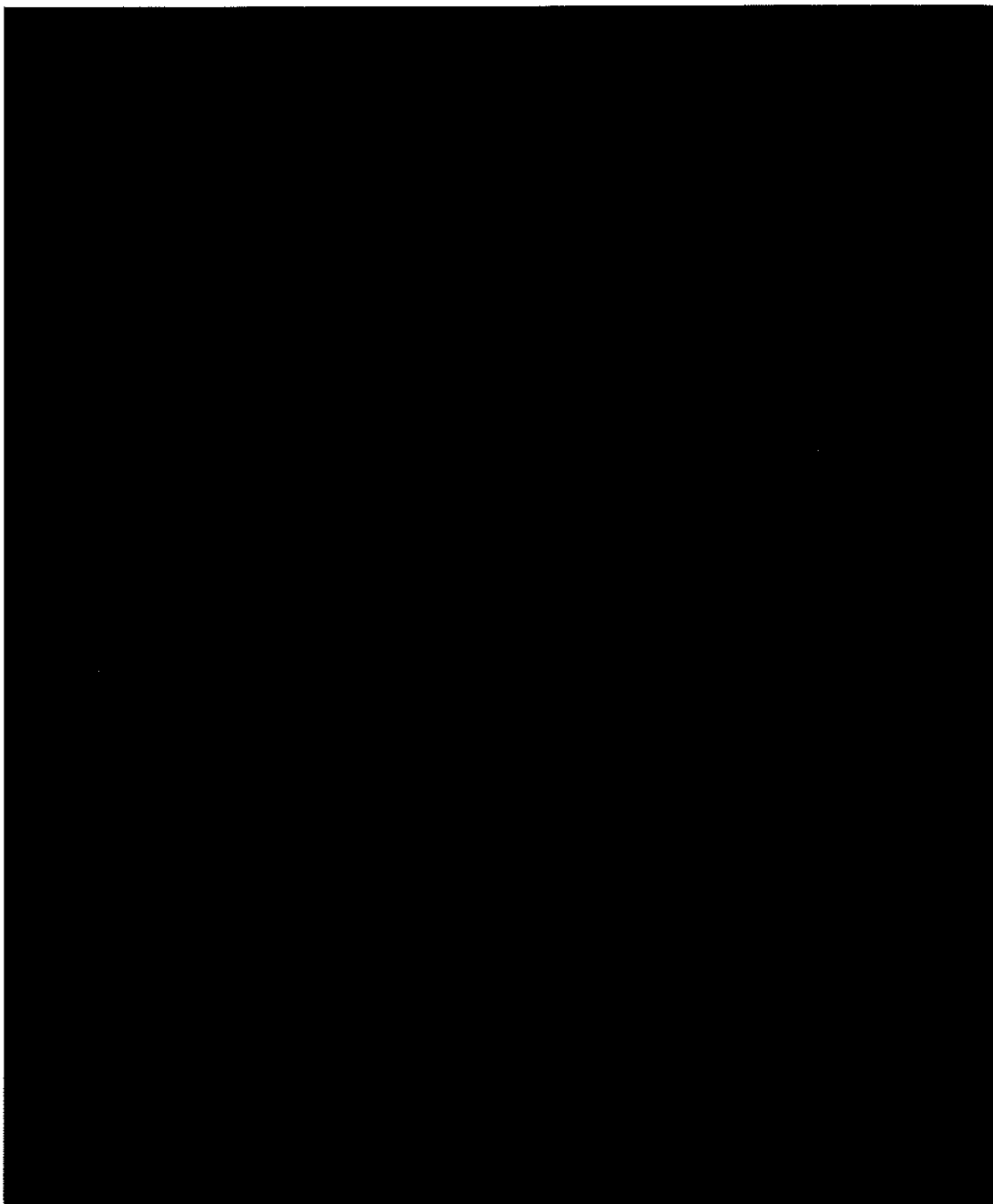
3. On the basis of the facts submitted by the applicant, there is probable cause to believe that [50 U.S.C. § 1805(a)(3)]:

(a) [REDACTED] as further referenced in Exhibit B, together, constitute a group engaged in international terrorism or activities in preparation therefor, and, therefore, is a foreign power as defined by 50 U.S.C. § 1801(a)(4):

[REDACTED]

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

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



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

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

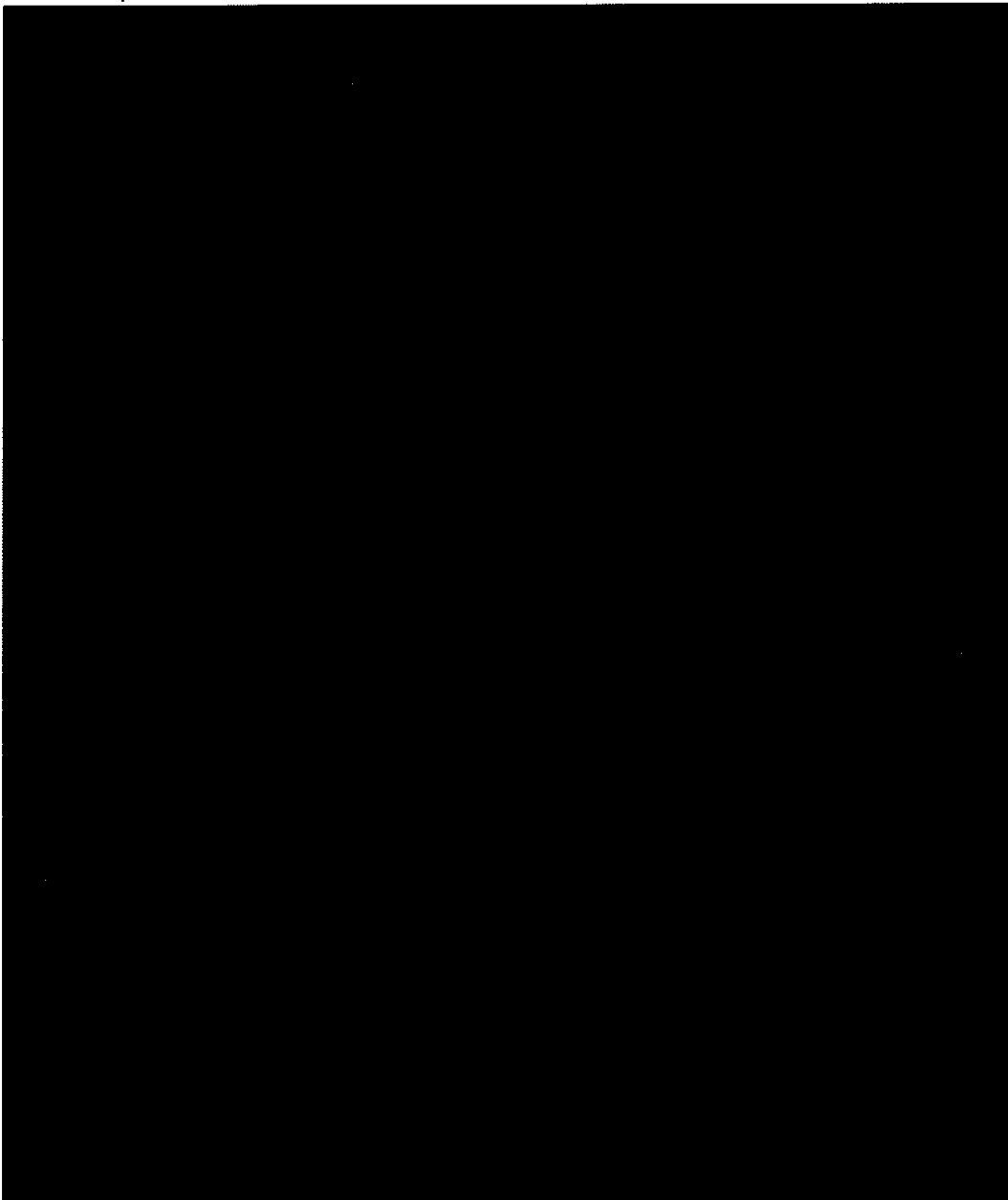
(b) the targets of this electronic surveillance, **Various Known and Unknown Agents of**

 presumed U.S. persons, described

in Exhibit A to the application, are agents of this foreign power, as defined by 50 U.S.C.

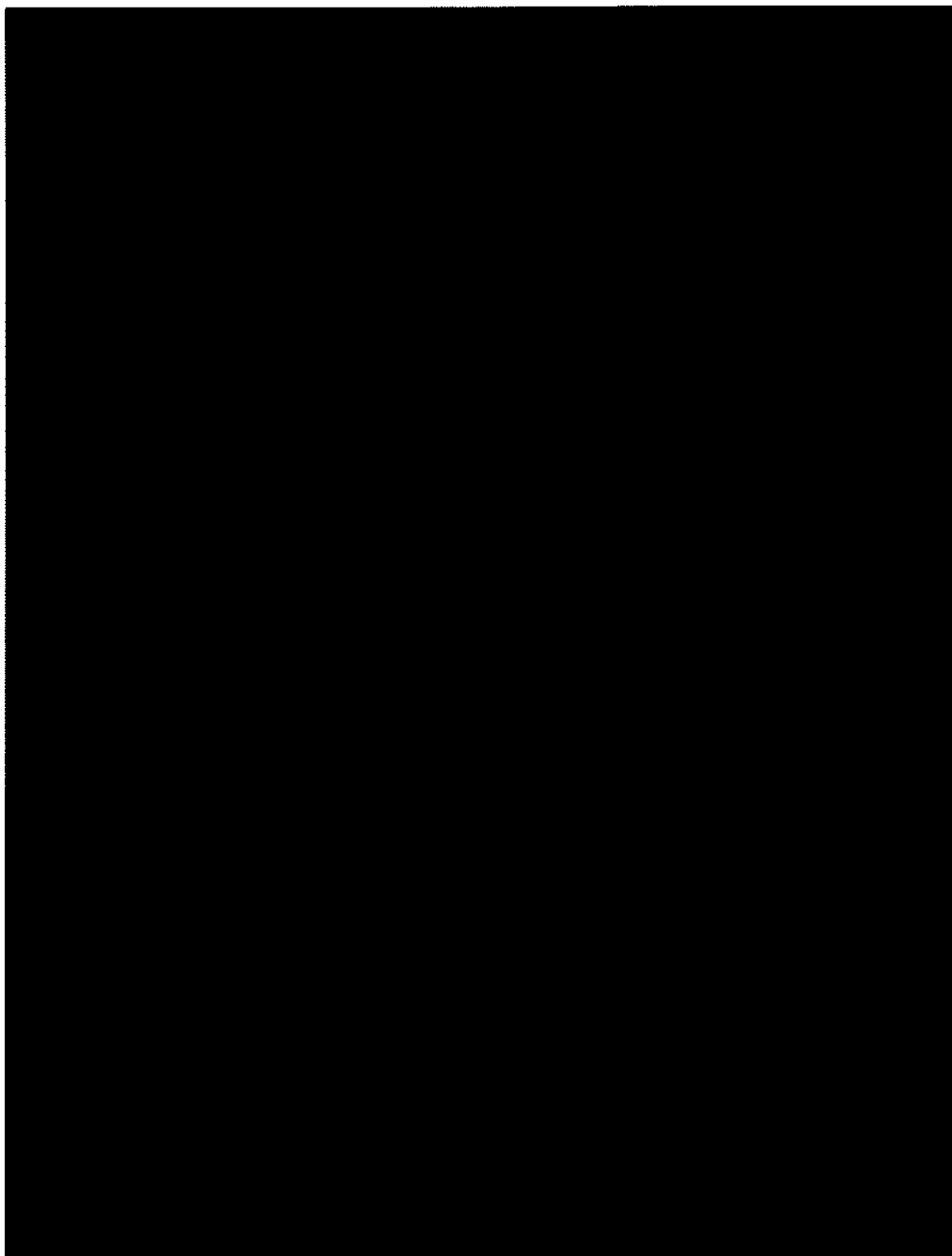
§ 1801(b)(2)(E) [50 U.S.C. § 1805(a)(3)(A)];

(c) each of the following telephone numbers,



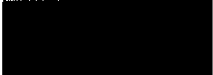
~~TOP SECRET//COMINT//NOFORN~~

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



at which the electronic surveillance is directed, is being used or is about to be used by

Various Known and Unknown Agents of 

 presumed U.S. persons, and electronic surveillance is authorized, using

for each facility either or both of the means identified below [50 U.S.C. § 1805(a)(3)(B)];

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

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

4. The minimization procedures proposed in the application have been adopted by the Attorney General and 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)].

The Court understands that the Government expects to file emergency FISA applications pursuant to 50 U.S.C. § 1805(f) seeking authority to intercept international communications to and from additional telephone numbers reasonably believed to be used by persons in the United States, where there arises probable cause to believe that such numbers are being used or are about to be used by known and unknown agents of [REDACTED]

[REDACTED] The Court understands that the Government has proposed a streamlined FISA emergency application form, attached as Exhibit G to the application, specifically and exclusively for this purpose. The Court finds that for any such application made under docket number [REDACTED] b(7)(E) the form of this proposed application is consistent with FISA subject to § 1805(d).

The Court also understands that the effectiveness of the surveillance proposed in this application and subsequent emergency applications made under this docket depends upon the manner of its operation remaining unknown to terrorists, and that it is critical to United States' counterterrorism operations that agents of [REDACTED] subject to such surveillance do not learn that they have been identified by the Government. The Court accordingly determines that the Government has established "good cause" within the meaning of section 1806(j) of Title 50 that a subject of emergency surveillance initiated by the Government

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

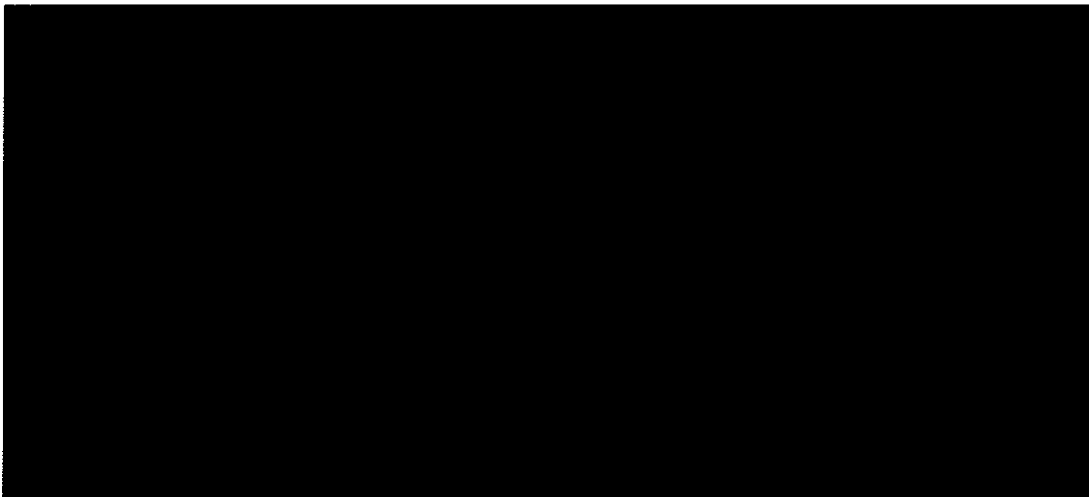
~~TOP SECRET//COMINT//NOFORN~~

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 forgo ordering the serving of the notice required under section 1806 (j) of Title 50.

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)]:

(1) 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 or places described in paragraph 3(c) above, subject to the minimization procedures specified in paragraph 4 above and specifically detailed in paragraph (3) below, for a period of **ninety days**, unless otherwise ordered by the Court, as follows:

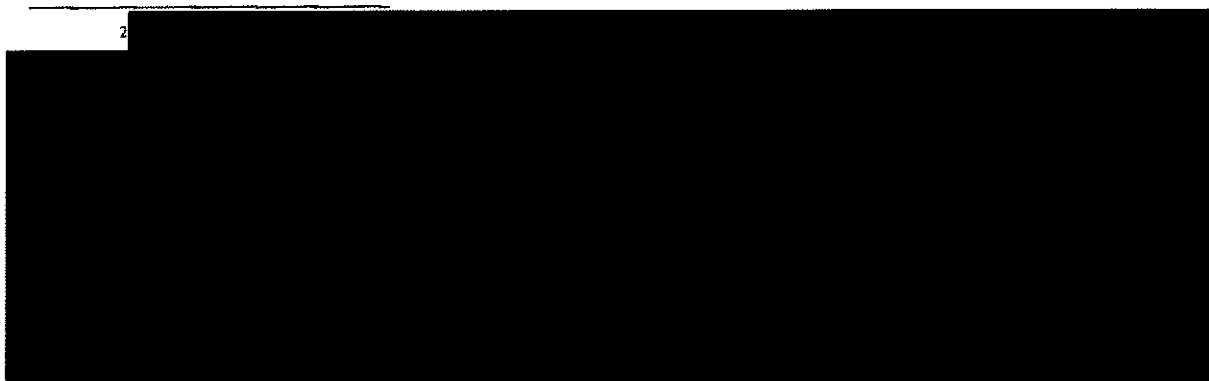


~~TOP SECRET//COMINT//NOFORN~~

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



2



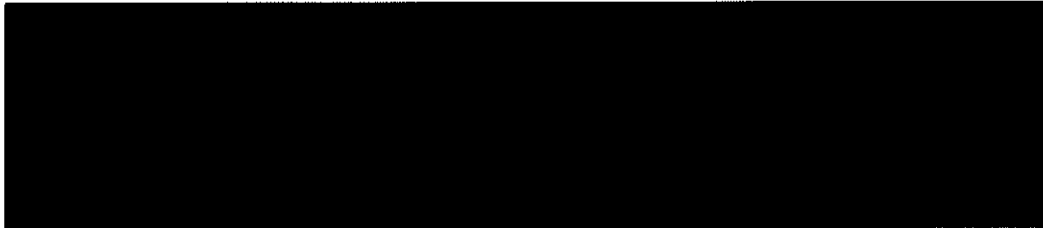
³ Although the NSA surveillance will be designed to acquire only international communications where one communicant is outside the United States, the Court understands that the communications infrastructure and the manner in which it routes communications do not permit complete assurance that no domestic 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~~

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

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



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, and/or technical assistance necessary to effect the authorities granted herein, or granted under any subsequent authorization made in connection with this docket number, all in accordance with the order 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)].

(3) As to all information gathered through the authorities requested herein, the NSA shall follow:

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

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

(a) The Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency (also known as Annex A to United States Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with this Court.

(b) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

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 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

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

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

(a) The Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency (also known as Annex A to United States Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with this Court.

(b) Certain of the modifications to the standard NSA FISA minimization procedures adopted by this Court in *In re Electronic Surveillance and Physical Search of International Terrorist Groups, Their Agents, and Related Targets*, Order, No. (7)(E) (May 10, 2002) ("*Raw Take Motion*"), which modifications are set forth below:

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 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

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

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

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:⁴

(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 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. 12,333 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. 12,333, 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.

⁴ and b(7)(E)

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

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

5. The following shall be added to the 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.

(c) The following additional modifications to these standard NSA FISA procedures:

1. Notwithstanding sections 3(c)(2) and (e), 5(b), and 6(a) of these standard NSA FISA procedures, communications acquired under this Order may be retained for five years, unless this Court approves retention for a longer period.

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~~

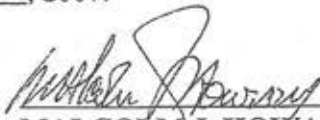
~~TOP SECRET//COMINT//NOFORN~~

(4) The CIA shall minimize all communications received under this Order as provided in Exhibit F to the application.

Signed 10 JAN 2007, 4:15 pm Eastern Time
Date Time

This authorization regarding Various Known and Unknown Agents of [REDACTED]

[REDACTED] presumed U.S. persons, expires at 3:00 pm
on the 6th day of APRIL, 2007.


MALCOLM J. HOWARD
Judge, United States Foreign
Intelligence Surveillance Court

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

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

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE [REDACTED] :

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

:

:

ORDER AND MEMORANDUM OPINION

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

I. INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

II. THE SURVEILLANCE AT ISSUE

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

²(...continued).

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

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

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

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

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

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

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

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

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

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

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

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

⁵ [REDACTED]

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

[REDACTED] Id. at 22 n.34.

⁷ [REDACTED]

(continued...)

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

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

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

⁷(...continued)

[REDACTED]

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

[REDACTED]

⁸

[REDACTED]

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

[REDACTED]

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

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

address does not appear to have been authorized under FISA prior to Docket No. [REDACTED] (b)(7)(E) and is discussed further below.

III. PROBABLE CAUSE FINDINGS

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

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

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

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

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

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

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

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

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

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

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

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

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

[REDACTED] Proposed Order at 2-6.

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

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

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

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

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

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

¹² The record does not disclose to what extent the surveillance conducted under Docket No. [REDACTED] (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. [REDACTED] (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]

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

In view of this apparent likelihood, the government’s implicit request that the Court exercise jurisdiction over the submitted application, the Court’s prior acceptance of jurisdiction in Docket No. [REDACTED] (b)(7)(E) and prior decisions of this Court that have accepted jurisdiction in similar cases [REDACTED] (b)(7)(E) and [REDACTED] (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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

circumstances, such as surveillances that acquired

Tellingly, none

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

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

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

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

(continued...)

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

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

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

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

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

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

¹⁹(...continued)

and b(7)(E) [REDACTED]

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

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

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

²² See notes 7 and 8 *supra*.

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

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

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

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

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

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

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

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

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

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

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

Contrary to this intent of Congress, the probable cause inquiry proposed by the government could not possibly restrain executive branch decisions to direct surveillance at any particular individual, telephone number or e-mail address. Under § 1805(a)(3)(B), the government would have the Court assess [REDACTED] See Alexander Decl. at 6-8, 11-12], and make a highly abstract and generalized probable cause finding [REDACTED] However, such a probable cause finding could be made with equal validity [REDACTED]

²⁵(...continued)

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

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

²⁷

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

IV. MINIMIZATION

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

specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Accordingly, it is hereby ORDERED as follows:

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

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

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

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

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

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

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

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

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


ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

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

[REDACTED] b(6) and b(7)(C)
I, [REDACTED] Clerk,
do hereby certify that this document
is a true and correct copy
of the original [REDACTED] b(6) b(7)(C)

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

b(6) and b(7)(C)

CLERK

UNITED STATES

02

FOREIGN INTELLIGENCE SURVEILLANCE COURT

U.S. Foreign Intelligence
Surveillance Court

WASHINGTON, D.C.

IN RE

(S)

Docket Number: b(7)(E)

SUPPLEMENTAL MEMORANDUM OF LAW IN SUPPORT OF APPLICATION FOR
AUTHORITY TO CONDUCT ELECTRONIC SURVEILLANCE OF

Classified by:

b(6) and b(7)(C)

Deputy Counsel

for Intelligence Operations, NSD, DOI

Reason: 1.4(c)

Declassify on: X1

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

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

INTRODUCTION (U)

This Court requested additional briefing in the above-captioned matter, in which the United States has sought authorization to establish an early warning system under the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. §§ 1801-1862, to alert the United States to international communications of members or agents of the [REDACTED] foreign powers:

[REDACTED]
Specifically, the Court requested an additional submission addressing whether the Application's request to [REDACTED] specifically described in the supporting documents is consistent with FISA's requirement that the application specify the "facilities or places at which the electronic surveillance is directed." 50 U.S.C. § 1804(a)(4)(B). The Court's questions concerned (i) whether [REDACTED]

[REDACTED]; and (ii) whether [REDACTED]
[REDACTED]
[REDACTED] As further explained below, the [REDACTED]

[REDACTED] as the "facilities" at which surveillance is "directed" is fully consistent with the plain and ordinary meaning of these statutory terms; with the overall structure and purpose of FISA; and with this Court's precedents.¹ ~~(TS//NF)~~

¹ The National Security Agency has reviewed this memorandum of law for factual accuracy. (U)

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

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

I. Directing Surveillance at the "Facilities" [REDACTED] Will Establish a Technologically Feasible and Effective Means for Collecting Vital Intelligence About the Targets that Would Otherwise Be Lost (S)-

One of the most serious challenges the United States confronts in its efforts to prevent another catastrophic terrorist attack on the Nation is the need quickly and effectively to track members and agents of international terrorist groups who manipulate modern technology in an attempt to communicate without detection. Declaration of John S. Redd, Director, National Counterterrorism Center ¶¶ 141-153 (Dec. 11, 2006) (Exhibit B to the Application) ("NCTC Declaration"). The [REDACTED] foreign powers that would be targeted by the proposed surveillance—[REDACTED]

[REDACTED]—pose the most serious of these threats. *Id.* ¶ 157. The Application proposes an "early warning" system under FISA aimed at addressing this national security imperative. The system would dramatically improve foreign intelligence surveillance of these target groups under FISA [REDACTED]

[REDACTED]² (TS//NF)

FISA authorizes the surveillance proposed in the Application. The Application satisfies FISA's statutory requirements by:

- establishing that there is probable cause to believe that the [REDACTED] of the surveillance are foreign powers, 50 U.S.C. § 1805(a)(3)(A); NCTC Declaration ¶¶ 7-134; Memorandum of Law in Support of Application for Authority to Conduct Electronic Surveillance of [REDACTED]

² [REDACTED]

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

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

[REDACTED]
at 15-22 (Dec. 12, 2006) (Exhibit A to the Application) ("Memorandum of Law");

- demonstrating that there is probable cause to believe that each of the facilities [REDACTED] is being used or is about to be used by a foreign power or its agents, 50 U.S.C. § 1805(a)(3)(B); Declaration of Lieutenant General Keith B. Alexander, Director of the National Security Agency ¶¶ 12-18, 38, 41, 44, 48, and 51-63 (Dec. 12, 2006) (Exhibit C to the Application) ("NSA Declaration"); Memorandum of Law at 33-36; and,
- setting forth rigorous and extensive minimization procedures that meet FISA's statutory standard, 50 U.S.C. § 1805(a)(4); Application ¶ 5; Memorandum of Law at 36-52.

As will be discussed in detail below, [REDACTED]

[REDACTED] are "facilities" as that term is used in FISA, and the surveillance proposed is "directed" at those facilities. It merits emphasis at the outset, however, why the Government has proposed the method of surveillance set forth in the Application—that is, why the more typical FISA approach would be inadequate to serve the critical early warning function that is the very purpose of the surveillance proposed in the Application. (~~S//SI//NF~~)

An effective early warning system must conduct surveillance with speed and agility that cannot be obtained through the more traditional approach of filing individual applications directed at specific e-mail addresses and phone numbers. To begin with, [REDACTED]

[REDACTED]

[REDACTED] Declaration of [REDACTED], NSA Program Manager for Counterterrorism Special Projects, National Security Agency ¶ 21 (Jan. 2, 2006) ("Supplemental NSA Declaration"). [REDACTED]

[REDACTED]

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

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

[REDACTED]

[REDACTED] NCTC Declaration ¶ 149; NSA Declaration ¶ 23; Supplemental NSA Declaration ¶¶ 15-16, 25. Were surveillance to be conducted by filing individual FISA applications for each new e-mail address and telephone number, the Court and the Government would confront a dramatic increase in emergency applications. The Government anticipates that, if the Application is approved, it will initiate collection [REDACTED] new telephone numbers and e-mail addresses each month. NSA Declaration ¶ 22; Supplemental NSA Declaration ¶¶ 19, 24. That would translate to filing a motion to amend a FISA order (or seeking Attorney General emergency authority) as many as [REDACTED] times each day, or filing one motion (or seeking one Attorney General authorization and filing a related application with the Court) covering as many as [REDACTED] new selectors each day if the surveillance were directed at specific telephone numbers and e-mail addresses. *See* Supplemental NSA Declaration ¶ 24. (TS//SI//NF)

But the difficulty with conducting the proposed surveillance using the more common framework of directing surveillance at specified telephone numbers and e-mail addresses to collect communications to and from them transcends the very real problem of resource constraints. Even if the Government were to seek emergency authorizations rather than filing individual applications with the Court before initiating collection on new telephone numbers and e-mail addresses, valuable intelligence *inevitably* would be lost, even given efficient processing of applications. *Id.* ¶ 25. [REDACTED]

[REDACTED] A significant advantage of allowing trained NSA analysts to make targeting decisions "on the ground" is that, once an analyst learns of a previously unknown telephone

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

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

number or e-mail address and determines that the number or address is reasonably believed to be used by a member or agent of [REDACTED] NSA generally can quickly initiate collection of communications to and from that number or address. *Id.* ¶ 22; *see also* NSA Declaration ¶ 23 (“Under established FISA procedures, NSA is unable to obtain authorization in time to immediately collect operational information sent to and from these new accounts, potentially losing vital information forever. . . . [T]he proposed collection procedures would permit NSA to rapidly analyze terrorist communications [and make it more likely for the NSA] to uncover quickly the existence of previously unknown terrorists.”). ~~(TS//SI//NF)~~

The collection of communications transmitted between the time that an NSA analyst could task an account and the time that the Attorney General would have been able to grant emergency authorization under section 105(f) of FISA is critical to the operation of the early warning system—it is always advantageous to collect intelligence as quickly as possible, and in some cases that information otherwise would be lost forever. *See* Supplemental NSA Declaration ¶¶ 23-25; NCTC Declaration ¶ 152 ([REDACTED])

[REDACTED]). In short, the proposed surveillance would enable collection of critical intelligence because the Government could target new telephone numbers and e-mail addresses with a higher degree of speed and agility than would be possible through the filing of individual FISA applications or requests for emergency approval. Supplemental NSA Declaration ¶¶ 23-24. ~~(TS//SI//NF)~~

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

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

And there are other ways in which the proposed surveillance would enable collection of communications that otherwise might not be acquired. Using the framework proposed in the Government's Application, rather than the more customary framework of directing surveillance at specified telephone numbers and e-mail addresses and collecting only communications to and from them, would allow the discovery and interception of new information about terrorist suspects. Supplemental NSA Declaration ¶ 27. [REDACTED]

[REDACTED] Obtaining these communications is essential to achieving the objectives of the proposed Order. ~~(TS//SI//NF)~~

[REDACTED] the NSA can collect communications not only to and from a tasked e-mail address, but also communications in which a tasked e-mail address appears in the substantive contents of a communication between two third parties. Supplemental NSA Declaration ¶ 28. (For example, [REDACTED]

[REDACTED] *Id.* ¶ 28.) [REDACTED]

[REDACTED] *Id.* ¶ 27. [REDACTED]

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

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



For all the reasons described above, by [REDACTED]

[REDACTED] the Government's

proposed surveillance would collect vital intelligence information that otherwise would be lost,

and thereby invaluablely contributes to the proposed early warning system under FISA. ~~(S//SI//NF)~~

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

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

II. The "Early Warning" System Set Forth in the Application is Fully Consistent With FISA (S)

A. FISA Establishes a Flexible and Common-Sense Regime for the Conduct of Foreign Intelligence Surveillance (U)

When it enacted FISA in 1978, Congress recognized the need for flexibility in the field of foreign intelligence collection. *See* H.R. Rep. No. 95-1283, Pt. I, at 27 (1978) ("No means of collection are barred by the bill, and the circumstances justifying collection are fully responsive to the intelligence agencies' needs as they have been expressed to this committee."); *see also id.* at 38 (1978) (explaining that the term "clandestine intelligence gathering activities" used in FISA "is supposed to be flexible with respect to what is being gathered because the intelligence priorities and requirements differ between nations over time, and this bill is intended to allow surveillance of different foreign powers' intelligence activities well into the future"). Congress prudently recognized that different methods of conducting electronic surveillance may be necessary to address different foreign intelligence threats. Accordingly, FISA places few specific constraints [REDACTED]

[REDACTED] at which surveillance may be directed. Nor does FISA reflect (as does its criminal analogue, Title III, 18 U.S.C. §§ 2510-2522) a statutory directive regarding the particular manner in which the information collected through electronic surveillance must be minimized.⁴ Instead, the central findings that the Court must make in exercising jurisdiction over the proposed electronic surveillance are straightforward and few: that there is probable cause to believe that the target is a foreign power or an agent of a foreign power, *see* 50 U.S.C.

⁴ *See* 18 U.S.C. § 2518(5) (requiring that interception "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under" Title III). FISA's legislative history confirms that FISA was not intended to have Title III's more stringent requirements for minimization at the point of acquisition. *See* H.R. Rep. 95-1293, pt. I, at 56 (1978) ("It is recognized that given the nature of intelligence gathering, minimizing acquisition should not be as strict as under [Title III]."). (U)

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

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

§ 1805(a)(3)(A); that there is probable cause to believe that "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," *id.* § 1805(a)(3)(B); and that the "proposed minimization procedures meet the definition of minimization procedures" under FISA, *id.* § 1805(a)(4). The term "minimization procedures," in turn, is defined fundamentally by reference to the surveillance's reasonableness; these procedures must be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination" of certain U.S. person information "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." *Id.*

§ 1801(h)(1). (S)

When considered together, these requirements establish a flexible, common-sense regime that allows the Government to propose, and the Court to approve, a wide range of methods for conducting foreign intelligence surveillance. This flexibility allows FISA to serve as a powerful tool for foreign intelligence collection while at the same time protecting the privacy of United States persons. FISA accomplishes these two objectives by placing few constraints on the manner in which surveillance is conducted, but at the same time requiring court-approved minimization procedures that are reasonable in light of the overall purpose and technique of the surveillance. *See* 50 U.S.C. § 1801(h); *see also* H.R. Rep. No. 95-1283, Pt. I, at 55 (1978) ("It is recognized that minimization procedures may have to differ depending upon the technique of the surveillance."). If the nature of the target (including the target's tradecraft) or the technology involved renders it advantageous to define the facilities broadly, FISA does not preclude the surveillance; instead, it allows the Government to conduct the surveillance if the Government

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

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

adopts rigorous minimization procedures, approved by this Court, that ensure that the privacy interests of U.S. persons are properly protected. *See, e.g.*, H.R. Rep. No. 95-1283, Pt. I, at 55 (1978) (“[I]n many cases it may not be possible for technical reasons to avoid acquiring all information. In those situations, the reasonable design of procedures must emphasize the minimization of retention and dissemination.”). (S)

As will be explained in detail below, this Court’s practice and precedents reflect the flexibility inherent in FISA’s statutory scheme. This Court has frequently authorized the Government to conduct surveillance in unique ways in response to changing technologies or difficult foreign intelligence challenges, after assuring itself that the surveillance would be conducted in a manner that reasonably protected the privacy interests of U.S. persons.⁵ *See infra* § II.B.2. Viewed in this light, the Court’s approval of this unique Application—under which surveillance would be [REDACTED] but would be conducted pursuant to extensive and rigorous minimization procedures—would be fully consistent with the text of FISA, its broader purpose, and this Court’s precedents. (TS//NF)

B. [REDACTED]

[REDACTED] Constitute “Facilities” Under
FISA (TS)

This Court has specifically inquired about whether the term “facilities” in FISA limits the Government to directing surveillance at individual e-mail addresses and telephone numbers [REDACTED]

⁵ In emphasizing the flexibility that inheres in FISA, the Government is not suggesting that FISA requires this Court to approve surveillance once it finds that a particular application proposes surveillance that would be “directed” at “facilities” as those terms are used in FISA. This Court retains considerable discretion to determine that proposed minimization procedures meet the definition of minimization procedures under FISA, and to determine whether the surveillance meets the requirements of the Fourth Amendment. (U)

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

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

[REDACTED]

[REDACTED] would be consistent with FISA's statutory scheme, which allows the Government the flexibility to optimize surveillance against national security threats, subject to reasonable minimization procedures, in order to achieve the objectives of the particular surveillance. *See supra* § II.A. As shown below, this understanding of the word "facilities" also is consistent with the plain meaning of the term and with this Court's precedents. ~~(TS//NF)~~

1. [REDACTED]

[REDACTED]

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

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

2. [REDACTED]

The breadth and flexibility of the term “facilities” in FISA are confirmed by this Court’s precedents. As set forth in detail in the Government’s memorandum of law, Memorandum of Law at 26-31, this Court has on numerous occasions authorized surveillance under applications that identified the “facility” [REDACTED]

[REDACTED] Most notably, in [REDACTED] Opinion and Order, No. PR/TI [REDACTED] (July 14, 2004) ([REDACTED]), this Court accepted the Government’s submission that [REDACTED] were “facilities” within the meaning of Title IV of FISA, explaining that the statute’s plain language did not “restrict the use of trap and trace devices to communications facilities associated with individual users.” *Id.* at 23.⁶ ~~(TS//NF)~~

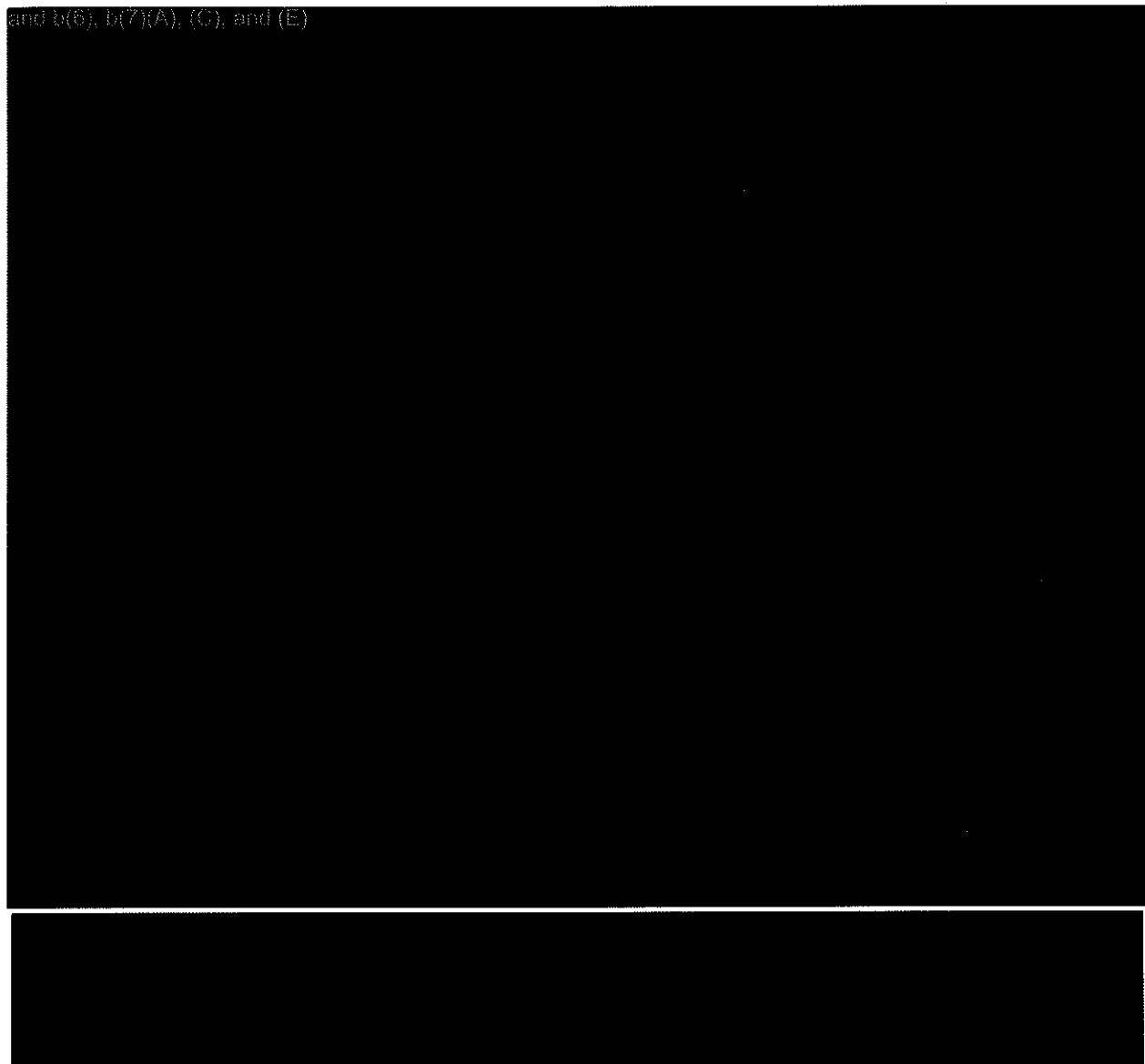
This Court has also frequently approved applications for electronic surveillance directed at “facilities” other than individual e-mail accounts or telephone numbers. For example, in [REDACTED] and b(7)(A) [REDACTED]

6 [REDACTED]

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

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

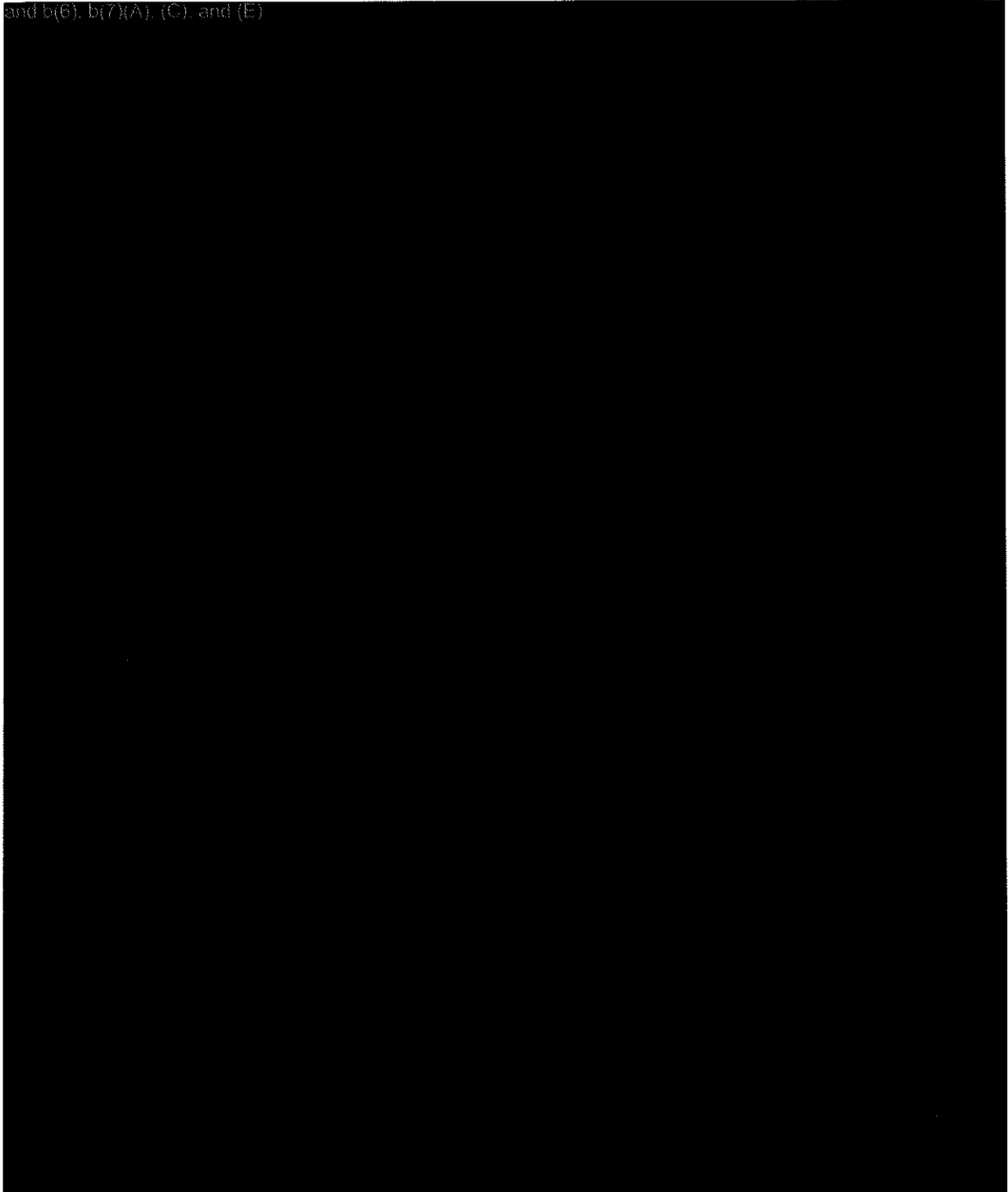
and b(6), b(7)(A), (C), and (E)



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

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

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



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

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

and b(7)(E)



3.



(S)



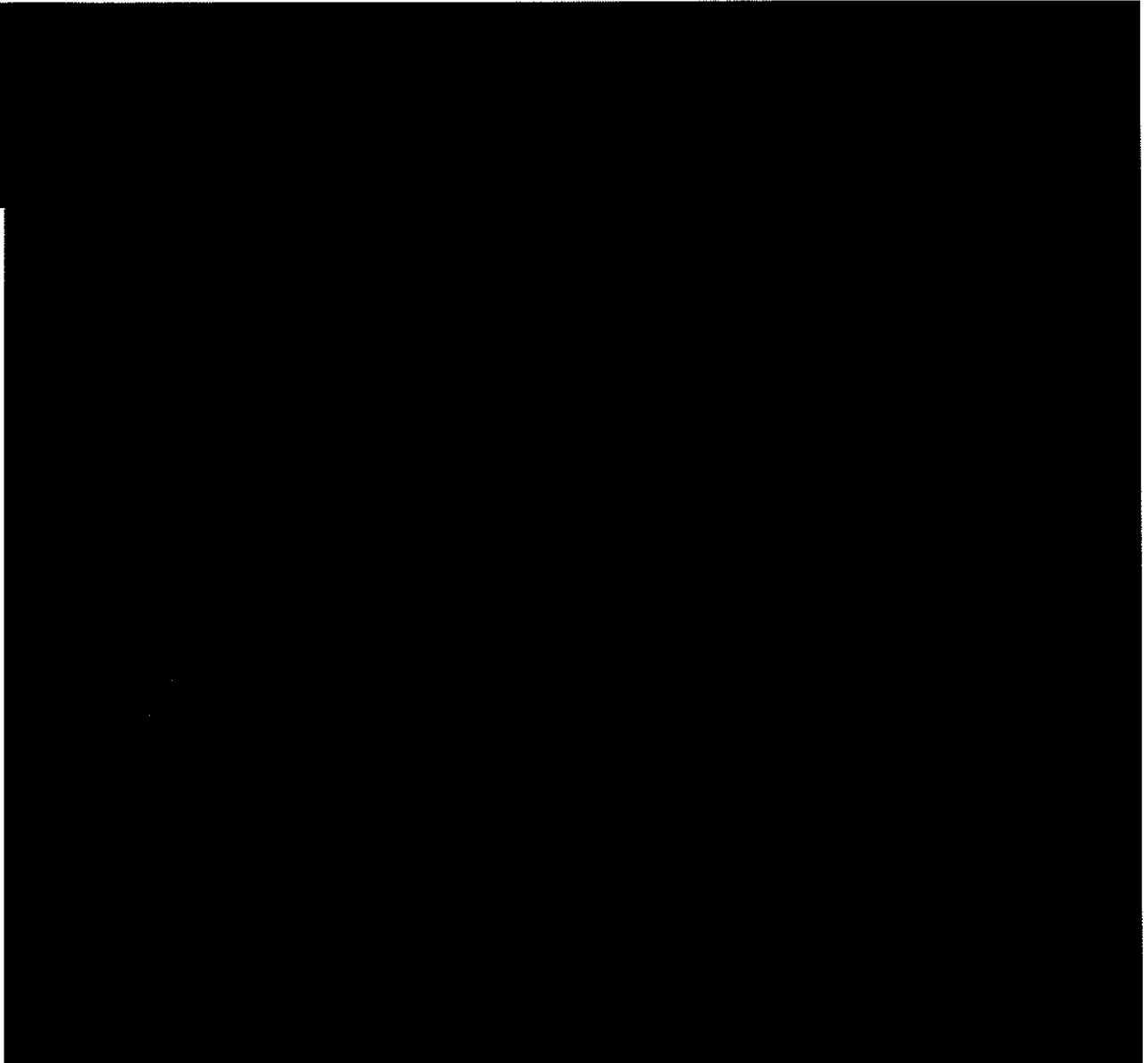
(TS//NF)

8



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

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



C. The Surveillance Proposed in the Application Would Be “Directed” at the Facilities [REDACTED] (U)

This Court has also asked whether the surveillance proposed is properly understood to be “directed” at the facilities [REDACTED]; the suggestion, as the Government understands it, is that the surveillance might be better understood as “directed” instead at the e-mail addresses and numbers the Government would task for collection under the proposed Order.

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

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

This question relates closely to the “facilities” question addressed above, and accordingly many of the arguments previously discussed—such as the flexibility that inheres in FISA’s statutory scheme, *supra* § II.A, [REDACTED]

[REDACTED] *supra* § II.B—also support the Government’s position. In the interests of completeness, however, this section explains why FISA clearly permits surveillance to be “directed” at the facilities [REDACTED]

[REDACTED] (TS) [REDACTED]

1. *The Plain Language of FISA Permits Surveillance to Be* [REDACTED]

(S)

FISA requires the applicant to set forth facts showing that “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.” 50 U.S.C. § 1804(a)(4)(B) (emphasis added); *see also id.* § 1805(a)(3)(B), § 1805(c)(1)(B). Because FISA does not define the term “directed,” we look to its ordinary meaning. *See, e.g., Engine Mfrs. Ass’n v. South Coast Air Quality Mgmt. Dist.*, 541 U.S. 246, 252 (2004) (“Statutory construction must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose.”) (quotations and citations omitted). The ordinary understanding of the term “directed” is that it refers to the places or facilities at which the Government intends to direct, or point, the surveillance device; that is, where the communications will be intercepted or the information acquired. *See Funk & Wagnalls New Standard Dictionary of the English Language* 718 (1946) (defining “direct” as “[t]o determine the direction of; especially, to cause to point or to go straight toward a thing”); *see also IV The Oxford English Dictionary* 701 (2d ed. 1989)

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

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

(defining "direct" as "[t]o cause (a thing or person) to move or point straight to or towards a place"). [REDACTED]

[REDACTED] (TS//NF)

This understanding is supported by the language of the relevant provisions, which refers to the facilities and *places* at which surveillance may be "directed." 50 U.S.C. § 1804(a)(4)(B); *see also id.* § 1805(a)(3)(B), § 1805(c)(1)(B). [REDACTED]

[REDACTED] Of course, the word "directed" should be understood to have the same meaning when it is read with respect to "facilities" as it does when it is read in conjunction with the term "places." *Cf. Brown v. Gardner*, 513 U.S. 115, 118 (1994) (The presumption that a term has the same meaning throughout a statute is "most vigorous when [the term] is repeated within a given sentence."). (S)

The conclusion that the surveillance at issue will be "directed" at the facilities [REDACTED] is confirmed by the relevant language of Title III's criminal wiretap provisions, on which this specific part of FISA, section 104(a)(4)(B), was based. *See* H.R. Rep. No. 95-1283, Pt. I, at 75 (1978) (section 104(a)(4)(B) of FISA "parallels existing law on surveillances

⁹ For example, as explained in the Memorandum of Law at 32-33. [REDACTED]

[REDACTED] (TS//SI//NF)

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

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

for law enforcement purposes"); *see also West Virginia Univ. Hosps., Inc. v. Casey*, 499 U.S. 83, 100 (1991) (citation omitted) ("[W]e construe [statutory terms] to contain that permissible meaning which fits most logically and comfortably into the body of both previously and subsequently enacted law."). Title III requires applications to contain "a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted." 18 U.S.C. § 2518(1)(b)(ii). To the extent there is any doubt, Title III's parallel provisions confirm the common-sense interpretation of "the facilities . . . at which the electronic surveillance is directed" described above: [REDACTED]

[REDACTED] (S)-

2. [REDACTED]

[REDACTED] FISA requires the Government's application to include "a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . 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." 50 U.S.C. § 1804(a)(4)(B). [REDACTED]

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

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

[REDACTED]
[REDACTED] (S)

[REDACTED]
[REDACTED]
[REDACTED] The Court's order must specify "the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known." *Id.* § 1805(c)(1)(B). The phrase "if known" means that the order does not have to specify the nature and location of each of the facilities at the time the order is issued if that is not possible. *See* H.R. Conf. Rep. No. 107-328, at 24 (2001) (addition of phrase "if known" to section 1805(c)(1)(B) "is designed 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"). [REDACTED]

[REDACTED]
[REDACTED] Here, the nature and location of the facilities at which surveillance will be directed is known and has been described in detail, *see* NSA Declaration ¶¶ 37, 40, 43, 46, 51-63, and can easily be specified by the Court in its order.

(S//SI)

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

[REDACTED]

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

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

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

In any event, here the Government cannot identify at the time of the Application all of the telephone numbers and e-mail addresses that would be tasked for collection under the proposed Order.¹⁰ The whole objective of the proposed surveillance is to establish an early warning system that would enable the Government to uncover currently unknown telephone numbers and e-mail addresses used by members and agents of the [REDACTED] foreign powers to communicate into and out of the United States, and quickly to collect the communications to and from those numbers and addresses without missing vitally important communications—the acquisition of which could mean the difference in our efforts to thwart the next catastrophic terrorist attack on the United States.¹¹ Moreover, as explained above, see *supra* at 6-7, there are several categories of e-mail communications—such as communications that include a reference to a tasked e-mail address—that in fact are *not* captured through the traditional approach of intercepting only communications to and from a particular tasked address. [REDACTED]

¹⁰ Although the NSA will within the first authorization period provide the Court with a list of [REDACTED] foreign numbers and addresses from which it would like initially to collect communications, even that list will be subject to change as intelligence priorities shift and new information is uncovered. Supplemental NSA Declaration ¶ 19. (TS//SI//NF)

¹¹ The specific telephone numbers and e-mail addresses to be targeted will be identified by NSA analysts during the course of the proposed surveillance, and will be approved by the Court. Application ¶ 5. (TS//SI//NF)

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

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

[REDACTED]

[REDACTED]

(S//SI)

3.

[REDACTED]

(S)

[REDACTED]

See 50 U.S.C. § 1801(h)(1) (minimization procedures are “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”) (emphasis added); [REDACTED] and b(7)(A)

[REDACTED]

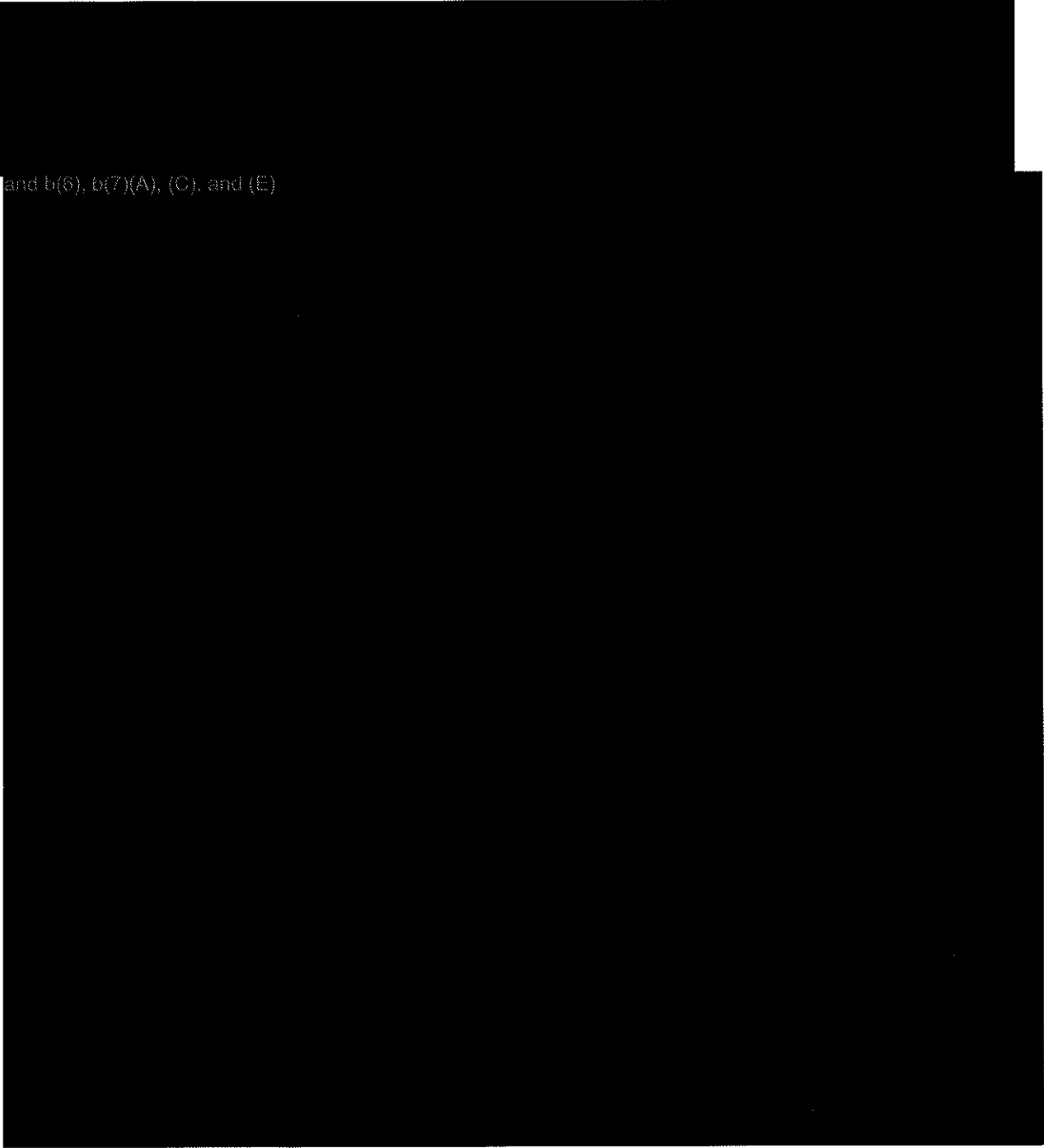
see also H.R. Rep. No. 95-1283, Pt. I, at 55-56 (1978) (“By minimizing acquisition, the committee envisions, for example, that . . . where a switchboard line is tapped

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

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

but only one person in the organization is the target, the interception should probably be discontinued where the target is not a party.”) (TS)

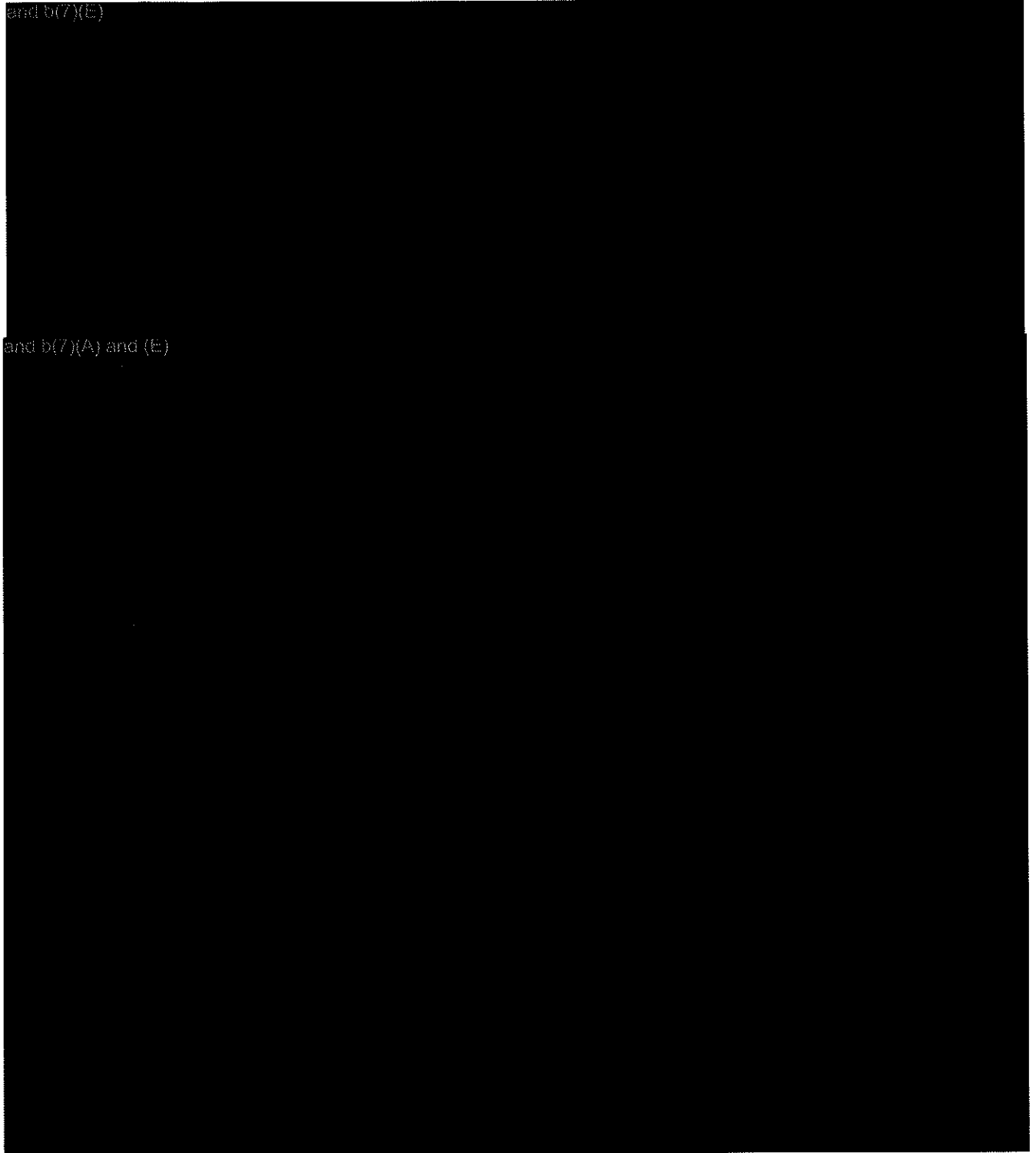
and b(6), b(7)(A), (C), and (E)



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

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

and b(7)(E)



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

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

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

4.

~~(S)~~

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

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

the more typical FISA approach of filing separate FISA applications directed at specific telephone numbers and e-mail addresses would be inadequate to serve the objective of the surveillance—to establish an effective “early warning” system under FISA to detect and

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

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

prevent a catastrophic terrorist attack. *Supra* § I. [redacted] and b(6), b(7)(A), (C), and (E)

[redacted] (S)

[redacted] and b(7)(A) and (E)

[redacted] the proposed surveillance will target for

collection only international communications of individuals the Government has probable cause to believe are members or agents of the [redacted] foreign powers.¹² Memorandum of Law at 36-41.

[redacted] (S)

[redacted] and b(7)(A) and (E)

[redacted] In this case, the Government

confronts a unique and formidable foreign intelligence challenge—the threat posed by shadowy and nebulous terror networks that exploit modern telecommunications technology in an effort to

¹² As noted in the Government's initial Memorandum of Law, [redacted] and b(6), b(7)(C) and (E)

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

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

communicate without detection—and seeks to meet it by directing surveillance [REDACTED]

[REDACTED] subject to exacting minimization procedures. [REDACTED]

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

[REDACTED] (S)

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

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

CONCLUSION (U)

For the foregoing reasons and the reasons set forth in the Government's initial Memorandum of Law, the Court should grant the requested Order. (U)

Respectfully submitted,

Dated: January 2, 2007

ALBERTO R. GONZALES
Attorney General

STEVEN G. BRADBURY
*Acting Assistant Attorney General,
Office of Legal Counsel*

JOHN A. EISENBERG
*Deputy Assistant Attorney General,
Office of Legal Counsel*

KENNETH L. WAINSTEIN
*Assistant Attorney General,
National Security Division*

MATTHEW G. OLSEN
*Acting Deputy Assistant Attorney General,
National Security Division*

BRETT C. GERRY
*Deputy Assistant Attorney General,
National Security Division*

b(6) and b(7)(C)

*Senior Counsel,
Office of Legal Counsel*

U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

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

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

APPROVED FOR PUBLIC RELEASE

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

2007 APR -4 PM 5:19

WASHINGTON, D. C.

CLERK

IN RE

:

: Docket Number:

:

(S):

ORDER

The United States of America has applied, pursuant to section 105(e)(2), 50 U.S.C. § 1805(e)(2), of the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801-1811 ("FISA" or "the Act"), for an extension of the orders issued in the above-captioned docket number (hereinafter "application for an extension").

The Court has given full consideration to the matters set forth in the Government's application for an extension and finds as follows:

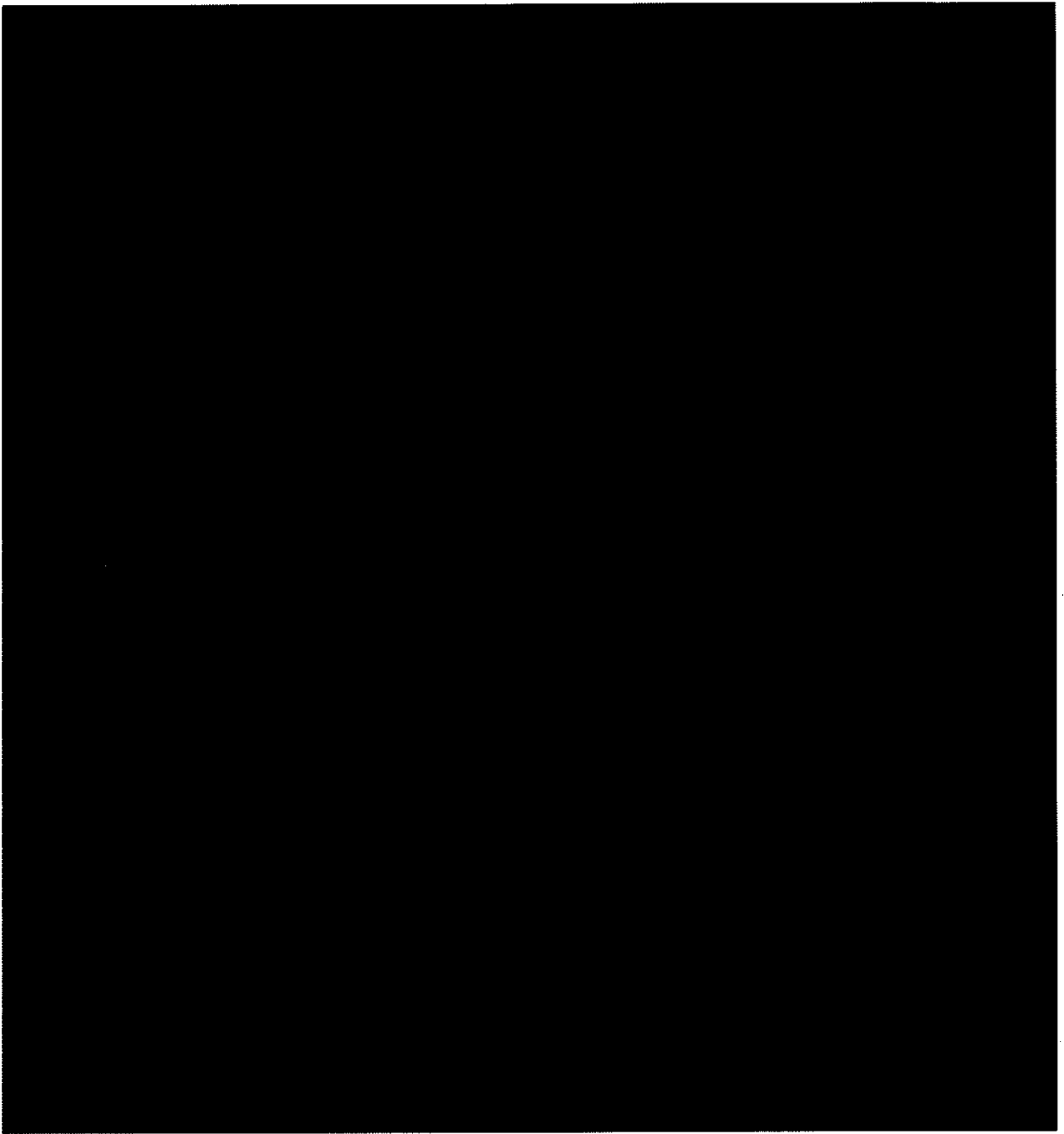
1. The President has authorized the Attorney General of the United States to approve applications for electronic surveillance for foreign intelligence information [50 U.S.C. § 1805(a)(1)];
2. The application has been made by a Federal officer and approved by the Attorney General [50 U.S.C. § 1805(a)(2)];

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

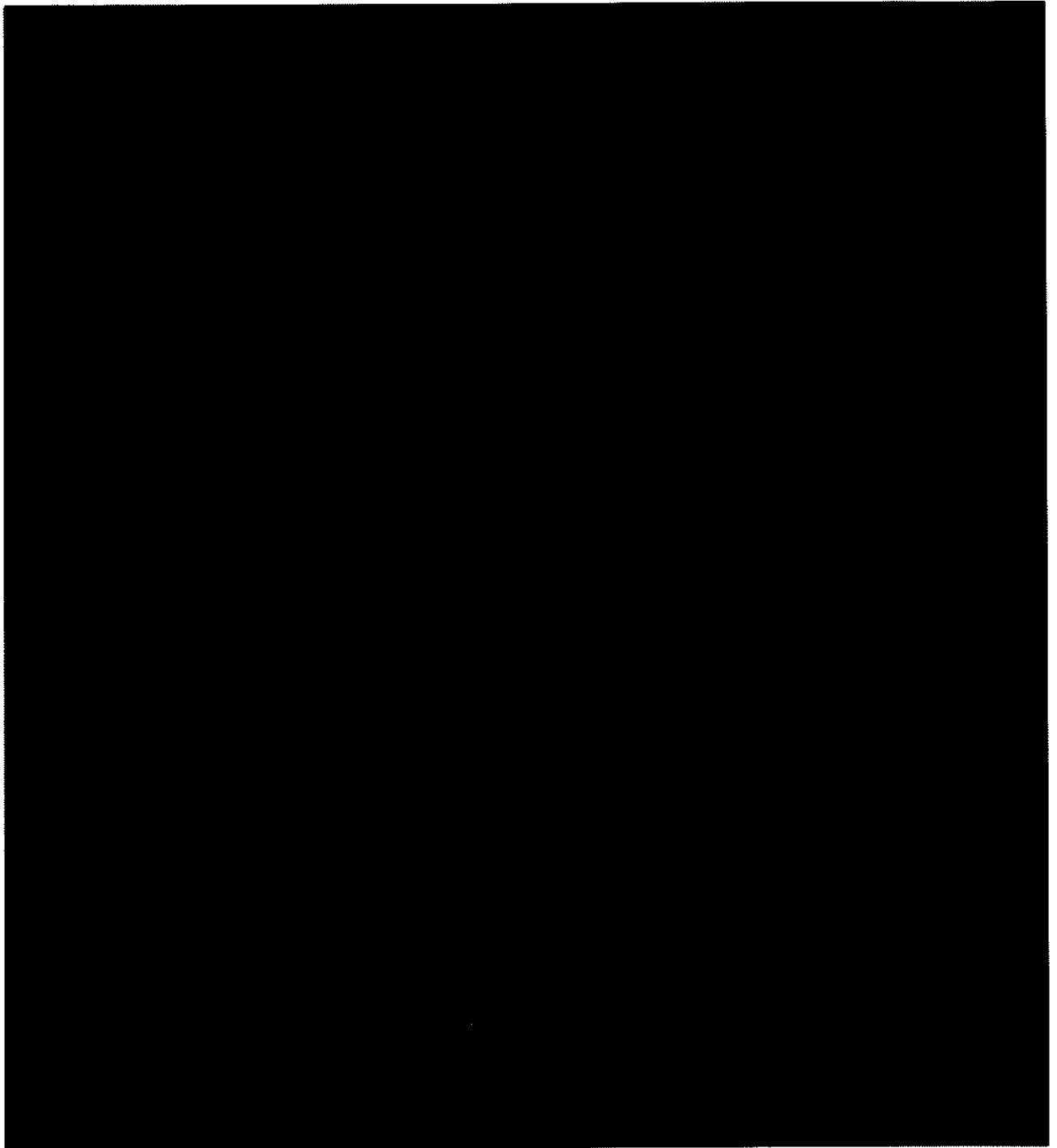
Derived from: Application to the USFISC in

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

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~~

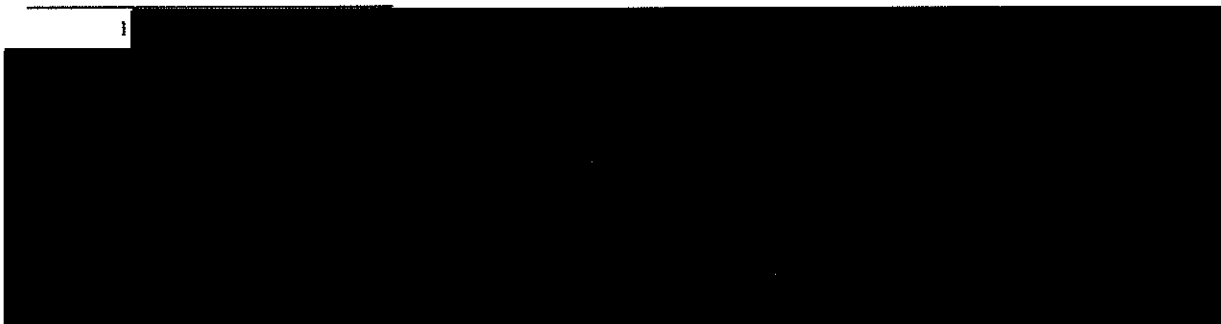


TOP SECRET//COMINT//NOFORN

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



1



2



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

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

(c) each of the facilities [REDACTED] 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 Exhibit A to the application for an extension [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 for an extension 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)].

WHEREFORE, IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application of the United States for an extension of the orders issued in the above-captioned docket number, as described in the application for an extension, is GRANTED, and it is

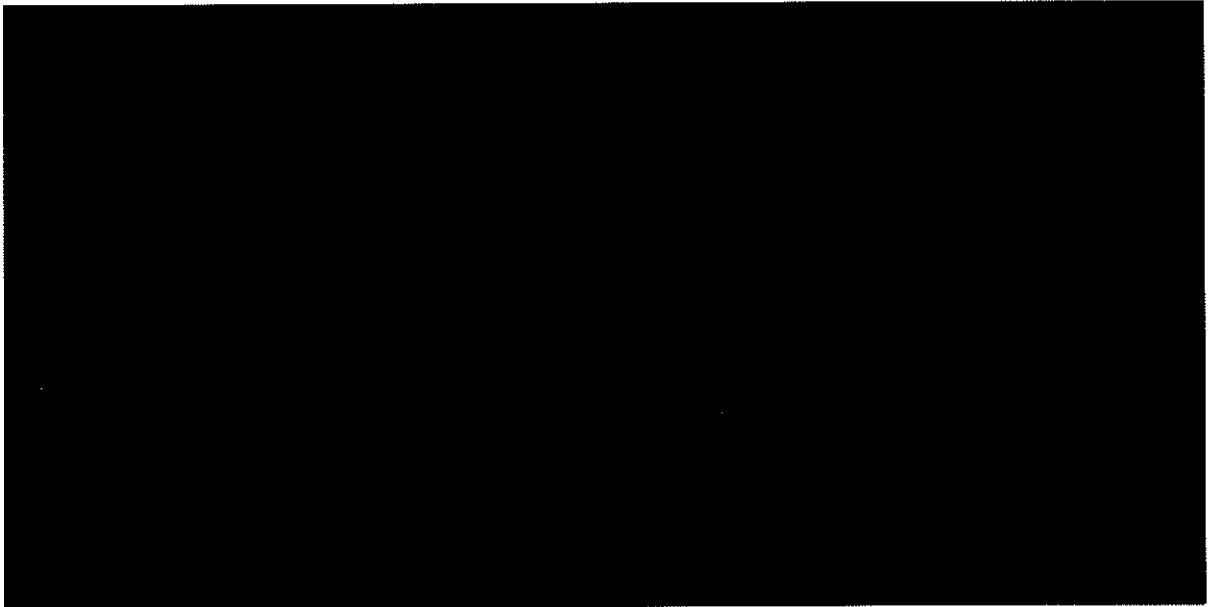
[REDACTED]

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

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

FURTHER ORDERED, as follows [50 U.S.C. § 1805(c)-(e)]:

(1) The orders issued in the above-captioned docket number, which authorized the United States 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 or places described in paragraph 3(c) above, subject to the minimization procedures specified in paragraph 4 above, including the application of the "minimization probable cause standard" specified below, are hereby extended for the period specified herein, as follows:



3



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

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

[REDACTED], NSA shall collect only communications that meet the minimization probable cause standard. In addition, with respect to communications that meet the minimization probable cause standard, the NSA

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] NSA shall collect only communications that meet the minimization probable cause standard. In addition, with respect to communications that meet the minimization probable cause standard, the NSA

[REDACTED]

[REDACTED]

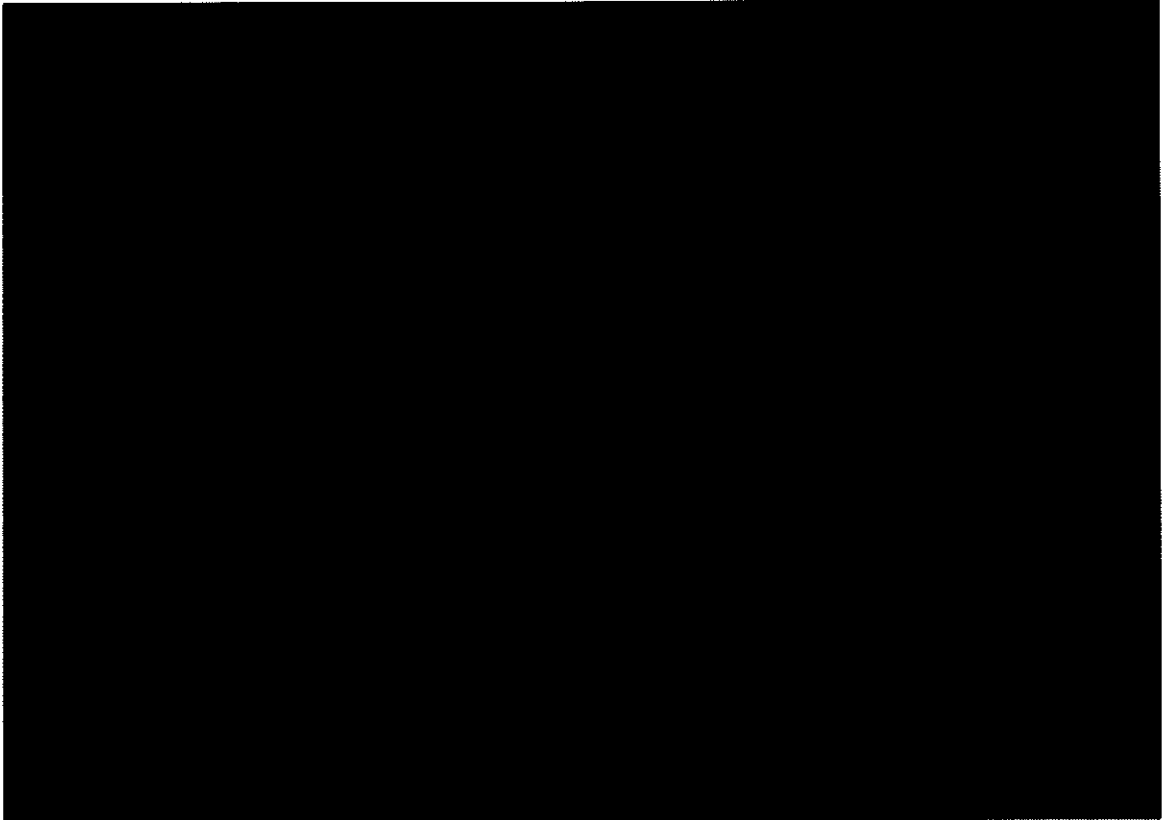
[REDACTED]

[REDACTED]

⁴ Although the NSA surveillance will be designed to acquire only international communications where one communicant is outside the United States, the Court understands that the communications infrastructure and the manner in which it routes communications do not permit complete assurance that this will be the case. 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~~



⁵ The Court understands that the system will select for delivery to NSA not only international Internet communications to and from agents or members of [REDACTED]

[REDACTED] but also Internet communications in which e-mail addresses [REDACTED] of such agents or members are mentioned in the Internet communication.

⁶

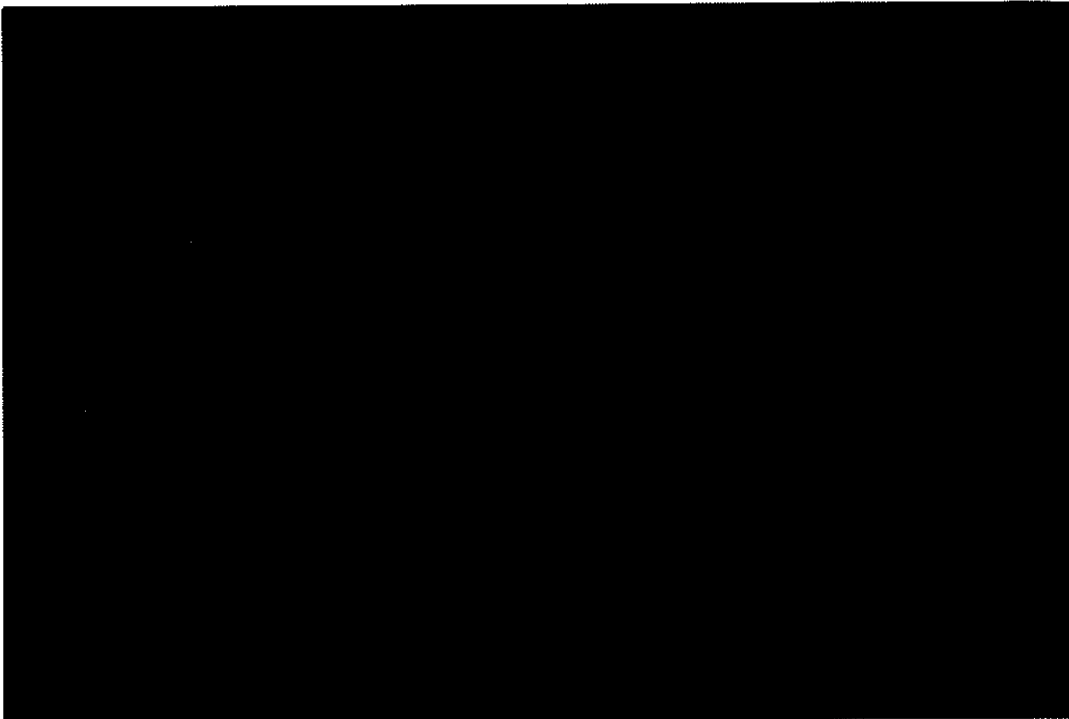


⁷

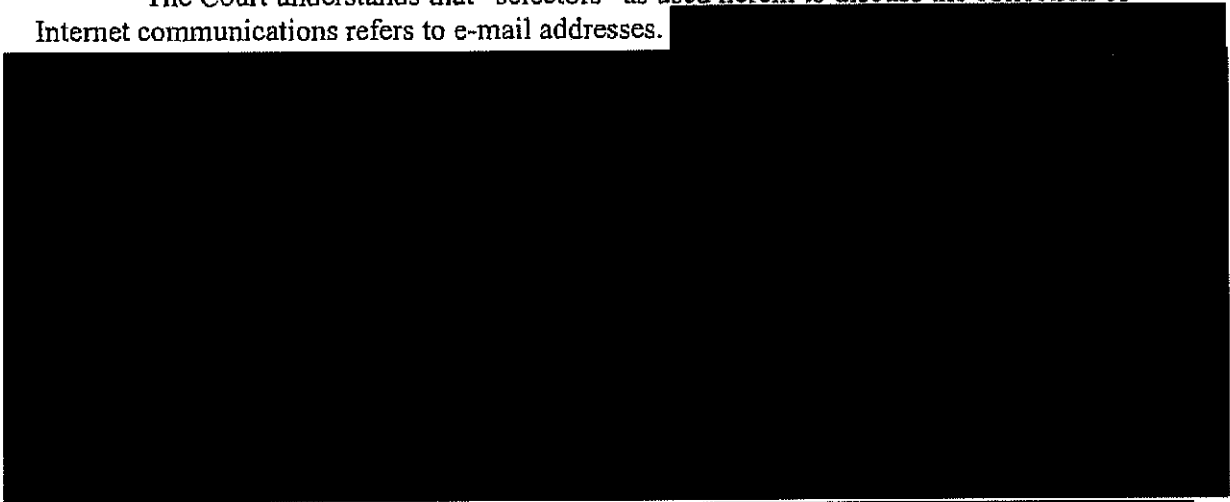


~~TOP SECRET//COMINT//NOFORN~~

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



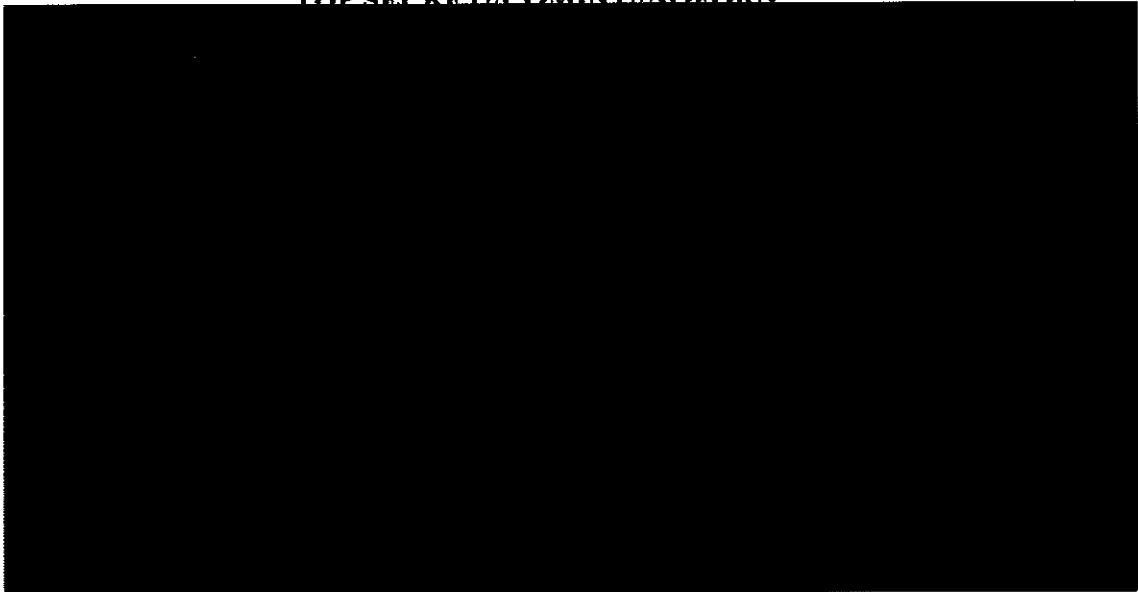
⁸ The Court understands that "selectors" as used herein to discuss the collection of Internet communications refers to e-mail addresses.



NSA shall handle non-target communications acquired as a result of this technical limitation in accordance with its standard FISA minimization procedures, as modified herein.

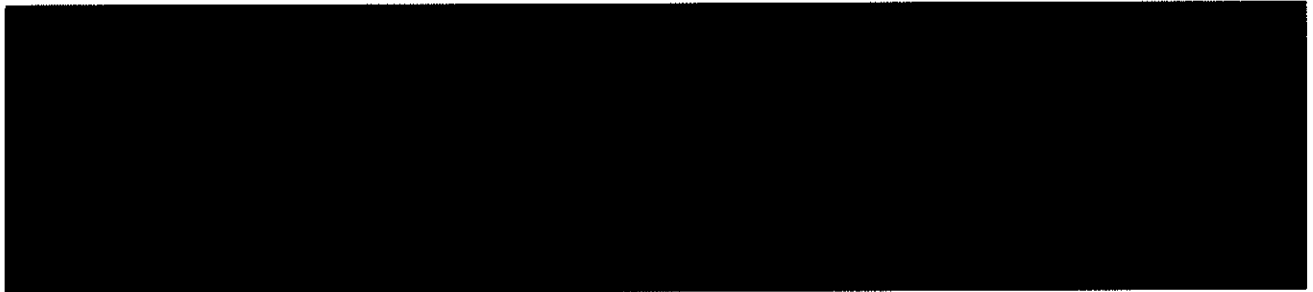
~~TOP SECRET//COMINT//NOFORN~~

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

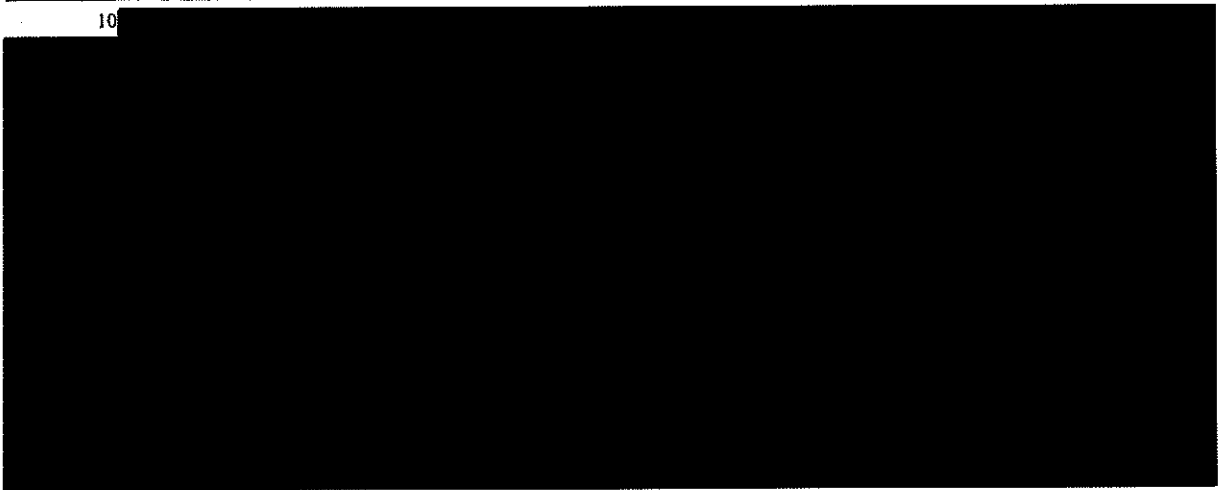


Unconsented physical entry is not authorized to implement the electronic surveillance approved herein.

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



10



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

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

[REDACTED]

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, and/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)].

(3) As to all information gathered through the authorities requested herein, the NSA shall follow the minimization probable cause procedure set forth below:

Minimization Probable Cause Standard. NSA shall apply two criteria in selecting communications to target for collection, both of which shall apply in each instance. First, NSA shall compile and update a list of telephone numbers and e-mail addresses (together, "selectors") for which it has determined, based on the totality of circumstances, there is probable cause to believe that the particular selector is used by [REDACTED]

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

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



Second, NSA shall acquire only communications for which there is probable cause to believe that at least one of the communicants is outside the United States. Together, these two criteria constitute the "minimization probable cause standard."

Use of Foreign Selectors. All selectors shall be telephone numbers or e-mail addresses that NSA reasonably believes are being used by persons outside the United States.¹¹

NSA Process for Determining that the Minimization Probable Cause Standard Has Been Met. All telephone numbers and e-mail addresses NSA analysts seek to use as a basis for acquiring communications from the facilities [REDACTED]

[REDACTED] shall be entered into a database that will show the telephone number or e-mail address the analyst has probable cause to believe is used by a member or agent of [REDACTED]

[REDACTED] and a statement of the

¹¹ The Court understands that a selector that NSA reasonably believes is being used outside the United States may on occasion be used in the United States. If NSA discovers that it has acquired communications from a selector while that selector was being used inside the United States, NSA shall handle any such inadvertently acquired communications as provided in the minimization procedures described in this Order.

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

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

reasons for such a belief. [REDACTED] as described in Exhibit A to the application for an extension. The proposed number or e-mail address and supporting documentation shall be reviewed by officials from the [REDACTED] Branch within NSA.¹² Prior to initiating acquisition of communications to or from a telephone number or to, from, or concerning an e-mail address [REDACTED] NSA officials from the [REDACTED] [REDACTED] Branch shall confirm that documentation regarding the first prong of the minimization probable cause standard is present in the file. If the reviewing officials find that the standard has not been documented appropriately, the telephone number or e-mail address will remain in the database, but shall be ineligible for tasking and will be designated as such.

Additional Oversight. The NSA shall apply the following additional oversight. The NSA's Inspector General (IG), General Counsel (GC), and the Signals Intelligence Directorate's Office of Oversight and Compliance shall each periodically review this electronic surveillance to ensure that it is being carried out lawfully, including that the processing and dissemination of U.S. person information is being accomplished in accordance with the procedures described herein.

¹² The Court understands that NSA is considering assigning this duty to another NSA component. If such a change in the assignment of this duty occurs and if different officials will determine whether proper documentation exists to support the determination that specific telephone numbers, e-mail addresses [REDACTED] meet the minimization probable cause standard, the Government shall inform the Court in the next application for a renewal of the Court's authorization.

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

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

Review by the Department of Justice and Reporting to this Court:

- (i) An attorney from the National Security Division at the Department of Justice shall review the NSA's justifications for targeting selectors.
- (ii) The Government shall submit a report to the Court every thirty (30) days listing new selectors that the NSA has tasked during the previous thirty days and briefly summarizing the basis for the NSA's determination that the first prong of the minimization probable cause standard has been met for each new selector.
- (iii) At any time, if the Court finds that there is not probable cause to believe that any particular selector is used by a member or agent of [REDACTED]

[REDACTED] the Court may direct that surveillance under this Order shall cease on that selector expeditiously. The Court may also direct that any communications acquired using that particular selector shall be segregated and/or disposed of in a manner approved by the Court.

(4) In addition to the minimization probable cause standard set forth above, as to all information gathered through the authorities requested herein, 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 Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with this Court;

[REDACTED] and b(7)(E)

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

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

[REDACTED]

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 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:¹³

[REDACTED]

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

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

(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 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. 12,333 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. 12,333, 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.

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

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

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.

(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 A to the application for an extension.

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~~

(5) The CIA shall minimize all communications received under this order as provided in Exhibit F to the initial application filed in the above-captioned docket number.

Signed 4.5.2007 1:15 pm Eastern Time
Date Time

This authorization regarding 

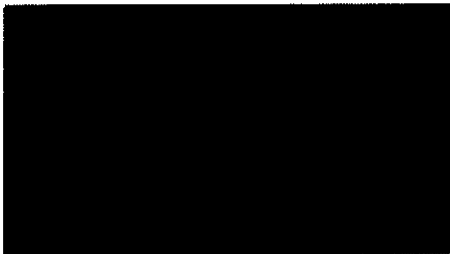
 expires at 5:00 p.m. Eastern Time

on the 31st day of May, 2007.



MALCOLM J. HOWARD

Judge, United States Foreign
Intelligence Surveillance Court

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



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:



:

:

ORDER

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

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

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

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

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

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

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

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

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

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

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

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

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

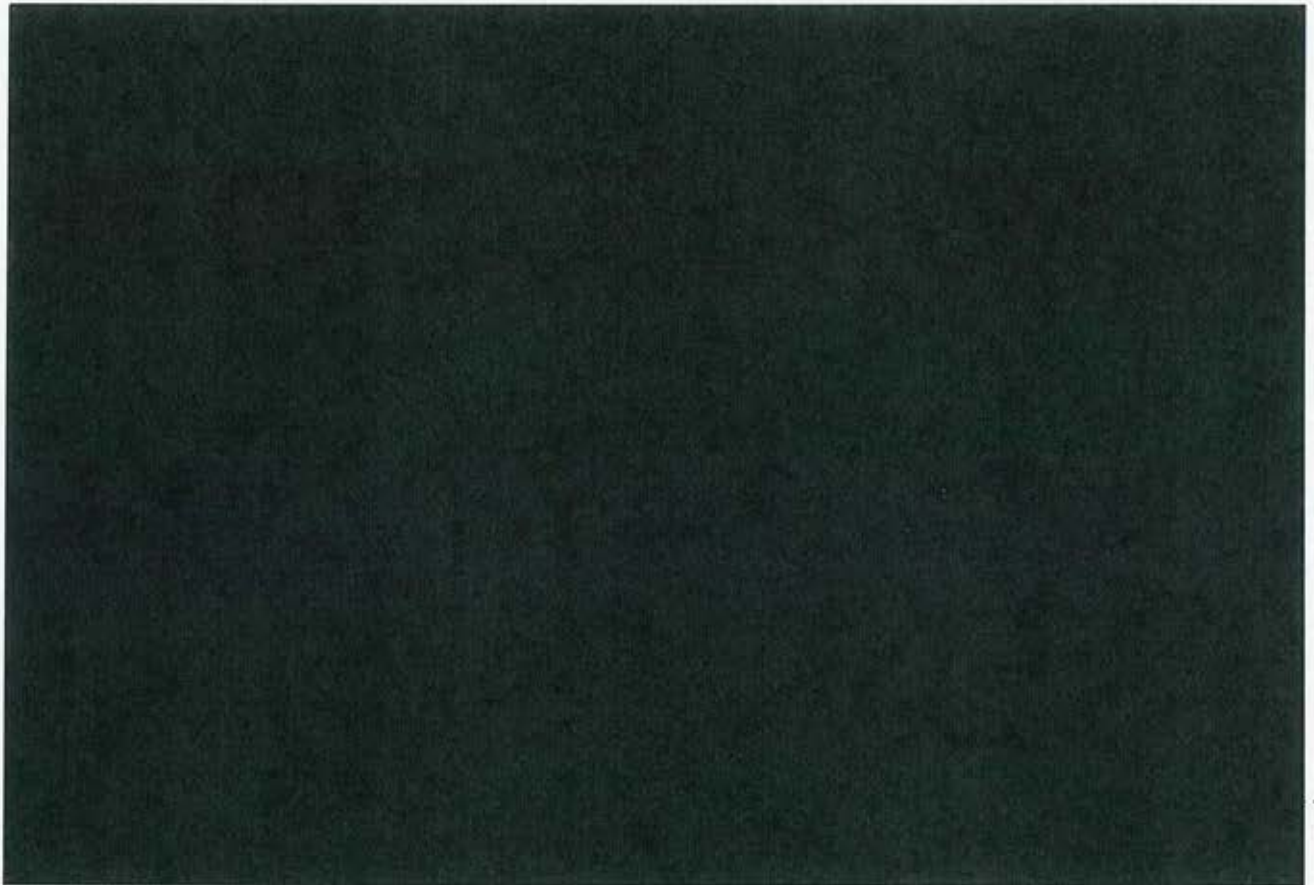
~~TOP SECRET//COMINT//NOFORN~~

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

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

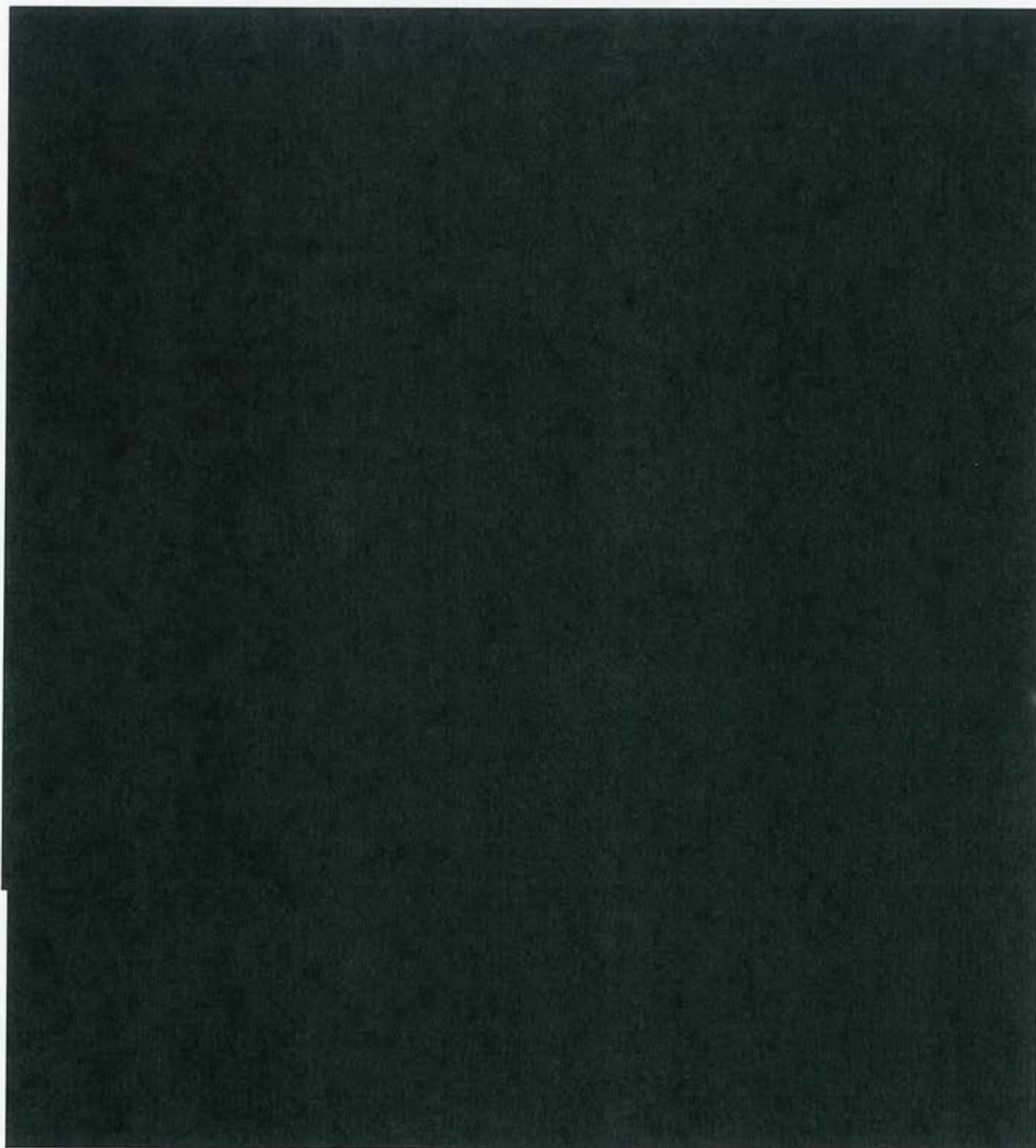
2. The application has been made by a Federal officer and approved by the Attorney General [50 U.S.C. § 1805(a)(2)];

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



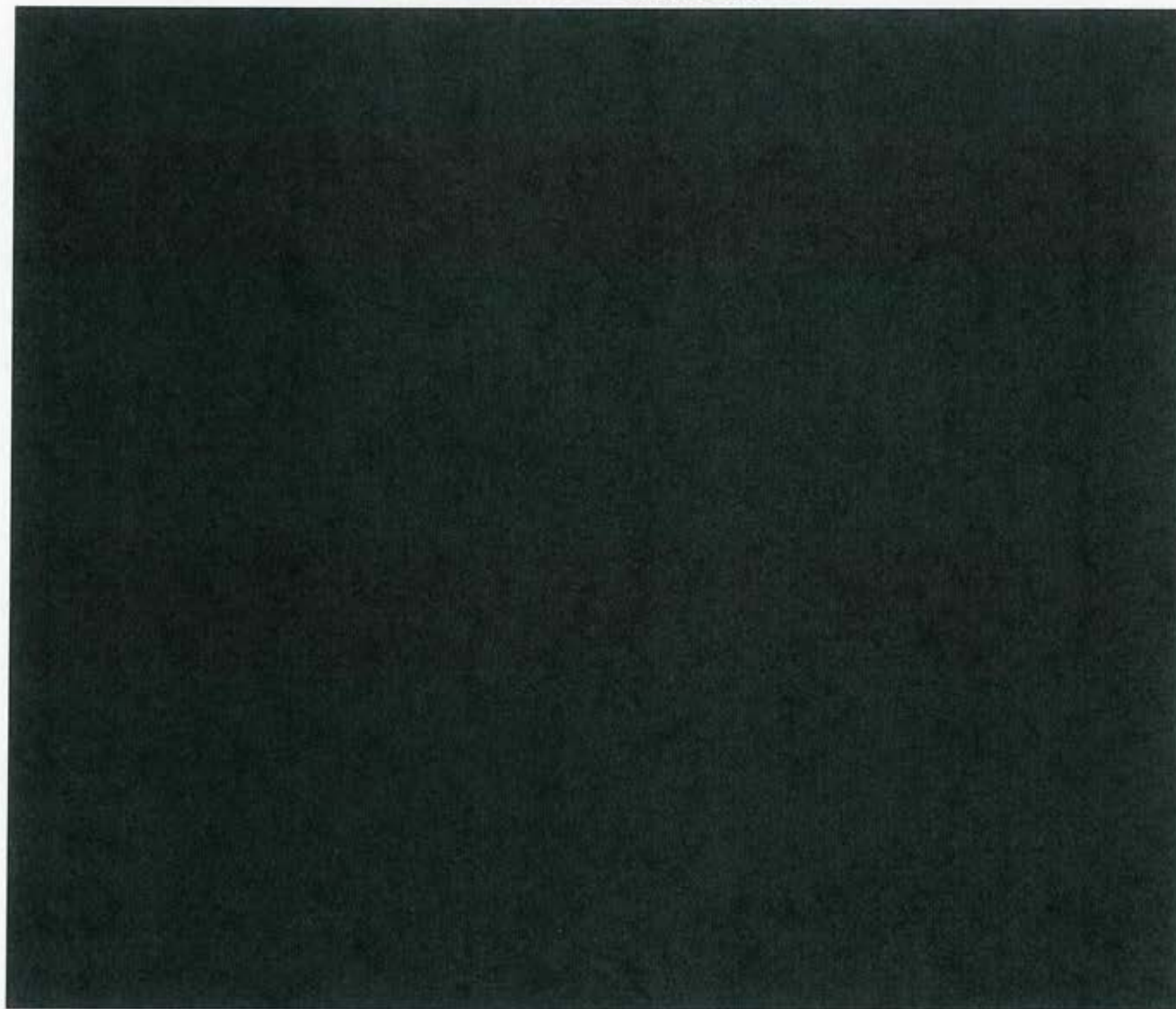
~~TOP SECRET//COMINT//NOFORN~~

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



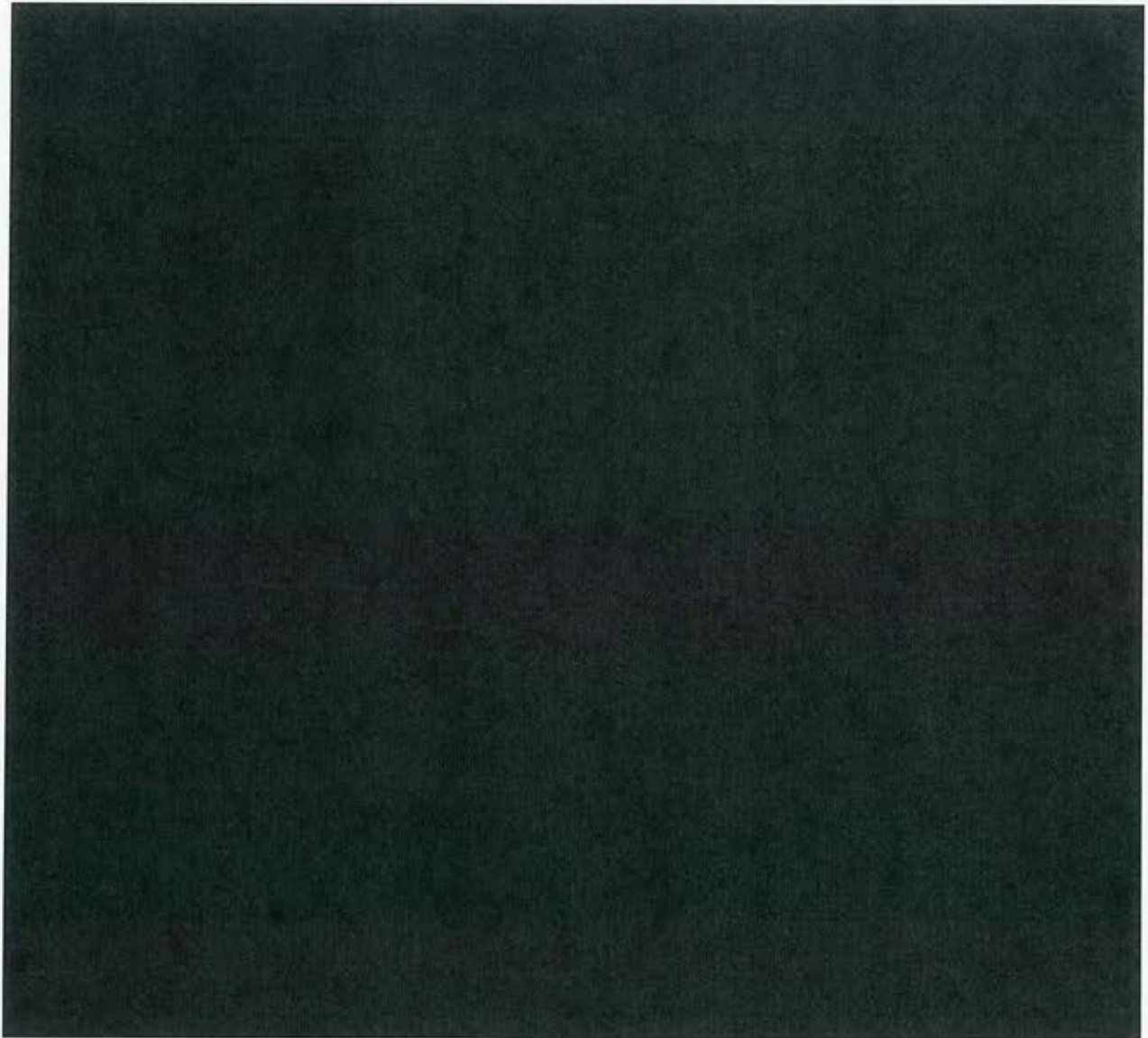
~~TOP SECRET//COMINT//NOFORN~~

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



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

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



2



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

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

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

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

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



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

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

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

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

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

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

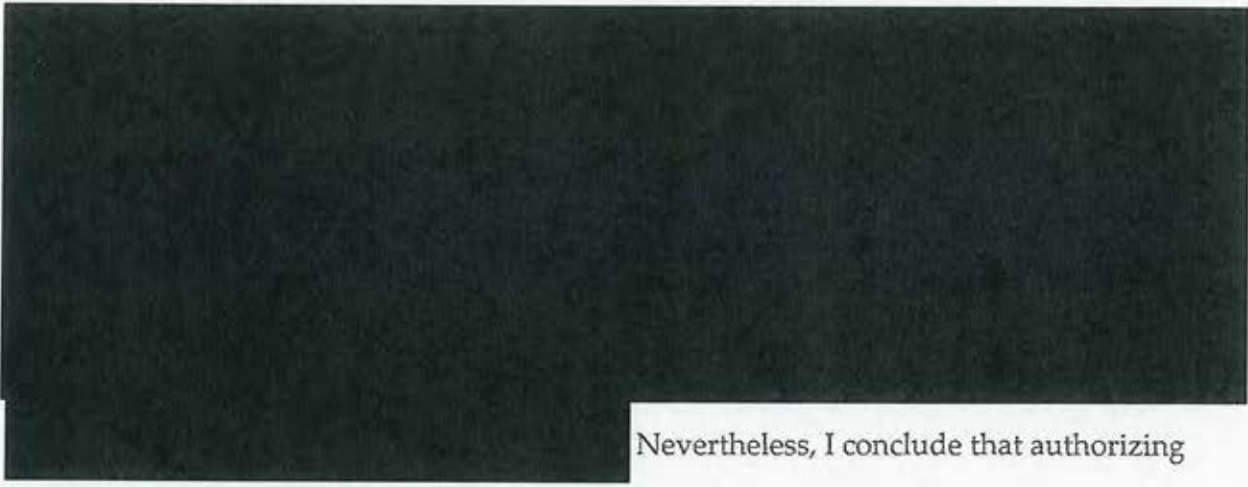


Id., at 89, 94-98.

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

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

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



Nevertheless, I conclude that authorizing

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

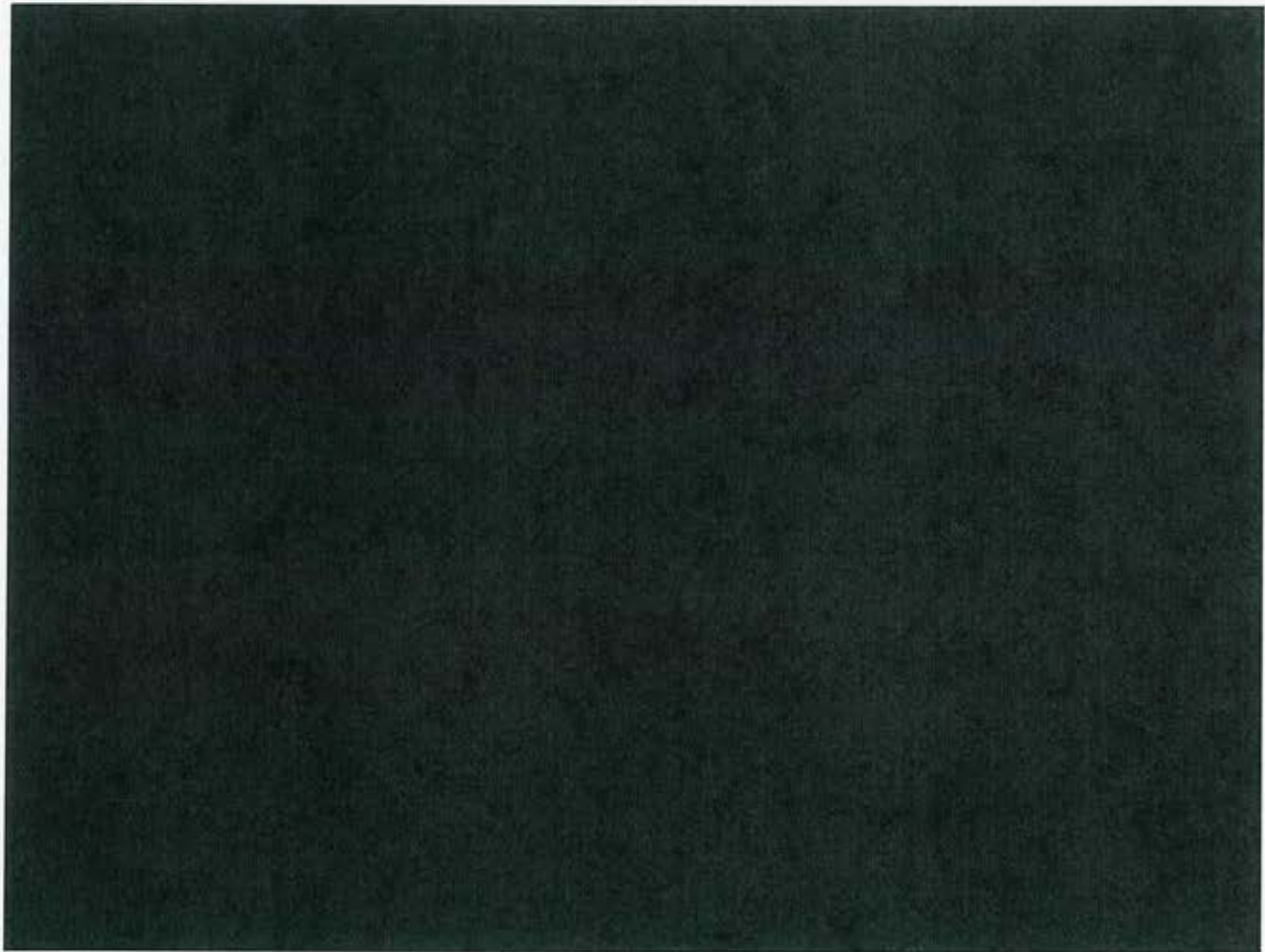
[REDACTED] that is subject to electronic surveillance under this Order at the time of acquisition (targeted [REDACTED]), under one of the following circumstances:

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

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

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

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



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]

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

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

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

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

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

[REDACTED] and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Such notice shall include:

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

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

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

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

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

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

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

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

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

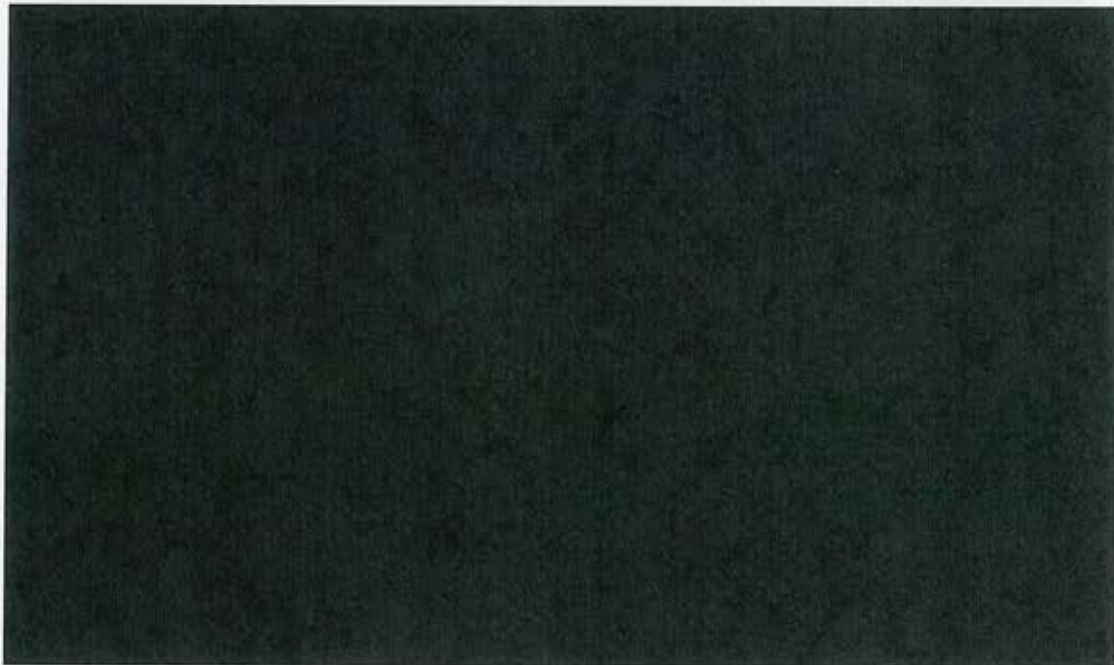
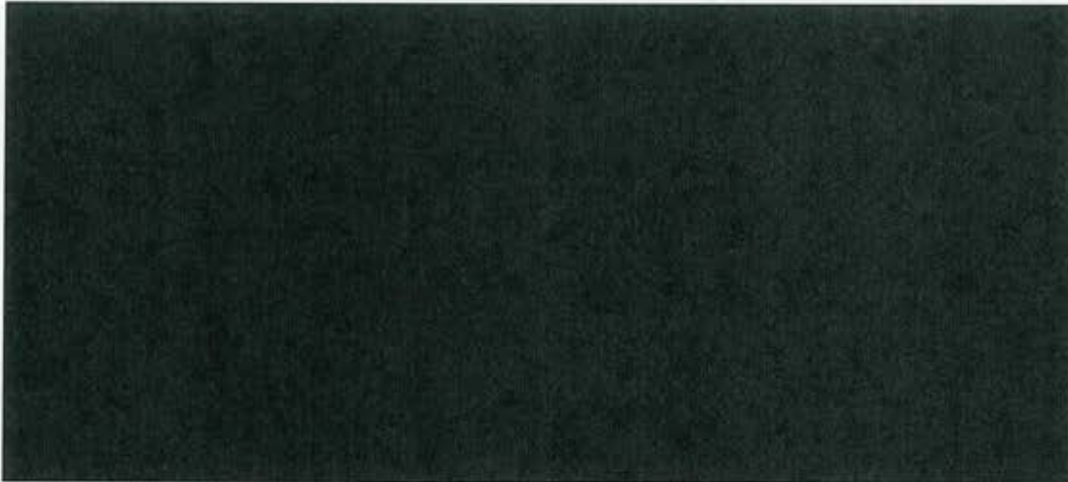
~~TOP SECRET//COMINT//NOFORN~~

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



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

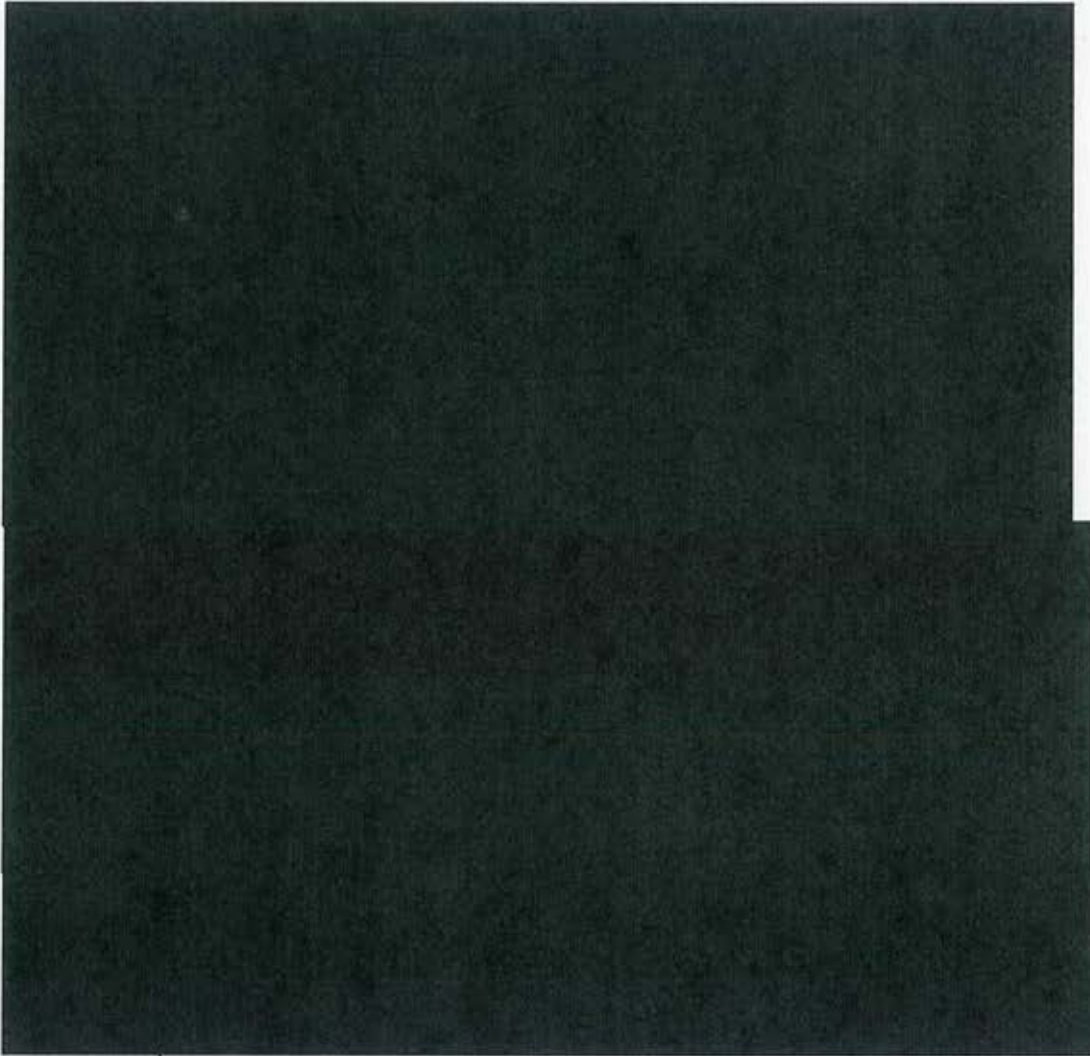
~~TOP SECRET//COMINT//NOFORN~~



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

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

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



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



TOP SECRET//COMINT//NOFORN

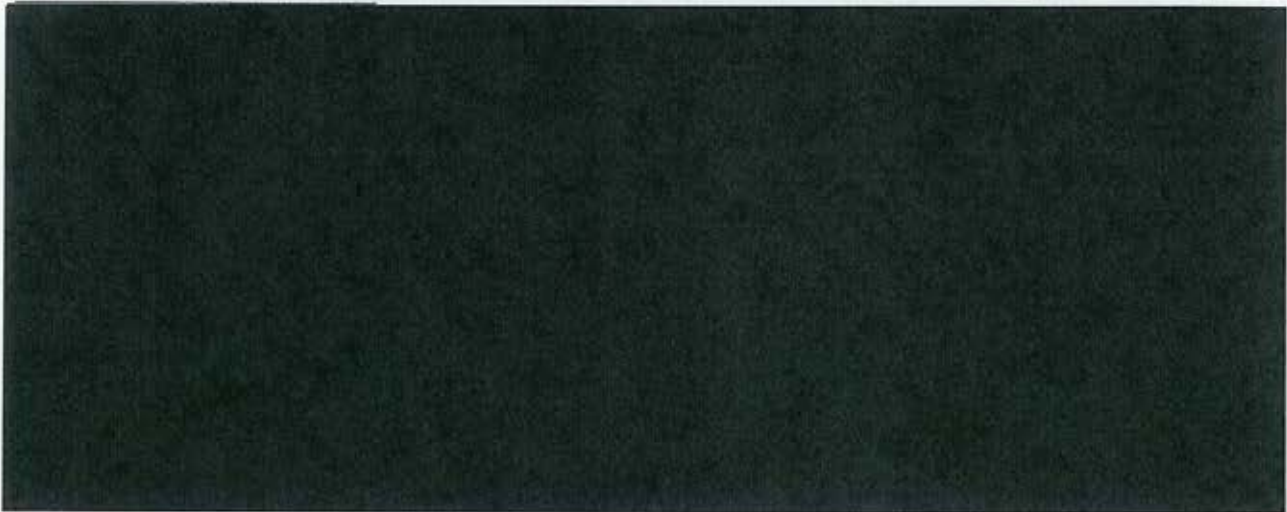
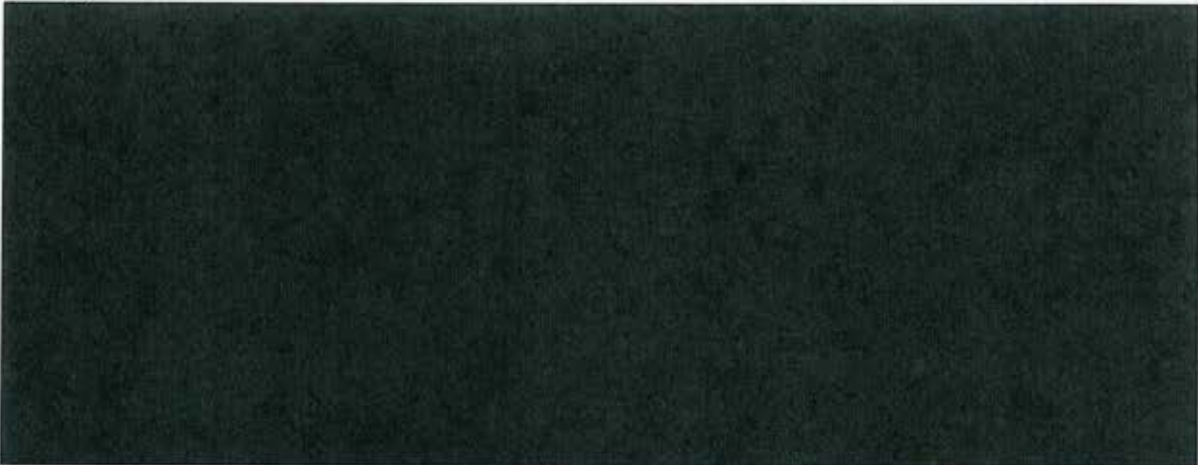
~~TOP SECRET//COMINT//NOFORN~~

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



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

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



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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

(1) Disseminations to [REDACTED]

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

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

14

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Signed 05-31-2007 10:14 Eastern Time
Date Time

This authorization regarding [REDACTED]

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

on the 24th day of August, 2007.



ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

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

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

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

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT



:

:

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

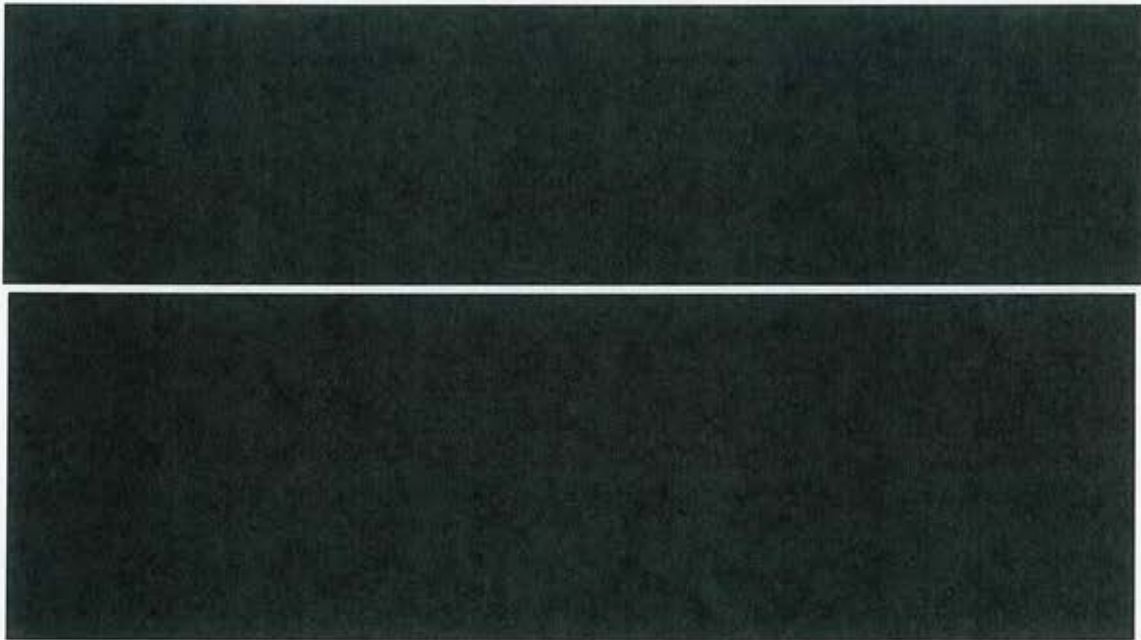
With the benefit of some two months of implementation, it can be seen that this provision of the May 31 Order requires clarification. As stated in the motion, and further addressed at the hearing, NSA has encountered different situations in which it has found the proper interpretation of this provision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

[REDACTED]

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~~

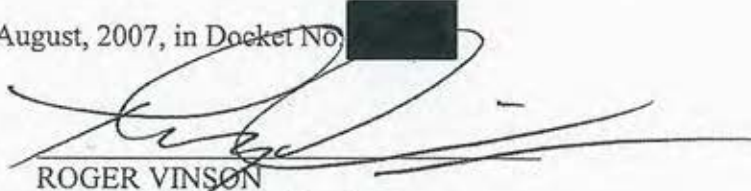
~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

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~~