B. The Methods By Which NSA Proposes to Obtain This Information Involve the Use of "Pen Registers" and "Trap and Trace Devices."

NSA proposes to obtain meta data in the above-described Categories [redacted]

[redacted]

Because the application of the definitions of "pen register" and "trap and trace device" to this means of collection involves a similar analysis for meta data in Categories [redacted], these groups of information are discussed separately below.

1. The Methods of Collecting Categories [redacted] Fall Within the Plain Meaning of the Statutory Definitions.

The above-described means of collecting information in Categories [redacted] satisfies each of the elements of the applicable statutory definition of a "pen register." It consists of "a device or process which records or decodes" non-content routing or addressing information "transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). [redacted]

[redacted]

[11] "Transmit" means "1. To convey or dispatch from one person, thing, or place to another. . . . 4. *Electron.* To send (a signal), as by wire or radio." Webster's II New College Dictionary 1171 (2001).

[redacted]

Finally, the proposed collection does not involve "any device or process used . . . for billing, or recording as an incident to billing, for communications services . . . or . . . for cost accounting or other like purposes," which is excluded from the definition of "pen register" under section 3127(3).

Accordingly, based on "the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose," Engine Mfrs. Ass'n v. South Coast Air Quality Mgmt. Dist., 124 S. Ct. 1756, 1761 (2004) (internal quotations and citation omitted), the Court concludes that the means by which the NSA proposes to collect

---

[12] For ease of reference, this Opinion and Order generally speaks of "electronic communications." The communication involved will usually be an "electronic communication" under the above-quoted definition at 18 U.S.C. § 2510(12). In the event that the communication consists of an "aural transfer," i.e., "a transfer containing the human voice at any point between and including the point of origin and the point of reception," id. § 2510(18), then it could fall instead under the above-quoted definition of "wire communication" at § 2510(1). In either case, the communication would be "a wire or electronic communication," as required to fall within the definitions at §§ 3127(3) and 3127(4).

meta data in Categories [redacted] above falls under the definition of "pen register" at section 3127(3).

The application also seeks authority to collect at least some of the same meta data by the same means under the rubric of a "trap and trace device" as defined at section 3127(4). Although it appears to the Court that all of the collection authorized herein comes within the definition of "pen register," the Court additionally finds that such collection, as it pertains to meta data in Categories [redacted] (for example, information from the "from" line of an e-mail), also satisfies the definition of "trap and trace device" under section 3127(4).

Under section 3127(4), a "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other [non-content] dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." As discussed above, the proposed collection would use a device or process to obtain non-content meta data [redacted]

[redacted]

[redacted] Thus, based on the plain meaning of

---

[13] "Capture" is defined as, inter alia, " . . . 3. To succeed in preserving in a permanent form." Webster's II New College Dictionary 166 (2001).

[redacted]

[redacted]

Such a result could be argued to violate the "cardinal principle of statutory construction that we must give effect, if possible, to every clause and word of a statute." Williams v. Taylor, 529 U.S. 362, 404 (2000) (internal quotations and citation omitted).

[redacted]

the applicable definitions, the proposed collection involves a form of both pen register and trap and trace surveillance.

[redacted]

[redacted]

[redacted]

[redacted] The Court accordingly finds that the plain meaning of sections 3127(3) and 3127(4) encompasses the proposed collection of meta data.

Alternatively, the Court finds that any ambiguity on this point should be resolved in favor of including this proposed collection within these definitions, since such an interpretation would promote the purpose of Congress in enacting and amending FISA regarding the acquisition of non-content addressing information. Congress amended FISA in 1998, and again in 2001,

to relax the requirements for Court-authorized surveillance to obtain non-content addressing information through pen register and trap-and-trace devices, recognizing that such information is not protected by the Fourth Amendment. See page 29 below. As part of the USA PATRIOT Act in 2001, Congress also amended FISA to provide for Court orders for the production of "any tangible things," such as business records, under the same relevance standard as was adopted for pen register/trap and trace authorizations. See Pub. L. No. 107-56, Title II, § 215, 115 Stat. 290, codified at 50 U.S.C. § 1861.

[redacted] like other forms of meta data, is not protected by the Fourth Amendment because users of e-mail do not have a reasonable expectation of privacy in such information. See pages 59-62 below. It is a form of non-content addressing information, which Congress has determined should receive a limited form of statutory protection under a relevance standard if obtained through pen register/trap and trace devices pursuant to 50 U.S.C. § 1842, and/or through compelled production of business records (e.g., toll records for long-distance phone calls) under 50 U.S.C. § 1861.

A narrow reading of the definitions of "pen register" and "trap-and-trace device" to exclude [redacted] would

remove this particular type of non-content addressing information from the statutory framework that Congress specifically created for it. Based on such a narrow interpretation, this information could not be collected through pen register/trap and trace surveillance, even where it unquestionably satisfies the relevance standard. Nor could this information be obtained under the business records provision, because it is not generally retained by communications service providers. See page 41 below.

There is no indication that Congress believed that the availability of non-content addressing information under the relevance standard should hinge on the technical means of collection. If anything, the legislative history, see 147 Cong. Rec. S11000 (daily ed. Oct. 25, 2001) (statement of Sen. Patrick Leahy) (supporting clarification of "the statute's proper application to tracing communications in an electronic environment . . . in a manner that is technology neutral"), and the adoption of an identical relevance standard for the production of business records and other tangible things under section 1861, suggest otherwise.

Accordingly, the Court alternatively finds that, if the application of sections 3127(3) and 3127(4) to the [redacted] were thought to be ambiguous, such

ambiguity should be resolved in favor of an interpretation of the definitions of "pen register" and "trap and trace device" that encompasses the proposed collection.

3. The Proposed Collection is Consistent With Other Provisions of FISA

Nothing that is fairly implied by other provisions of FISA governing pen register and trap and trace surveillance would prevent authorization of the proposed collection as a form of pen register/trap and trace surveillance. One provision requires that an order authorizing a pen register or trap and trace surveillance specify "the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." 50 U.S.C. § 1842(d)(2)(A)(ii). Plainly, there is no requirement to state the identity of such a person if it is not "known." However, this provision might still be read to imply that Congress expected that such facilities would be leased or listed to some particular person, even if the identity of that person were unknown in some cases. However, even if Congress had such a general expectation, the language of the statute does not require that there be such a person for every facility to which a pen register or trap and trace device is to be attached or applied. Drawing the contrary conclusion

from the wording of § 1842(d)(2)(A)(ii) would make the applicability of the statute depend on the commercial or administrative practices of particular communications service providers - a result that here would serve no apparent purpose of Congress. Cf. Smith v. Maryland, 442 U.S. 735, 745 (1979) (finding that the "fortuity of whether or not the phone company elects to make [for its own commercial purposes] a quasi-permanent record of a particular number dialed" is irrelevant to whether the Fourth Amendment applies to use of a pen register).[16]

In this case [redacted]

[16] Similarly, for purposes of the subchapter on pen register/trap and trace surveillance, FISA defines an "aggrieved person," in relevant part, as any person "whose communication instrument or device was subject to the use of a pen register or trap and trace device . . . to capture incoming electronic or other communications impulses." 50 U.S.C. § 1841(3)(B). The term "whose" suggests a relationship between some person and "a communication instrument or device" that was "subject to the use of a pen register or trap and trace device." [redacted] Indeed, the use of different language implies that these phrases can refer to different objects, so that the definition of "aggrieved person" sheds no light on whether a "facility" under § 1842(d)(2)(A)(ii)-(iii) is necessarily associated with an individual user.

[redacted] The Court is satisfied that this Opinion and Order complies with the specification requirements of § 1842(d)(2)(A).

The Court recognizes that, by concluding that these definitions do not restrict the use of pen registers and trap and trace devices to communication facilities associated with individual users, it is finding that these definitions encompass an exceptionally broad form of collection. Perhaps the opposite result would have been appropriate under prior statutory language.[17] However, our "starting point" must be "the existing

[17] Prior to amendments in 2001 by the USA PATRIOT Act, Public Law 107-56, Title II, § 216(c), 18 U.S.C. § 3127(3) defined "pen register" as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached," and § 3127(4) defined "trap and trace device" as a "device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 18 U.S.C.A. § 3127(3), (4) (2000). Despite this textual focus on telephone communications, especially in § 3127(3), many (though not all) courts expansively construed both definitions to apply as well to e-mail communications. Memorandum of Law and Fact at 25-26 & n.16; Orin S. Kerr, Internet Surveillance Law

(continued...)

statutory text," not "predecessor statutes," Lamie, 124 S. Ct. at 1030, and analysis of that text shows that collecting information in Categories [redacted] above by the means described in the application involves use of "pen registers" and "trap and trace devices."[18]

Of course, merely finding that the proposed collection falls within these definitions does not mean that the requirements for an order authorizing such collection have been met. We turn now to those requirements.

---

[17](...continued)
After the USA PATRIOT Act: The Big Brother That Isn't, 97 Nw. U. L. Rev. 607, 633-36 (2003). Extending these prior definitions to bulk collection regarding e-mail communications would have required further departure from the pre-USA PATRIOT Act statutory language.

[18] The legislative history of the USA PATRIOT Act indicates that Congress sought to make the definitions of "pen register" and "trap and trace device" "technology neutral" by confirming that they apply to Internet communications. See footnote 45 below. It does not suggest that Congress specifically gave thought to whether the new definitions would encompass collection in bulk from communications facilities that are not associated with individual users. The silence of the legislative history on this point provides no basis for departing from the plain meaning of the current definitions. See Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479, 495 n.13 (1985).

II. THE STATUTORY REQUIREMENTS FOR ISSUING AN ORDER AUTHORIZING THE PROPOSED PEN REGISTER AND TRAP AND TRACE SURVEILLANCE HAVE BEEN MET.

Under FISA's pen register/trap and trace provisions:

> Notwithstanding any other provision of law, the Attorney General . . . may make an application for an order . . . authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism . . ., provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the [FBI] under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

50 U.S.C. § 1842(a)(1). This authority "is in addition to the authority . . . to conduct . . . electronic surveillance" under §§ 1801-1811. Id. § 1842(a)(2).

> Such applications shall include, inter alia, a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism . . ., provided that such investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution.

Id. § 1842(c)(2). "Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register

or trap and trace device if the judge finds that the application satisfies the requirements of [§ 1842]." Id. § 1842(d)(1).

Obviously, the application has been made by the Attorney General, § 1842(a)(1), has been approved by the Attorney General, § 1842(c), and has been submitted in writing and under oath to a judge of this Court. § 1842(b)(1). The application, at 5, identifies the DIRNSA as "the Federal officer seeking to use the pen register or trap and trace device." § 1842(c)(1).

The application also contains a certification by the Attorney General, at 26, containing the language specified in § 1842(c)(2). The Government argues that FISA prohibits the Court from engaging in any substantive review of this certification. In the Government's view, the Court's exclusive function regarding this certification would be to verify that it contains the words required by § 1842(c)(2); the basis for a properly worded certification would be of no judicial concern. See Memorandum of Law and Fact at 28-34.

The Court has reviewed the Government's arguments and authorities and does not find them persuasive.[19] However, in

---

[19] For example, the Government cites legislative history that "Congress intended to 'authorize[] FISA judges to issue a pen register or trap and trace order upon a certification that the information sought is relevant to'" an FBI investigation.
(continued...)

this case the Court need not, and does not, decide whether it would be obliged to accept the applicant's certification without any explanation of its basis. Arguing in the alternative, the Government has provided a detailed explanation of 1) the threat currently posed by [redacted] 2) the reason the bulk collection described in the application is believed necessary as a means for NSA [redacted] 3) how that information will contribute to FBI investigations to protect against [redacted] and 4) what safeguards will be observed to ensure that the information collected will not be used for unrelated purposes or

---

[19](...continued)
Memorandum of Law and Fact at 30 (quoting S. Rep. No. 105-185, at 27 (1998). However, authorizing the Court to issue an order when a certification is made, and requiring it to do so without resolving doubts about the correctness of the certification, are quite different.

The Government also cites United States v. Hallmark, 911 F.2d 399 (10th Cir. 1990), in arguing that the Court should not review the basis of the certification. However, the Hallmark court reserved the analogous issue under Title 18 - "the precise nature of the court's review under 18 U.S.C. § 3123" of the relevancy certification in an application for a law enforcement pen register or trap and trace device - and expressed "no opinion as to whether the court may, for instance, inquire into the government's factual basis for believing the pen register or trap and trace information to be relevant to a criminal investigation." Id. at 402 n.3.

otherwise misused. The Government also provides legal arguments that, under these specific circumstances, the proposed collection satisfies the relevancy requirement of § 1842(c)(2), despite its resulting in the collection of meta data from an enormous volume of communications, the large majority of which will be unrelated to international terrorism. In view of this record, the Court will assume for purposes of this case that it may and should consider the basis of the certification under § 1842(c)(2).

Nonetheless, the Court is mindful that FISA does not require any finding of probable cause in order for pen register and trap and trace surveillance to be authorized. In this regard, the statutory provisions that govern this case contrast sharply with those that apply to other forms of electronic surveillance and physical search.[20] Before Congress amended FISA in 1998 to add §§ 1841-1846, this Court could authorize pen register and trap and trace surveillance only upon the same findings as would be required to authorize interception of the full contents of

---

[20] To issue an electronic surveillance order, the Court must find "probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power" and "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. § 1805(a)(3). Similar probable cause findings are required for warrants authorizing physical search under id. § 1824(a)(3).

communications. See S. Rep. 105-185, at 27 (1998). When it originally enacted §§ 1841-1846 in 1998, Congress recognized that pen register and trap and trace information is not protected by the Fourth Amendment and concluded that a lower standard for authorization "was necessary in order to permit, as is the case in criminal investigations, the use of this very valuable investigative tool at the critical early stages of foreign intelligence and international terrorism investigations." Id. These 1998 provisions included a form of a "reasonable suspicion" standard for pen register/trap and trace authorizations.[21] As part of the USA PATRIOT Act in 2001, Congress lowered the standard again, to the current requirement of relevance.[22] Given this history, it is obvious that Congress intended pen register

---

[21] Under the provisions enacted in 1998, a pen register or trap and trace application had to include "information which demonstrates that there is reason to believe" that a communication facility "has been or is about to be used in communication with," inter alia, "an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities." Public Law 105-272 § 601(2).

[22] The legislative history of the USA PATRIOT Act reflects that, "in practice," the standard passed in 1998 was "almost as burdensome as the requirement to show probable cause required . . . for more intrusive techniques" and that the FBI "made a clear case that a relevance standard is appropriate for counterintelligence and counterterrorism investigations." 147 Cong. Rec. S11003 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

and trap and trace authorizations to be more readily available than authorizations for electronic surveillance to acquire the full contents of communications.

The Court also recognizes that, for reasons of both constitutional authority and practical competence, deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats[23] and in determining the potential significance of intelligence-related information.[24] Such deference is particularly

---

[23] See, e.g., Reno v. American-Arab Anti-Discrimination Comm., 525 U.S. 471, 491 (1999) ("a court would be ill equipped to determine [the] authenticity and utterly unable to assess [the] adequacy" of the executive's security or foreign policy reasons for treating certain foreign nationals as "a special threat"); Regan v. Wald, 468 U.S. 222, 243 (1984) (giving "the traditional deference to executive judgment" in foreign affairs in sustaining President's decision to restrict travel to Cuba against a Due Process Clause challenge); cf. Department of Navy v. Egan, 484 U.S. 518, 529 (1988) (outside body reviewing executive branch decisions on eligibility for security clearances could not "determine what constitutes an acceptable margin of error in assessing the potential risk").

[24] The Supreme Court has observed that, in deciding whether disclosing particular information might compromise an intelligence source, what "may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context." CIA v. Sims, 471 U.S. 159, 178 (1985) (internal quotation and citation omitted). Accordingly, the decisions of [redacted] "who must of course be familiar with 'the whole picture,' as judges are not, are worthy of great deference given the magnitude of the national security interests and potential

(continued...)

appropriate in this context, where the Court is not charged with making independent probable cause findings.

A. The Government Has Provided Information In Support of the Certification of Relevance.

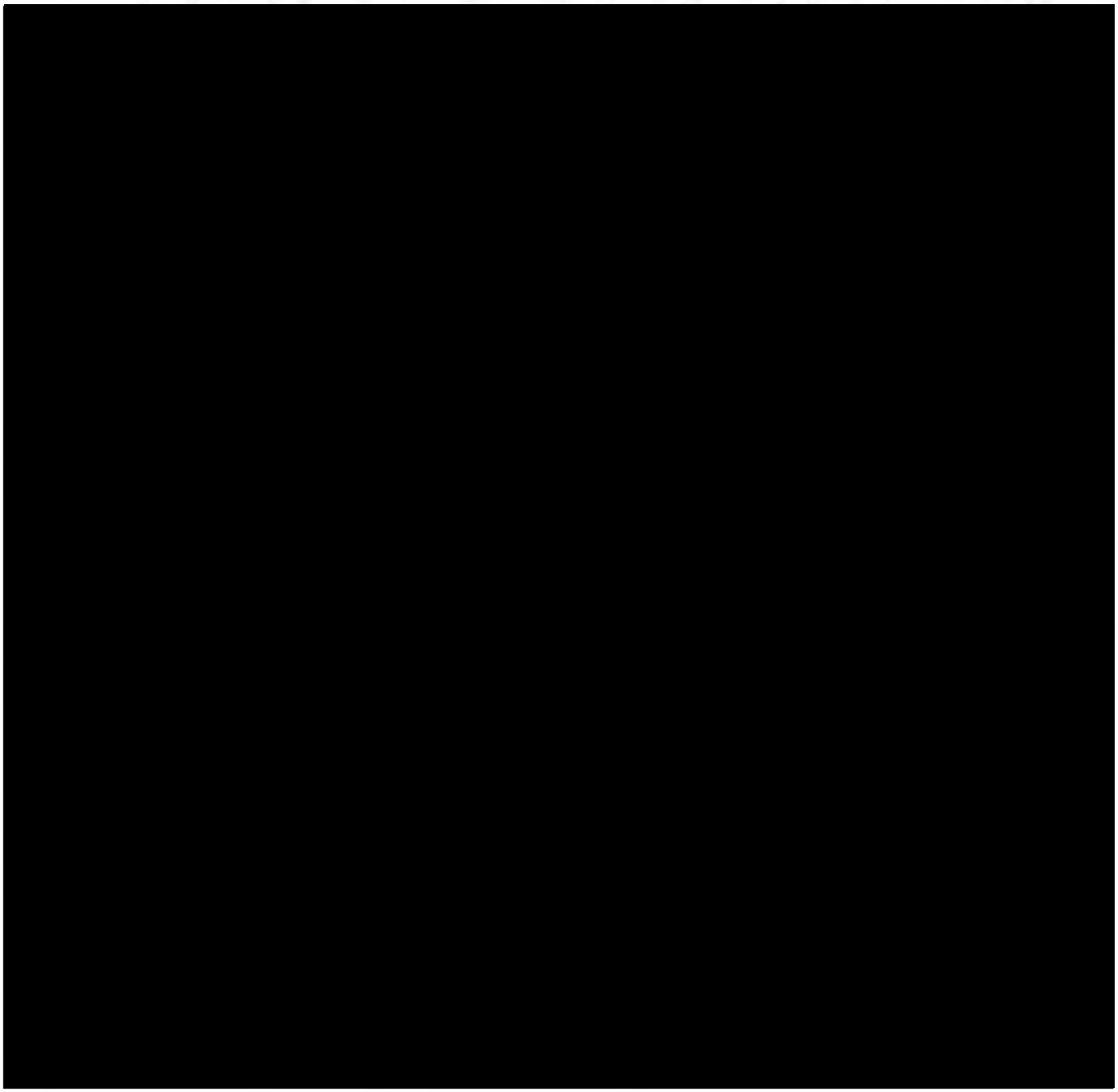
In support of the certification of relevance, the Government relies on the following facts and circumstances:

1. The Threat Currently Posed [redacted]

[redacted]

[24](...continued)
risks at stake." Id. at 179.

[25] For simplicity, this opinion standardizes the variant spellings of foreign names appearing in different documents submitted in support of the application.



[redacted]

2. FBI Investigations to Track and Identify [redacted] in the United States

[redacted]

[redacted]

3. The Use of the Internet by [redacted]

[redacted]

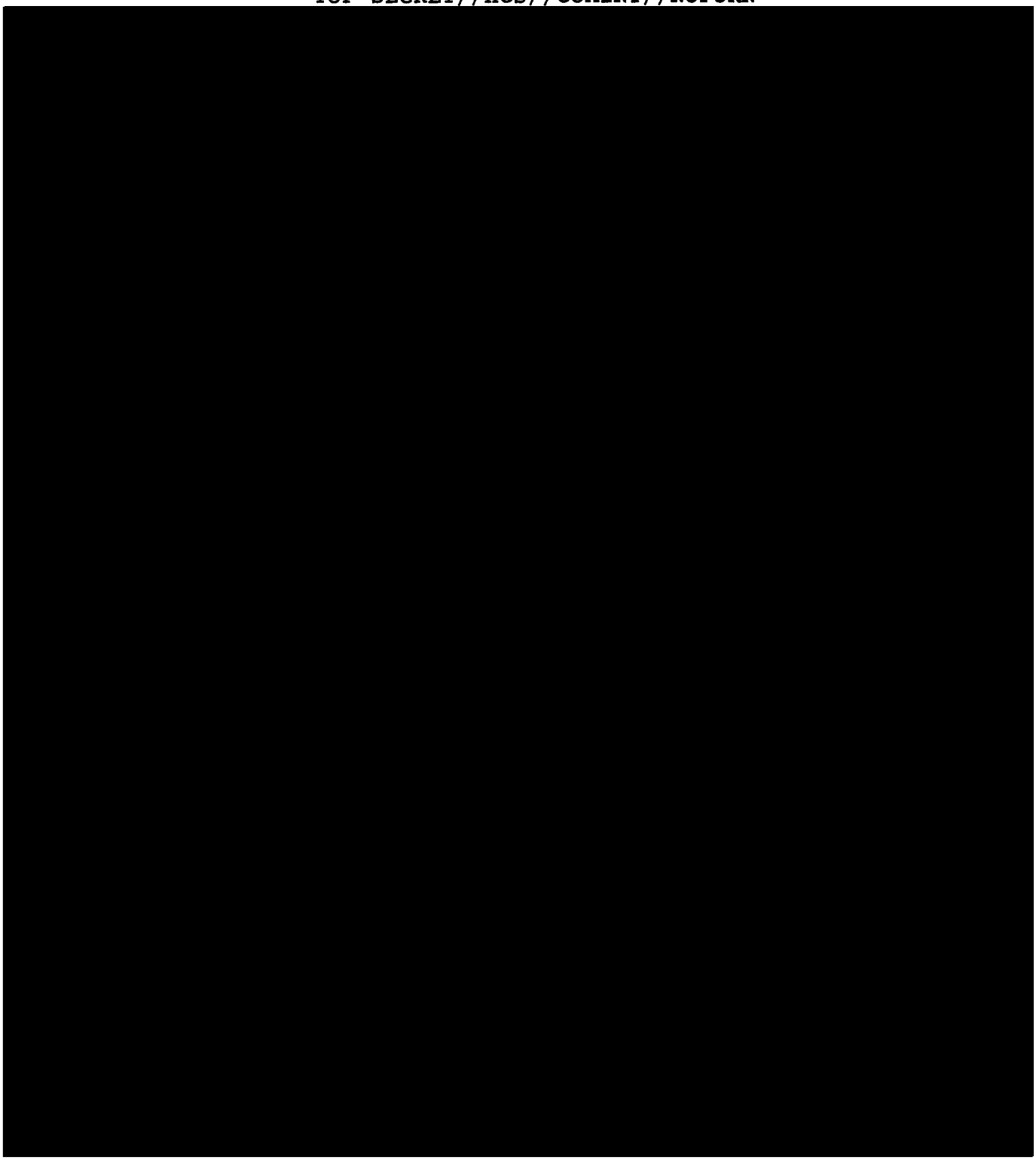
[redacted]

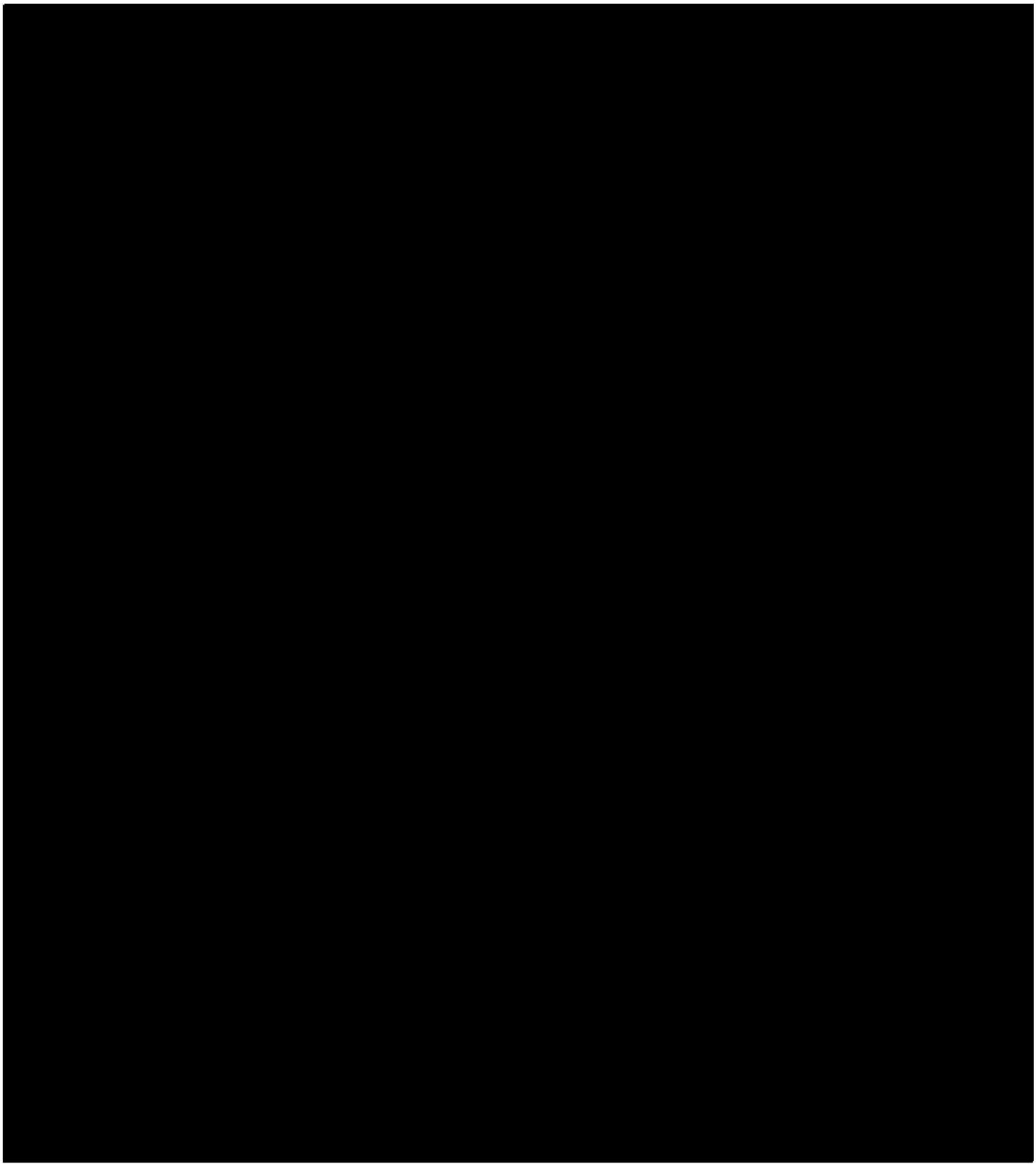
4. The Scope of the Proposed Collection of Meta Data

In an effort both to identify unknown and to track known operatives [redacted] through their Internet communications, NSA seeks to acquire meta data, as described above, from all e-mail [redacted] are described in detail in the application and the DIRNSA Declaration. In brief, they are:

[redacted]

[27] For ease of reference, the term [redacted] is used to mean [redacted]





[redacted]

The raw volume of the proposed collection is enormous. NSA estimates that this collection will encompass [redacted] In absolute terms, the proposed surveillance "will result in the collection of meta data pertaining to [redacted] electronic communications, including meta data pertaining to communications of United States persons located within the United States who are not the subject of any FBI investigation." Application at 4. Some proportion of these communications - less than half, but still a huge number in absolute terms - can be expected to be communications [redacted]

[redacted] who bear no relation to [redacted]

[redacted]

5. How NSA Proposes to Use this Data to Track Known [redacted]

As noted above, the purpose of this collection is to track known operatives and to identify unknown operatives of [redacted] through their Internet communications. NSA

---

[29] As noted above, collection of meta data from [redacted]

[redacted]

states that even identified operatives [redacted]

[redacted]

Through the proposed bulk collection, NSA would acquire an archive of meta data for large volumes of communications that, in NSA's estimation, represent a relatively rich environment for finding [redacted] communications through later analysis.[31]

---

[31] See DIRNSA Declaration at 5 [redacted]

NSA asserts that more precisely targeted forms of collection against known accounts would tend to screen out the "unknowns" that NSA wants to discover, so that NSA needs bulk collection in order to identify unknown [redacted] communications. See id. at 14 ("It is not possible . . . to target collection solely to known terrorist E-mail accounts and at the same time use the advantages of meta data analysis to discover the enemy."), 15 ("To be able to fully exploit meta data, the data must be collected in bulk. Analysts know that terrorists' E-mails are located somewhere in the billions of data bits; what they cannot know ahead of time is exactly where.")

NSA proposes to employ two analytic methods on the body of archived meta data it seeks to collect. Both these methods involve querying the archived meta data regarding a particular "seed" account. In the Government's proposal, an account would qualify as a seed account only if NSA concludes, "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with [redacted]

[redacted]

[redacted] Application at 19-20; accord DIRNSA Declaration at 19. The two methods are:

(1) Contact chaining. NSA will use computer algorithms to identify within the archived meta data all e-mail [redacted] accounts that have been in contact with the seed account, as well as all accounts that have been in contact with an account within the first tier of accounts that had direct contact with the seed account, and [redacted] DIRNSA Declaration at 15-16.

[redacted]

An example may illustrate the claimed benefits of bulk collection and subsequent analysis of meta data. [redacted] Without an archive of meta data, the Government could target prospective collection on that account, but information about past use would be unavailable. [redacted].[32]

However, if an archive of meta data were available, NSA could use the newly discovered account as a "seed" account. Accounts previously in contact with the "seed" account could be identified and further investigation could be pursued to determine if the users of those accounts are [redacted]

---

[32] Assuming that applicable legal requirements could be met, the Government also could collect the full contents of future messages by electronic surveillance of the account and of stored prior messages by physical search of the account. However, [redacted] could thwart these forms of collection also.

[redacted]

These avenues of discovery made possible by archived meta data provide the basis for NSA's assertion that bulk collection to accumulate a meta data archive "will substantially increase NSA's ability to detect and identify members of [redacted] DIRNSA Declaration at 15.

6. How FBI Investigations Would Benefit from the NSA's Collection and Analysis

The Government asserts that NSA's collection and analysis of this meta data will be relevant to [redacted] FBI investigations in two ways. First, ongoing FBI investigations may develop grounds for reasonable suspicion that particular accounts are used in furtherance of [redacted] The FBI may identify such accounts to NSA for use as "seed" accounts. Using the methods described above, NSA may obtain from the archived data other accounts that are in contact with, or appear to have the same user as, the "seed" account. This information may then be passed to the FBI as investigative leads in furtherance of its investigation. Memorandum of Law and Fact at 27-28. Alternatively, NSA querying of the archived meta data based on information from sources other than the FBI may identify accounts that appear to be used by someone involved in

[redacted] activities. If such accounts are relevant to FBI investigative responsibilities - for example, if it appears that their users are in the United States - then NSA will provide information to the FBI, which may prove relevant to ongoing FBI investigations or provide the predicate for new investigations of persons involved in [redacted] Under the proposed program, NSA estimates that roughly 400 accounts would be "tipped" to the FBI and CIA[33] annually, with an estimated twenty-five percent of that number associated with U.S. persons. DIRNSA Declaration at 20.

7. The Government's Proposed Procedures for Accessing, Retaining, and Disseminating Collected Information

The application specifies proposed procedures and restrictions for accessing, retaining, and disseminating information from this bulk collection of meta data. Application at 18-24. These procedures and restrictions, with certain modifications, are set out at pages 82-87 below.

[33] As long as the proposed collection satisfies the standard of relevance to an FBI investigation described in section 1842(a)(1), (c)(2), dissemination of information to other agencies when it is relevant to their responsibilities is appropriate.

B. The Information To Be Obtained is Likely to be Relevant to Ongoing FBI Investigations to Protect Against International Terrorism

As shown above, the application and supporting materials demonstrate that the FBI has numerous pending investigations on [redacted] subjects and that a major challenge faced by the FBI is the identification of [redacted] within the United States. [redacted] The application and DIRNSA declaration provide detailed explanations of why NSA regards bulk collection of meta data as necessary for contact chaining [redacted] and how those analytical methods can be expected to uncover and monitor unknown [redacted] who could otherwise elude detection. The DIRNSA also explains why NSA has chosen the proposed [redacted] and selection criteria in order to build a meta data archive that will be, in relative terms, richly populated with [redacted] related communications. On each of these points, the Court has received sufficient information to conclude that the Government's

assessments are fully considered and plausibly grounded in facts submitted to the Court.

Accordingly, the Court accepts for purposes of this application that the proposed bulk collection of meta data is necessary for NSA to employ contact chaining [redacted] The Court similarly accepts that those analytic tools are likely to generate useful investigative leads for ongoing efforts by the FBI (and other agencies) to identify and track [redacted] potentially including unidentified operatives in place to facilitate or execute imminent large scale attacks within the United States.

The question remains whether these circumstances adequately support the certification that "the information likely to be obtained . . . is relevant to an ongoing investigation to protect against international terrorism," § 1842(c)(2), even though only a very small percentage of the information obtained will be from [redacted] communications and therefore directly relevant to such an investigation. As the Government points out, the meaning of "relevant" is broad enough, at least in some contexts, to encompass information that may reasonably lead to the discovery of directly relevant information. Memorandum of Law and Fact at 34. Here, the bulk collection of meta data - i.e.,

the collection of both a huge volume and high percentage of unrelated communications - is necessary to identify the much smaller number of [redacted] communications.

The Court is persuaded that, in the circumstances of this case, the scope of the proposed collection is consistent with the certification of relevance.[34] In so finding, the Court concludes that, under the circumstances of this case, the applicable relevance standard does not require a statistical "tight fit" between the volume of proposed collection and the much smaller proportion of information that will be directly relevant to [redacted]

---

[34] The Government analogizes this case to ones in which the Court has authorized overbroad electronic surveillance under 50 U.S.C. §§ 1801-1811. Memorandum of Fact and Law at 42-43. The Court has authorized the latter form of collection where it is not technologically possible to acquire [redacted] The two situations are similar in that they both involve collection of an unusually large volume of non-foreign intelligence information as a necessary means of obtaining the desired foreign intelligence information. Yet there are also important differences between these cases. An overbroad electronic surveillance under 50 U.S.C. §§ 1801-1811 requires probable cause to believe that the target is an agent of a foreign power and uses the particular facility at which surveillance will be directed. § 1805(a)(3). In this case under 50 U.S.C. §§ 1841-1846, no probable cause findings are required, and the bulk collection is justified as necessary to discover unknown [redacted] persons and facilities, rather than to acquire communications to and from identified agents of a foreign power. Because of these differences, the authorization of bulk collection under §§ 1841-1846 should not be taken as precedent for similar collection of the full contents of communications under §§ 1801-1811.

[redacted] FBI investigations. In reaching this conclusion, the Court finds instructive Supreme Court precedents on when a search that is not predicated on individualized suspicion may nonetheless be reasonable under the Fourth Amendment. See Memorandum of Law and Fact at 43-48.[35]

The Supreme Court has recognized a "longstanding principle that neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance." National Treasury Employees Union v. Von Raab, 489 U.S. 656, 665 (1989); accord, e.g., Board of Educ. of Indep. School Dist. No. 92 of Pottawatomie County v. Earls, 536 U.S. 822, 829 (2002); United States v. Martinez-Fuerte, 428 U.S. 543, 560-61 (1976). Specifically, the Court has held that, "where a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's

---

[35] For the reasons explained below at pages 59-66, the Court finds that there is no privacy interest protected by the Fourth Amendment in the meta data to be collected. Nevertheless, the Court agrees with the Government's suggestion that the balancing methodology used to assess the reasonableness of a Fourth Amendment search or seizure is helpful in applying the relevance standard to this case. Memorandum of Law and Fact at 43.

interests to determine whether it is impractical to require a warrant or individualized suspicion in the particular context." Von Raab, 489 U.S. at 665-66; accord, e.g., Earls, 536 U.S. at 829.

This balancing analysis considers "the nature of the privacy interest allegedly compromised" and "the character of the intrusion" upon that interest. Earls, 536 U.S. at 830, 832. The privacy interest in the instant meta data is not of a stature protected by the Fourth Amendment. See pages 59-66 below. Moreover, the nature of the intrusion is mitigated by the restrictions on accessing and disseminating this information, under which only a small percentage of the data collected will be seen by any person. Cf. Earls, 536 U.S. at 833 (finding that restrictions on access to drug-testing information lessen the testing program's intrusion on privacy).

The assessment of reasonableness under the Fourth Amendment also considers "the nature and immediacy of the government's concerns and the efficacy of the [program] in meeting them." Id. at 834. In this case, the Government's concern is to identify and track [redacted] operatives, and ultimately to thwart terrorist attacks. This concern clearly involves national

security interests beyond the normal need for law enforcement[36] and is at least as compelling as other governmental interests that have been held to justify searches in the absence of individualized suspicion. See, e.g., Earls (drug testing of secondary school students engaged in extracurricular activities); Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (highway checkpoints to identify drunk drivers); Von Raab (drug testing of Customs Service employees applying for promotion to sensitive positions); Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989) (drug and alcohol testing of railroad workers).[37] The Government's interest here has even greater "immediacy" in view of the above-described intelligence reporting and assessment regarding ongoing plans for large scale attacks within the United States.

As to efficacy under the Fourth Amendment analysis, the Government need not make a showing that it is using the least intrusive means available. Earls, 536 U.S. at 837; Martinez-

---

[36] See In Re Sealed Case, 310 F.3d 717, 744-46 (Foreign Int. Surv. Ct. Rev. 2002) (per curiam) (discussing the prevention of terrorist attacks as a special need beyond ordinary law enforcement).

[37] Moreover, the Government's need in this case could be analogized to the interest in discovering or preventing danger from "latent or hidden conditions," which may justify suspicionless searches. See, e.g., Von Raab, 489 U.S. at 668.

Fuerte, 428 U.S. at 556-57 n.12. Rather, the question is whether the Government has chosen "a reasonably effective means of addressing" the need. Earls, 536 U.S. at 837. In structuring a program involving suspicionless search or seizure, e.g., in positioning roadblocks at certain points, "the choice among . . . reasonable alternatives remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources." Sitz, 496 U.S. at 453-54; see also Martinez-Fuerte, 428 U.S. at 566 ("deference is to be given to the administrative decisions of higher ranking officials"). A low percentage of positive outcomes among the total number of searches or seizures does not necessarily render a program ineffective.[38]

In this case, senior responsible officials, whose judgment on these matters is entitled to deference, see pages 30-31 above, have articulated why they believe that bulk collection and archiving of meta data are necessary to identify and monitor [redacted] operatives whose Internet communications would

[38] See Sitz, 496 U.S. at 454 ("detention of the 126 vehicles that entered the checkpoint resulted in the arrest of two drunken drivers"); Martinez-Fuerte, 428 U.S. at 546 & n.1, 554 (checkpoint near border to detect illegal migrants: out of "roughly 146,000 vehicles" temporarily "'seized,'" 171 were found to contain deportable aliens).

otherwise go undetected in the huge streams of [redacted] These officials have also explained why they seek to collect meta data [redacted] identified in the application. Based on these explanations, the proposed collection appears to be a reasonably effective means to this end.

In summary, the bulk collection proposed in this case is analogous to suspicionless searches or seizures that have been upheld under the Fourth Amendment in that the Government's need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of detecting and monitoring [redacted] related operatives and thereby obtaining information likely to be [redacted] to ongoing FBI investigations. In these circumstances, the certification of relevance is consistent with the fact that only a very small proportion of the huge volume of information collected will be directly relevant to the FBI's [redacted] investigations.

---

[39] Cf. Martinez-Fuerte, 428 U.S. at 557 (requiring reasonable suspicion for stops at highway checkpoints "on major routes . . . would be impractical because the flow of traffic tends to be too heavy to allow the particularized study of a given car").

C. The Pertinent FBI Investigations of U.S. Persons Are Not Conducted Solely Upon the Basis of First Amendment Activities.

When the information likely to be obtained concerns a U.S. person, § 1842(c)(2) requires a certification that the "ongoing investigation . . . of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." The certification in this case states that the pertinent investigation is not being conducted on such a basis. Application at 26. The application refers to numerous FBI National Security investigations "being conducted under guidelines approved by the Attorney General pursuant to Executive Order No. 12,333."[40] Id. at 6.

> Those investigations are being conducted on the basis of activities of [redacted] and unknown [redacted] affiliates in the United States and abroad, and to the extent these subjects of investigation are United States persons, not solely on the basis of activities that are protected by the First Amendment to the Constitution.

Id.

Thus, the certification and application contain the proper assurance that the relevant investigations of U.S. persons are

---

[40] § 1842(a)(1) permits the filing of applications for installation and use of pen register and trap and trace devices to obtain information relevant to certain investigations "under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order."

not being conducted solely on the basis of activities protected by the First Amendment. However, the unusual breadth of this collection and its relation to the pertinent FBI investigations calls for further attention to this issue. In the usual case, the FBI conducts pen register and trap and trace surveillance of a particular communications facility (e.g., a phone number or e-mail address) because it carries communications of a person who is the subject of an FBI investigation. The required certification typically varies depending on whether the subject is a U.S. person: if not, the certification will state, in the language of § 1842(c)(2), that the information likely to be obtained "is foreign intelligence information not concerning a United States person;" if the subject is a U.S. person, the certification will state that such information is "relevant to an ongoing investigation to protect against international terrorism . . ., provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This usual practice conforms to the clear statutory purpose that pen register/trap and trace information about the communications of U.S. persons will not be targeted for collection unless it is relevant to an

investigation that is not solely based upon First Amendment activities.

In this case, the initial acquisition of information is not directed at facilities used by particular individuals of investigative interest, but meta data concerning the communications of such individuals' [redacted] Here, the legislative purpose is best effectuated at the querying stage, since it will be at a point that an analyst queries the archived data that information concerning particular individuals will first be compiled and reviewed. Accordingly, the Court orders that NSA apply the following modification of its proposed criterion for querying the archived data: [redacted] will qualify as a seed [redacted] only if NSA concludes, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known [redacted] is associated with [redacted] provided, however, that an [redacted] believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First

Amendment to the Constitution.[41] For example, an e-mail account used by a U.S. person could not be a seed account if the only information thought to support the belief that the account is associated with [redacted] is that, in sermons or in postings on a web site, the U.S. person espoused jihadist rhetoric that fell short of "advocacy . . . directed to inciting or producing imminent lawless action and . . . likely to incite or produce such action." Brandenberg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam).

III. THE PROPOSED COLLECTION AND HANDLING OF META DATA DO NOT VIOLATE THE FIRST OR FOURTH AMENDMENTS.

Because this case presents a novel use of statutory authorities for pen register/trap and trace surveillance, the Court will also explain why it is satisfied that this surveillance comports with the protections of the Fourth Amendment and the First Amendment.

A. Fourth Amendment Issues

The foregoing analysis has observed at various points that the Fourth Amendment does not apply to the proposed collection of

---

[41] This modification will realize more fully the Government's suggestion that "[t]he information actually viewed by any human being . . . will be just as limited - and will be based on the same targeted, individual standards - as in the case of an ordinary pen register or trap and trace device." Government's Letter of [redacted] at 3.

meta data. See, e.g., pages 19, 50-51 above. This section explains the basis for that conclusion.

First, as a general matter, there is no reasonable expectation of privacy under the Fourth Amendment in the meta data to be collected. This conclusion follows directly from the reasoning of Smith v. Maryland, 442 U.S. 735 (1979), which concerned the use of a pen register on a home telephone line. In that case, the Supreme Court found that it was doubtful that telephone users had a subjective expectation of privacy in the numbers they dialed, id. at 742-43, and that in any case such an expectation "is not 'one that society is prepared to recognize as reasonable.'" Id. at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)). The Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," since he "assume[s] the risk" that the third party would reveal that information to the government. Id. at 743-44.[42] The Court found this principle applicable to dialed phone numbers, regardless of the automated means by which the call is placed and the "fortuity of whether or

[42] This principle applies even if there is an understanding that the third party will treat the information as confidential. See SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984); United States v. Miller, 425 U.S. 435, 443 (1976).

not the phone company in fact elects to make a quasi-permanent record of a particular number dialed." Id. at 744-45.[43]

The same analysis applies to the meta data involved in this application. Users of e-mail [redacted] voluntarily expose addressing information for communications they send and receive to communications service providers. Having done so, they lack any legitimate expectation of privacy in such information for Fourth Amendment purposes.[44] Moreover, the relevant statutes put this form of pen register/trap and trace surveillance on a par with pen register/trap and trace surveillance of telephone calls, on the

---

[43] While Smith involved a pen register, its reasoning equally applies to trap and trace devices that capture the originating numbers of incoming calls. See, e.g., United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990).

[44] Cf. Guest v. Leis, 255 F.3d 325, 335-36 (6th Cir. 2001) (users of computer bulletin board service lacked reasonable expectation of privacy in subscriber information that they provided to systems operator); United States v. Kennedy, 81 F.Supp.2d 1103, 1110 (D. Kan. 2000) (no reasonable expectation of privacy in subscriber information provided to ISP); United States v. Hambrick, 55 F.Supp.2d 504, 508-09 (W.D. Va. 1999) (no reasonable expectation of privacy in screen name and other information provided to ISP), aff'd, 225 F.3d 656 (4th Cir. 2000) (Table).

premise that neither form of surveillance involves a Fourth Amendment search or seizure.[45]

This conclusion is equally well-founded for the proposed collection of [redacted] Nothing in the Smith analysis depends on the fact that a telephone pen register acquires addressing information for a call while it is being placed, rather than from data [redacted] Indeed, the controlling principle – that voluntary disclosure of information to a third party vitiates any legitimate expectation that the third party will not provide it to the government – has been applied to records [redacted] See Jerry T. O'Brien, Inc., 467 U.S. at 737-38, 743 (records of prior stock

[45] The USA PATRIOT Act amended 18 U.S.C. § 3127 to clarify that its definitions of "pen register" and "trap and trace device" applied to Internet communications. See Public Law 107-56, Title II, § 216(c); 147 Cong. Rec. S11000 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) (noting that prior statutory language was "ill-equipped" for Internet communications and supporting clarification of "the statute's proper application to tracing communications in an electronic environment . . . in a manner that is technology neutral"). Authorization to install such devices requires relevance to an investigation, but not any showing of probable cause. See 18 U.S.C. § 3123(a)(1), (2) (ordinary criminal investigation); 50 U.S.C. § 1842(a)(1), (c)(2) (investigation conducted under guidelines approved under Executive Order 12333).

trading); Miller, 425 U.S. at 436-38, 443 (checks, deposit slips, and other bank records).[46]

For these reasons, it is clear that, in ordinary circumstances, pen register/trap and trace surveillance of Internet communications does not involve a Fourth Amendment search or seizure. However, since this application involves unusually broad collection and distinctive modes of analyzing information, the Court will explain why these special circumstances do not alter its conclusion that no Fourth Amendment search or seizure is involved.

First, regarding the breadth of the proposed surveillance, it is noteworthy that the application of the Fourth Amendment depends on the government's intruding into some individual's reasonable expectation of privacy. Whether a large number of persons are otherwise affected by the government's conduct is irrelevant. Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched."

[redacted]

Steagald v. United States, 451 U.S. 204, 219 (1981); accord, e.g., Rakas v. Illinois, 439 U.S. 128, 133 (1978) ("'Fourth Amendment rights are personal rights which . . . may not be vicariously asserted.'") (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)). Since the Fourth Amendment bestows "a personal right that must be invoked by an individual," a person "claim[ing] the protection of the Fourth Amendment . . . must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable." Minnesota v. Carter, 525 U.S. 83, 88 (1998). So long as no individual has a reasonable expectation of privacy in meta data, the large number of persons whose communications will be subjected to the proposed pen register/trap and trace surveillance is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur.

Regarding the proposed analytical uses of the archived meta data, it might be thought that [redacted] not immediately available from conventional pen register/trap and

trace surveillance might itself implicate the Fourth Amendment.[47] However, that suggestion would be at odds with precedent that the subsequent use of the results of a search cannot itself involve an additional or continuing violation of the Fourth Amendment. For example, in United States v. Calandra, 414 U.S. 338 (1974), it was argued that each question before a grand jury "based on evidence obtained from an illegal search and seizure constitutes a fresh and independent violation of the witness' constitutional rights," and that such questioning involved "an additional intrusion" into the privacy of the witness "in violation of the

---

[47] The public disclosure of aggregated and compiled data has been found to impinge on privacy interests protected under the Freedom of Information Act (FOIA), even if the information was previously available to the public in a scattered, less accessible form. See United States Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989) (FBI "rap sheets," including public-record information on arrests and disposition of criminal charges, qualified for "personal privacy" exemption from disclosure under FOIA, 5 U.S.C. § 552(b)(7)(C)); but cf. Paul v. Davis, 424 U.S. 693, 712-13 (1976) (circulating a flyer publicizing an arrest for shoplifting did not violate constitutional right to privacy). In this case, because section 1842 authorizes the Attorney General to apply for pen register/trap and trace authorities "[n]othwithstanding any other provision of law," 50 U.S.C. § 1842(a)(1), and states that the Court "shall enter an ex parte order . . . approving the installation and use of a pen register or trap and trace device" upon a finding "that the application satisfies the requirements of [section 1842]," id. § 1842(d)(1), the Court has no need to consider how other statutes, such as the Privacy Act, 5 U.S.C. § 552a, might apply to the proposed activities of the Government.

Fourth Amendment." 414 U.S. at 353 & n.9 (internal quotations omitted). The Court rejected this argument, explaining:

> The purpose of the Fourth Amendment is to prevent unreasonable governmental intrusions into the privacy of one's person, house, papers, or effects. . . . That wrong . . . is fully accomplished by the original search without probable cause. Grand jury questions based on evidence obtained thereby involve no independent governmental invasion of one's person, house, papers, or effects . . . . Questions based on illegally obtained evidence are only a derivative use of the product of a past unlawful search and seizure. They work no new Fourth Amendment wrong.

414 U.S. at 354 (emphasis added); accord United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990); United States v. Leon, 468 U.S. 897, 906 (1984); see also United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information.").

In this case, sophisticated analysis of archived meta data may yield more information about a person's Internet communications than what would at first be apparent. Nevertheless, such analysis would, like the grand jury questioning in Calandra, involve merely a derivative use of information already obtained, rather than an independent governmental invasion of matters protected by the Fourth

Amendment. Accordingly, the Court finds that the proposed collection and analysis does not involve a search or seizure under the Fourth Amendment.

B. First Amendment Issues

By letter dated [redacted] the Court asked the Government to address "the general First Amendment implications of collecting and retaining this large volume of information that is derived, in part, from the communications of U.S. persons." In response, the Government acknowledges that surveillance that acquires "the contents of communications might in some cases implicate First Amendment interests, in particular the freedom of association," Government's Letter of [redacted] at 1, but denies or minimizes the First Amendment implications of surveillance that only acquires non-content addressing information.

The weight of authority supports the conclusion that Government information-gathering that does not constitute a Fourth Amendment search or seizure will also comply with the First Amendment when conducted as part of a good-faith criminal investigation. See Reporters Comm. for Freedom of the Press v. AT&T, 593 F.2d 1030, 1051 (D.C. Cir. 1978) (First Amendment protects activities "subject to the general and incidental

burdens that arise from good faith enforcement of otherwise valid criminal and civil laws that are not themselves" directed at First Amendment conduct; accordingly, subpoenas to produce reporters' telephone toll records without prior notice did not violate the First Amendment) (emphasis in original); United States v. Aguilar, 883 F.2d 662, 705 (9th Cir. 1989) (use of undercover informants "to infiltrate an organization engaged in protected first amendment activities" must be part of investigation "conducted in good faith; i.e., not for the purpose of abridging first amendment freedoms"); United States v. Gering, 716 F.2d 615, 620 (9th Cir. 1983) (mail covers targeting minister at residence and church upheld against First Amendment challenge absent showing "that mail covers were improperly used and burdened . . . free exercise or associational rights"). Conversely,

> all investigative techniques are subject to abuse and can conceivably be used to oppress citizens and groups, rather than to further proper law enforcement goals. In some cases, bad faith use of these techniques may constitute an abridgment of the First Amendment rights of the citizens at whom they are directed.

Reporters Comm., 593 F.2d at 1064.[48]

---

[48] Part of Judge Wilkey's opinion in Reporters Comm. categorically concludes that the First Amendment affords no protections against government investigation beyond what is

(continued...)

Here, the proposed collection of meta data is not for ordinary law enforcement purposes, but in furtherance of the compelling national interest of identifying and tracking [redacted] and ultimately of thwarting terrorist attacks. The overarching investigative effort against [redacted] is not aimed at curtailing First Amendment activities and satisfies the "good faith" requirement described in the above-cited cases. However, the extremely broad nature of this collection carries with it a heightened risk that collected information could be subject to various forms of misuse, potentially involving abridgement of First Amendment rights of innocent persons. For this reason, special restrictions on the accessing, retention, and dissemination of such information are necessary to guard against such misuse. See pages 82-87 below. With such restrictions in place, the proposed collection of non-

---

[48](...continued)
provided by the Fourth and Fifth Amendments. Id. at 1053-60. However, that part of the opinion was not joined by the other judge in the majority, who opined that the result of First Amendment analysis "may not always coincide with that attained by application of Fourth Amendment doctrine." Id. at 1071 n.4 (Robinson, J.).

content addressing information does not violate the First Amendment.[49]

IV. TO ENSURE LAWFUL IMPLEMENTATION OF THIS SURVEILLANCE AUTHORITY, NSA IS ORDERED TO COMPLY WITH THE PROPOSED RESTRICTIONS AND PROCEDURES, AS MODIFIED BY THE COURT.

The proposed collection involves an extraordinarily broad implementation of a type of surveillance that Congress has regulated by statute, even in its conventional, more narrowly targeted form. To ensure that this authority is implemented in a lawful manner, NSA is ordered to comply with the restrictions and procedures set out below at pages 82-87, which the Court has adapted from the Government's application.[50] Adherence to them

---

[49] The court in Paton v. La Prade, 469 F. Supp. 773, 780-82 (D.N.J. 1978), held that a mail cover on a dissident political organization violated the First Amendment because it was authorized under a regulation that was overbroad in its use of the undefined term "national security." In contrast, this pen register/trap and trace surveillance does not target a political group and is authorized pursuant to statute on the grounds of relevance to an investigation to protect against "international terrorism," a term defined at 50 U.S.C. § 1801(c). This definition has been upheld against a claim of First Amendment overbreadth. See United States v. Falvey, 540 F. Supp. 1306, 1314-15 (E.D.N.Y. 1982).

[50] The principal changes that the Court has made from the procedures described in the application are the inclusion of a "First Amendment proviso" as part of the "reasonable suspicion" standard for an [redacted] to be used as the basis for querying archived meta data, see pages 57-58 above, the adoption of a date after which meta data may not be retained, see pages 70-71 below, and an enhanced role for the NSA's Office of

(continued...)

will help ensure that this information is used for the stated purpose of its collection - the identification and tracking of [redacted] their Internet communications - thereby safeguarding the continued validity of the certification of relevance under § 1842(c)(2). These procedures will also help effectuate 50 U.S.C. § 1845(a)(2), which directs that no information from a Court-authorized pen register or trap and trace device "may be used or disclosed by Federal officers or employees except for lawful purposes," and ensure that such use and disclosure will not abridge First Amendment rights.

The Court's letter of [redacted] asked the Government to explain "[f]or how long . . . the information collected under this authority [would] continue to be of operational value to the counter-terrorism investigation(s) for which it is collected." The Government's letter of [redacted], stated that such information "would continue to be of significant operational value for at least 18 months," based on NSA's "analytic judgment." [redacted] Letter at 3. During that period, meta

---

[50](...continued)
General Counsel in the implementation of this authority, see pages 84-85 below. The Court recognizes that, as circumstances change and experience is gained in implementing this authority, the Government may propose other modifications to these procedures.

data would be available to analysts online for authorized querying. After 18 months, NSA "believes that there continues to be operational value in retaining e-mail meta data . . . in an 'off-line' storage system," since "in certain circumstances" information of that age could "provide valuable leads for the investigation into [redacted]" Id. However, the value of such information "would diminish over time," so that "NSA assesses that meta data would have operational value in off-line storage for a period of three years, and could be destroyed after that time (that is, a total of four and one-half years after it was initially collected)." Id. In accordance with this assessment, NSA is ordered to destroy archived meta data collected under this authority no later than four and one-half years after its initial collection.

* * *

Accordingly, a verified application having been made by the Attorney General of the United States for an order authorizing installation and use of pen registers and trap and trace devices pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States Code (U.S.C.), §§ 1801-1811, 1841-1846, and full consideration having been given

to the matters set forth therein, the Court finds, on the grounds explained above, that:

1. The Attorney General is authorized to approve applications for pen registers and trap and trace devices under the Act and to make such applications under the Act.

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

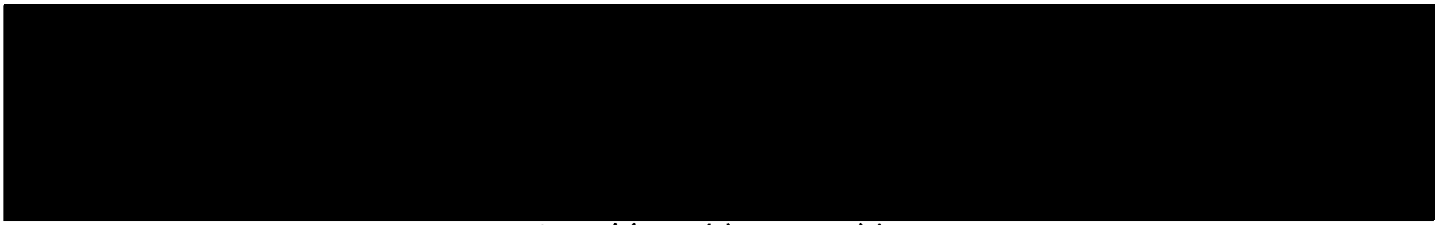
3. [redacted] in the United States and abroad are the subjects of National Security investigations conducted by the Federal Bureau of Investigation (FBI) under guidelines approved by the Attorney General pursuant to Executive Order No. 12333.

4. The pen registers and trap and trace devices [redacted]

[redacted]

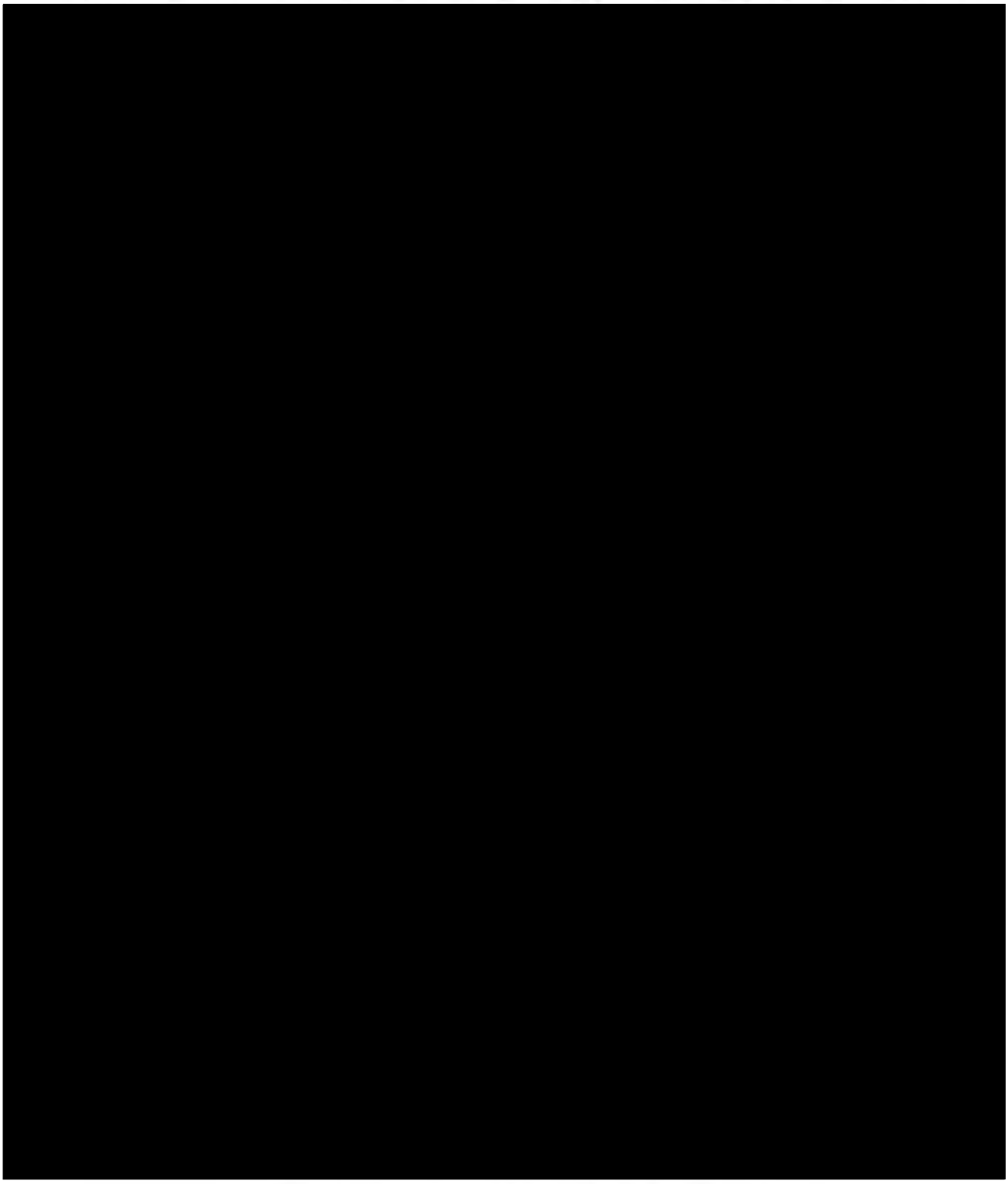
[51] The Government has represented that it is overwhelmingly likely that at [redacted]

[52] The Government has represented that it is overwhelmingly likely that [redacted]



[redacted]

[53] The Government has represented that it is overwhelmingly likely that [redacted]

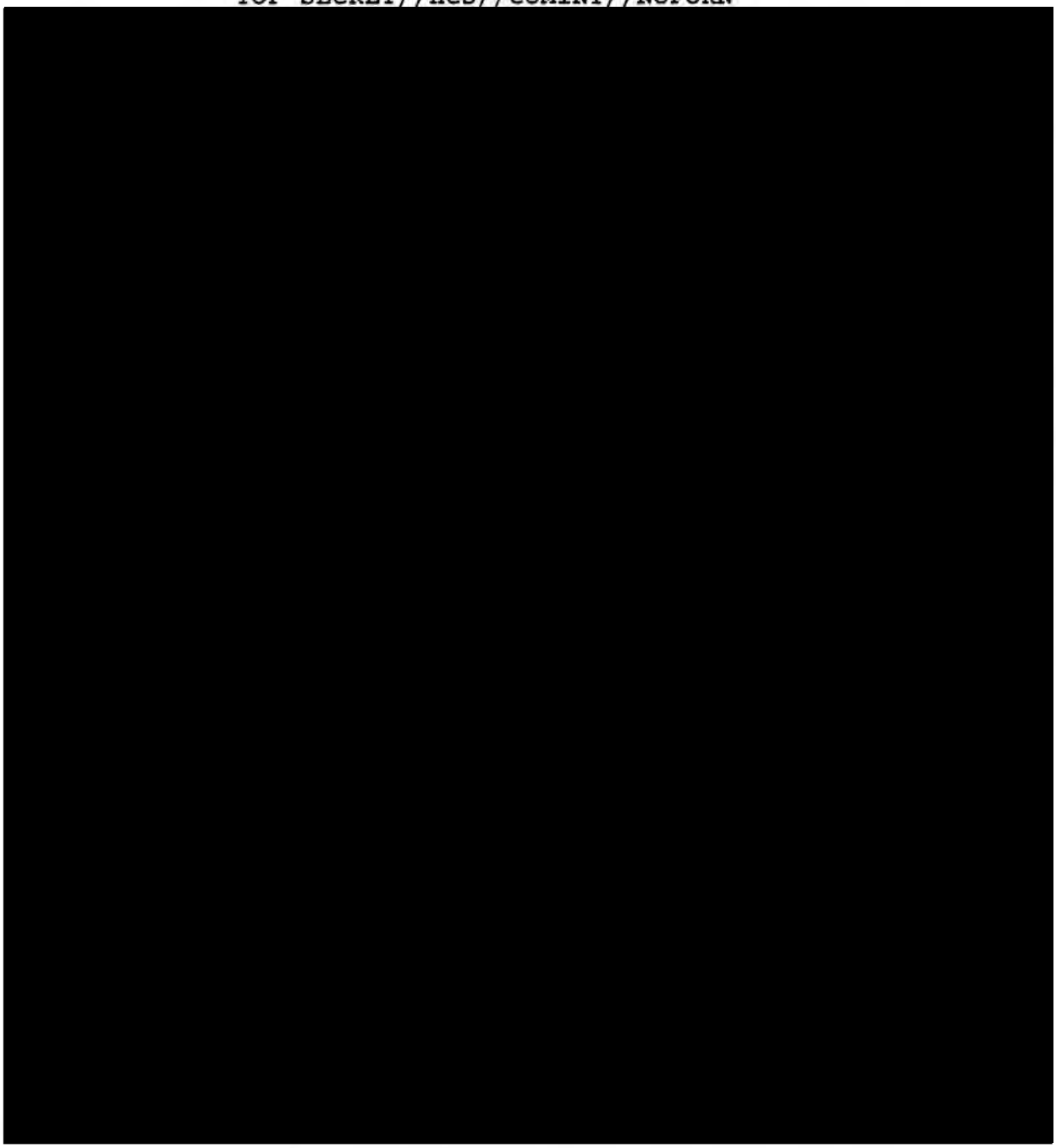


[redacted]

[54] The Government has represented that the majority of the communications [redacted]

[redacted]

[55] Because electronic communications will [redacted]



[redacted]

WHEREFORE, the Court finds that the application of the United States [redacted] pen registers and trap and trace devices, as described in the application, satisfies the requirements of the Act and specifically of 50 U.S.C. § 1842 and, therefore,

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

FURTHER ORDERED, as follows:

(1) Installation and use of pen registers and trap and trace devices as requested in the Government's application is authorized for a period of **ninety days** from the date of this Opinion and Order, unless otherwise ordered by this Court, as follows: installation and use of pen registers and/or trap and

trace devices as described above to collect all addressing and routing information reasonably likely to identify the sources or destinations of the electronic communications identified above on [redacted] identified above, including the "to," "from," "cc," and "bcc" fields for those communications [redacted] Collection of the contents of such communications as defined by 18 U.S.C. § 2510(8) is not authorized.

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

(3) As requested in the application, [redacted] (specified persons), are directed to furnish the NSA with

---

[57] Although the application makes clear that the assistance of these specified persons is contemplated, it does not expressly request that the Court direct these specified persons to assist the surveillance. However, because the application, at 24, requests that the Court enter the proposed orders submitted with the application and those proposed orders would direct the specified persons to provide assistance, the application effectively requests the Court to direct such assistance.

any information, facilities, or technical assistance necessary to accomplish the installation and operation of pen registers and trap and trace devices in such a manner as will protect their secrecy and produce a minimum amount of interference with the services each specified person is providing to its subscribers. Each specified person shall not disclose the existence of the investigation or of the pen registers and trap and trace devices to any person, unless or until ordered by the Court, and shall maintain all records concerning the pen registers and trap and trace devices, or the aid furnished to the NSA, under the security procedures approved by the Attorney General [redacted] that have previously been or will be furnished to each specified person and are on file with this Court.

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

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

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

b. The ability to access such information shall be limited to ten specially cleared analysts and to specially cleared administrators. The NSA shall ensure that the mechanism for accessing such information will automatically generate a log of auditing information for each occasion when the information is accessed, to include the accessing user's login, IP address, date and time, and retrieval request.

c. Such information shall be accessed only through queries using the contact chaining [redacted] methods described at page 43 above. Such queries shall be performed only on the basis of a particular known [redacted] after the NSA has concluded, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, that there are facts giving rise to a reasonable articulable suspicion that [redacted] is associated with [redacted] provided, however, that [redacted] believed to be used by a U.S. person shall not be regarded as associated with [redacted]

[redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution. Queries shall only be conducted with the approval of one of the following NSA officials: the Program Manager, Counterterrorism Advanced Analysis; the Chief or Deputy Chief, Counterterrorism Advanced Analysis Division; or a Counterterrorism Advanced Analysis Shift Coordinator in the Analysis and Production Directorate of the Signals Intelligence Directorate.

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

i) ensure that analysts with the ability to access such information receive appropriate training and guidance regarding the querying standard set out in paragraph c. above, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of such information.

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

iii) to ensure appropriate consideration of any First Amendment issues, review and approve proposed queries of meta data in online or "off-line" storage based on seed accounts used by U.S. persons.[58]

e. The NSA shall apply the Attorney General-approved guidelines in United States Signals Intelligence Directive 18 (Attachment D to the application) to minimize information concerning U.S. persons obtained from the pen registers and trap and trace devices authorized herein. Prior to disseminating any U.S. person information outside of the NSA, the Chief of Customer Response in the NSA's Signals Intelligence Directorate shall determine that the information is related to counterterrorism information and is necessary to understand the counterterrorism information or to assess its importance.

f. Information obtained from the authorized pen registers and trap and trace devices shall be available

---

[58] The Court notes that, in conventional pen register/trap and trace surveillances, there is judicial review of the application before any [redacted] In this case, the analogous decision to use a particular e-mail account as a seed account takes place [redacted] In these circumstances, it shall be incumbent on NSA's Office of General Counsel to review the legal adequacy for the basis of such queries, including the First Amendment proviso, set out in paragraph c. above.

online for querying, as described in paragraphs b. and c. above, for eighteen months. After such time, such information shall be transferred to an "off-line" tape system, which shall only be accessed by a cleared administrator in order to retrieve information that satisfies the standard for online accessing stated in paragraph c. above and is reasonably believed, despite its age, to be relevant to an ongoing investigation of [redacted] Searches of meta data in "off-line" storage shall be approved by one of the officials identified in paragraph c. above.

g. Meta data shall be destroyed no later than 18 months after it is required to be put into "off-line" storage, i.e., no later than four and one-half years after its initial collection.

h. Any application to renew or reinstate the authority granted herein shall include:

i) a report discussing queries that have been made since the prior application to this Court and the NSA's application of the standard set out in paragraph c. above to those queries.

ii) detailed information regarding [redacted] proposed to be added to such authority.

iii) any changes in the description of the [redacted] above or in the nature of the communications [redacted]

iv) any changes in the proposed means of collection, to include [redacted] the pen register and/or trap and trace devices [redacted]

Signed [redacted] 10:30 a.m. E.D.T.
Date Time

This authorization regarding [redacted] **in the United States and Abroad** expires on the [redacted] at 5:00 p.m., Eastern Daylight Time.

Colleen Kollar-Kotelly

COLLEEN KOLLAR-KOTELLY
Presiding Judge, United States Foreign Intelligence Surveillance Court

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR 13-158

MEMORANDUM

The Court has today issued the Primary Order appended hereto granting the "Application for Certain Tangible Things for Investigations to Protect Against International Terrorism" ("Application"), which was submitted to the Court on October

10, 2013, by the Federal Bureau of Investigation ("FBI"). The Application requested the issuance of orders pursuant to 50 U.S.C. § 1861, as amended (also known as Section 215 of the USA PATRIOT Act), requiring the ongoing daily production to the National Security Agency ("NSA") of certain telephone call detail records in bulk.

The Primary Order appended hereto renews the production of records made pursuant to the similar Primary Order issued by the Honorable Claire V. Eagan of this Court on July 19, 2013 in Docket Number BR 13-109 ("July 19 Primary Order"). On August 29, 2013, Judge Eagan issued an Amended Memorandum Opinion setting forth her reasons for issuing the July 19 Primary Order ("August 29 Opinion"). Following a declassification review by the Executive Branch, the Court published the July 19 Primary Order and August 29 Opinion in redacted form on September 17, 2013.

The call detail records to be produced pursuant to the orders issued today in the above-captioned docket are identical in scope and nature to the records produced in response to the orders issued by Judge Eagan in Docket Number BR 13-109. The records will be produced on terms identical to those set out in Judge Eagan's July 19 Primary Order and for the same purpose, and the information acquired by NSA through the production will be subject to the same provisions for oversight and identical restrictions on access, retention, and dissemination.

This is the first time that the undersigned has entertained an application requesting the bulk production of call detail records. The Court has conducted an independent review of the issues presented by the application and agrees with and adopts Judge Eagan's analysis as the basis for granting the Application. The Court writes separately to discuss briefly the issues of "relevance" and the inapplicability of the Fourth Amendment to the production.

Although the definition of relevance set forth in Judge Eagan's decision is broad, the Court is persuaded that that definition is supported by the statutory analysis set out in the August 29 Opinion. That analysis is reinforced by Congress's re-enactment of Section 215 after receiving information about the government's and the FISA Court's interpretation of the statute. Although the existence of this program was classified until several months ago, the record is clear that before the 2011 re-enactment of Section 215, many Members of Congress were aware of, and each Member had the opportunity to learn about, the scope of the metadata collection and this Court's interpretation of Section 215. Accordingly, the re-enactment of Section 215 without change in 2011 triggered the doctrine of ratification through re-enactment, which provides a strong reason for this Court to continue to adhere to its prior interpretation of Section 215. See Lorillard v. Pons, 434 U.S. 575, 580 (1978); see also EEOC v. Shell Oil Co., 466 U.S. 54, 69 (1984); Haig v. Agee, 453 U.S. 280, 297-98 (1981).

The undersigned also agrees with Judge Eagan that, under Smith v. Maryland, 442 U.S. 735 (1979), the production of call detail records in this matter does not constitute a search under the Fourth Amendment. In Smith, the Supreme Court held that the use of a pen register to record the numbers dialed from the defendant's home telephone did not constitute a search for purposes of the Fourth Amendment. In so holding, the Court stressed that the information acquired did not include the contents of any communication and that the information was acquired by the government from the telephone company, to which the defendant had voluntarily disclosed it for the purpose of completing his calls.

The Supreme Court's more recent decision in United States v. Jones, — U.S. —, 132 S. Ct. 945 (2012), does not point to a different result here. Jones involved the acquisition of a different type of information through different means. There, law enforcement officers surreptitiously attached a Global Positioning System (GPS) device to the defendant's vehicle and used it to track his location for 28 days. The Court held in Justice Scalia's majority opinion that the officers' conduct constituted a search under the Fourth Amendment because the information at issue was obtained by means of a physical intrusion on the defendant's vehicle, a constitutionally-protected area. The majority declined to decide whether use of the GPS device, without the physical intrusion, impinged upon a reasonable expectation of privacy.

Five Justices in Jones signed or joined concurring opinions suggesting that the precise, pervasive monitoring by the government of a person's location could trigger Fourth Amendment protection even without any physical intrusion. This matter, however, involves no such monitoring. Like Smith, this case concerns the acquisition of non-content metadata other than location information. See Aug. 29 Op. at 29 at 4 n.5; id. at 6 & n.10.

Justice Sotomayor stated in her concurring opinion in Jones that it "may be necessary" for the Supreme Court to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," which she described as "ill suited to the digital age." See Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing Smith and United States v. Miller, 425 U.S. 435, 443 (1976), as examples of decisions relying upon that premise). But Justice Sotomayor also made clear that the Court undertook no such reconsideration in Jones. See id. ("Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision."). The Supreme Court may some day revisit the third-party disclosure principle in the context of twenty-first century communications technology, but that day has not arrived. Accordingly, Smith remains controlling with respect to the acquisition by the government from service providers of non-content telephony

metadata such as the information to be produced in this matter.

In light of the public interest in this matter and the government's declassification of related materials, including substantial portions of Judge Eagan's August 29 Opinion and July 19 Primary Order, the undersigned requests pursuant to FISC Rule 62 that this Memorandum and the accompanying Primary Order also be published and directs such request to the Presiding Judge as required by the Rule.

ENTERED this 11th day of October, 2013.

Mary A. McLaughlin

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

[redacted]

~~TOP SECRET//SI//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR 13-158

PRIMARY ORDER

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

~~TOP SECRET//SI//NOFORN~~

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

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number BR 13-109 and its predecessors. [50 U.S.C. § 1861(c)(1)]

Accordingly, and as further explained in the accompanying Memorandum, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

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

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"[1] created by [redacted]

B. The Custodian of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

[1] For purposes of this Order "telephony metadata" includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer. Furthermore, this Order does not authorize the production of cell site location information (CSLI).

thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by [redacted] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [redacted]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.[2] The BR metadata shall carry unique markings such

[2] The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.[3] Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms[4] that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

---

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

[3] The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.

[redacted]

but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through queries of the BR metadata to obtain contact chaining information as described in paragraph 17 of the Declaration o[redacted] [redacted] attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.[5] NSA shall ensure,

[5] For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.

through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.[6]

(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [redacted]

[redacted]

[6] This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[redacted]

[redacted] provided, however, that NSA's Office of General Counsel (OGC)

[redacted]

shall first determine that any selection term reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [redacted] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. The preceding sentence shall not apply to selection terms under surveillance

[redacted]

pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated with [redacted] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.[9,10]

---

[9] The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the selection term is or was associated with a Foreign Power shall be specified. The automated query process described in the [redacted] Declaration limits the first hop query results to the specified time frame. Analysts conducting manual queries using that selection term shall continue to properly minimize information that may be returned within query results that fall outside of that timeframe.

[10] The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to this Orde[redacted]

(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.[11] This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns the hop-limited results from those queries to a "corporate store." The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms. The specifics of the automated query process, as described in the [redacted] Declaration, are as follows:

[redacted]

[11] This automated query process was initially approved by this Court in its November 8, 2012 Order amending docket number BR 12-178.

[12] As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms have not expired. This step does not use expired RAS-approved selection terms to create the list of "authorized query terms" (described below) regardless of whether the list of RAS-approved selection terms is up-to-date.

[redacted]

D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first

---

[redacted]

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.[15] NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.[16] Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch

[15] In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

[16] In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.[17] OGC shall provide NSD/DoJ with copies

[17] The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.

(vii) Other than the automated query process described in the [redacted] Declaration and this Order, prior to implementation of any new or modified automated query processes, such new or modified processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of NSA's application of the RAS standard, as well as NSA's implementation and operation of the automated query process. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials

authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

This authorization regarding [redacted] expires on the 3RD day of January, 2014, at 5:00 p.m., Eastern Time.

Signed 10-11-2013 P12:05 Eastern Time
Date Time

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR 13-109

AMENDED MEMORANDUM OPINION

I. Background.

On July 18, 2013, a verified Final "Application for Certain Tangible Things for Investigations to Protect Against International Terrorism" (Application) was submitted to the Court by the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States

Code (U.S.C.), § 1861, as amended (also known as Section 215 of the USA PATRIOT Act),[1] requiring the ongoing daily production to the National Security Agency (NSA) of certain call detail records or "telephony metadata" in bulk.[2] The Court, after having fully considered the United States Government's (government) earlier-filed Proposed Application pursuant to Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 9(a),[3] and having held an extensive hearing to receive testimony and

---

[1] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) ("PATRIOT Act"), amended by, "USA PATRIOT Improvement Reauthorization Act of 2005," Pub. L. No. 109-177, 120 Stat. 192 (Mar. 9, 2006); "USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006," Pub. L. No. 109-178, 120 Stat. 278 (Mar. 9, 2006); and Section 215 expiration extended by "Department of Defense Appropriations Act, 2010," Pub. L. No. 111-118 (Dec. 19, 2009); "USA PATRIOT—Extension of Sunsets," Pub. L. No. 111-141 (Feb. 27, 2010); "FISA Sunsets Extension Act of 2011," Pub. L. No. 112-3 (Feb. 25, 2011); and, "PATRIOT Sunsets Extension Act of 2011," Pub. L. No. 112-14, 125 Stat. 216 (May 26, 2011).

[2] For purposes of this matter, "'telephony metadata' includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile station Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer." App. at 4. In addition, the Court has explicitly directed that its authorization does not include "the production of cell site location information (CSLI)." Primary Ord. at 3.

[3] Prior to scheduling a hearing in this matter, the Court reviewed the Proposed Application and its filed Exhibits pursuant to its standard procedure. Exhibit A consists of a Declaration from the NSA in support of the government's Application. As Ordered by this Court in Docket No. BR 13-80, Exhibit B is a Renewal Report to describe any significant changes proposed in the way in which records would be received, and any significant changes to controls NSA has in place to receive, store, process, and disseminate the information. [redacted] It also provides the final segment of information normally contained in the 30-day reports discussed below. As Ordered by this Court in Docket No. BR 13-80, Exhibit C is a summary of a meeting held by Executive Branch representatives to assess compliance with this Court's Orders. Furthermore, the Court reviewed the previously filed 30-day reports that were Ordered by this Court in Docket No. 13-80, discussing NSA's application of the reasonable, articulable suspicion (RAS) standard for approving selection terms and implementation of the automated query process. In addition, the 30-day reports describe disseminations of U.S.-person information obtained under this program.

evidence on this matter on July 18, 2013,[4] GRANTED the application for the reasons stated in this Memorandum Opinion and in a Primary Order issued on July 19, 2013, which is appended hereto.

In conducting its review of the government's application, the Court considered whether the Fourth Amendment to the U.S. Constitution imposed any impediment to the government's proposed collection. Having found none in accord with U.S. Supreme Court precedent, the Court turned to Section 215 to determine if the proposed collection was lawful and that Orders requested from this Court should issue. The Court found that under the terms of Section 215 and under operation of the canons of statutory construction such Orders were lawful and required, and the requested Orders were therefore issued.

---

[4] The proceedings were conducted *ex parte* under security procedures as mandated by 50 U.S.C. §§ 1803(c), 1861(c)(1), and FISC Rules 3, 17(a)-(b). See Letter from Presiding Judge Walton, U.S. FISC to Chairman Leahy, Senate Judiciary Committee (Jul. 29, 2013), at 7 (noting that initial proceedings before the FISC are handled *ex parte* as is the universal practice in courts that handle government requests for orders for the production of business records, pen register/trap and trace implementation, wiretaps, and search warrants), http://www.uscourts.gov/uscourts/fisc/honorable-patrick-leahy.pdf. Pursuant to FISC Rules 17(b)-(d), this Court heard oral argument by attorneys from the U.S. Department of Justice, and received sworn testimony from personnel from the FBI and NSA. The Court also entered into evidence Exhibits 1-7 during the hearing. Except as cited in this Memorandum Opinion, at the request of the government, the transcript of the hearing has been placed under seal by Order of this Court for security reasons. Draft Tr. at 3-4. At the hearing, the government notified the Court that it was developing an updated legal analysis expounding on its legal position with regard to the application of Section 215 to bulk telephony metadata collection. Draft Tr. at 25. The government was not prepared to present such a document to the Court. The Court is aware that on August 9, 2013, the government released to the public an "Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act" (Aug. 9, 2013). The Court, however, has not reviewed the government's "White Paper" and the "White Paper" has played no part in the Court's consideration of the government's Application or this Memorandum Opinion.

Specifically, the government requested Orders from this Court to obtain certain business records of specified telephone service providers. Those telephone company business records consist of a very large volume of each company's call detail records or telephony metadata, but expressly exclude the contents of any communication; the name, address, or financial information of any subscriber or customer; or any cell site location information (CSLI). Primary Ord. at 3 n.1.[5] The government requested production of this data on a daily basis for a period of 90 days. The sole purpose of this production is to obtain foreign intelligence information in support of [redacted] individual authorized investigations to protect against international terrorism and concerning various international terrorist organizations. See Primary Ord. at 2, 6; App. at 8; and, Ex. A. at 2-3. In granting the government's request, the Court has prohibited the government from accessing the data for any other intelligence or investigative purpose.[6] Primary Ord. at 4.

---

[5] In the event that the government seeks the production of CSLI as part of the bulk production of call detail records in the future, the government would be required to provide notice and briefing to this Court pursuant to FISC Rule 11. The production of all call detail records of all persons in the United States has never occurred under this program. For example, the government [redacted] App. at 13 n.4.

[6] The government may, however, permit access to "trained and authorized technical personnel ... to perform those processes needed to make [the data] usable for intelligence analysis," Primary Ord. at 5, and may share query results "[1] to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate lawful oversight functions." Id. at 14.

By the terms of this Court's Primary Order, access to the data is restricted through technical means, through limits on trained personnel with authorized access, and through a query process that requires a reasonable, articulable suspicion (RAS), as determined by a limited set of personnel, that the selection term (e.g., a telephone number) that will be used to search the data is associated with one of the identified international terrorist organizations.[7] Primary Ord. at 4-9. Moreover, the government may not make the RAS determination for selection terms reasonably believed to be used by U.S. persons solely based on activities protected by the First Amendment. Id. at 9; and see 50 U.S.C. § 1861(a)(1). To ensure adherence to its Orders, this Court has the authority to oversee compliance, see 50 U.S.C. § 1803(h), and requires the government to notify the Court in writing immediately concerning any instance of non-compliance, see FISC Rule 13(b). According to the government, in the prior authorization period there have been no compliance incidents.[8]

Finally, although not required by statute, the government has demonstrated through its written submissions and oral testimony that this production has been and remains valuable for obtaining foreign intelligence information regarding international

[7] A selection term that meets specific legal standards has always been required. This Court has not authorized government personnel to access the data for the purpose of wholesale "data mining" or browsing.

[8] The Court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information. Through oversight by this Court over a period of months, those issues were resolved.

terrorist organizations, see App. Ex. B at 3-4; Thirty-Day Report for Filing in Docket Number BR 13-80 (Jun. 25, 2013) at 3-4; Thirty-Day Report for Filing in Docket Number BR 13-80 (May 24, 2013) a 3-4.

II. Fourth Amendment.[9]

The production of telephone service provider metadata is squarely controlled by the U.S. Supreme Court decision in Smith v. Maryland, 442 U.S. 735 (1979). The Smith decision and its progeny have governed Fourth Amendment jurisprudence with regard to telephony and communications metadata for more than 30 years. Specifically, the Smith case involved a Fourth Amendment challenge to the use of a pen register on telephone company equipment to capture information concerning telephone calls,[10] but not the content or the identities of the parties to a conversation. Id. at 737, 741 (citing Katz v. United States, 389 U.S. 347 (1967), and United States v. New York Tel. Co., 434 U.S. 159 (1977)). The same type of information is at issue here.[11]

---

[9] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

[10] Because the metadata was obtained from telephone company equipment, the Court found that "petitioner obviously cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'" Id. at 741.

[11] The Court is aware that additional call detail data is obtained via this production than was acquired through the pen register acquisition at issue in Smith. Other courts have had the opportunity to review whether there is a Fourth Amendment expectation of privacy in call detail records similar to the data sought in this matter and have found that there is none. See United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009) (finding that because "data about the 'call origination, length, and time of call' ... is nothing more than pen register and trap and trace data, there is no Fourth Amendment 'expectation of privacy.'"

The Supreme Court in Smith recognized that telephone companies maintain call detail records in the normal course of business for a variety of purposes. Id. at 742 ("All subscribers realize ... that the phone company has facilities for making permanent records of the number they dial...."). This appreciation is directly applicable to a business records request. "Telephone users ... typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." Id. at 743. Furthermore, the Supreme Court found that once a person has transmitted this information to a third party (in this case, a telephone company), the person "has no legitimate expectation of privacy in [the] information...."[12] Id. The telephone user, having conveyed this information to a telephone company that retains the information in the ordinary course of business, assumes the risk that the company will provide that information to the

---

(citing Smith, 442 U.S. at 743-44)) cert. denied 559 U.S. 987, 988 (2010); United States Telecom Ass'n, 227 F.3d 450, 454 (D.C. Cir. 2000) (noting pen registers record telephone numbers of outgoing calls and trap and trace devices are like caller ID systems, and that such information is not protected by the Fourth Amendment); United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990) (recognizing that "[t]he installation and use of a pen register and trap and trace device is not a 'search' requiring a warrant pursuant to the Fourth Amendment," and noting that there is no "'legitimate expectation of privacy' at stake." (citing Smith, 442 U.S. at 739-46)).

[12] The Supreme Court has applied this principle – that there is no Fourth Amendment search when the government obtains information that has been conveyed to third parties – in cases involving other types of business records. See United States v. Miller, 425 U.S. 435 (1976) (bank records); see also S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984) ("It is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities.") (citing Miller, 425 U.S. at 443).

government. See id. at 744. Thus, the Supreme Court concluded that a person does not have a legitimate expectation of privacy in telephone numbers dialed and, therefore, when the government obtained that dialing information, it "was not a 'search,' and no warrant was required" under the Fourth Amendment. Id. at 746.[13]

In Smith, the government was obtaining the telephone company's metadata of one person suspected of a crime. See id. at 737. Here, the government is requesting daily production of certain telephony metadata in bulk belonging to companies without specifying the particular number of an individual. This Court had reason to analyze this distinction in a similar context in [redacted] In that case, this Court found that "regarding the breadth of the proposed surveillance, it is noteworthy that the application of the Fourth Amendment depends on the government's intruding into some individual's reasonable expectation of privacy." Id. at 62. The Court noted that Fourth Amendment rights are personal and individual, see id. (citing Steagald v. United States, 451 U.S. 204, 219 (1981); accord, e.g., Rakas v. Illinois, 439 U.S. 128, 133 (1978) ("'Fourth Amendment rights are personal rights which ... may not be vicariously asserted.'") (quoting Alderman v. United States, 394 U.S. 165, 174 (1969))), and that "[s]o long as no individual has a reasonable expectation of privacy

[13] If a service provider believed that a business records order infringed on its own Fourth Amendment rights, it could raise such a challenge pursuant to 50 U.S.C. § 1861(f).

in meta data, the large number of persons whose communications will be subjected to the ... surveillance is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur." Id. at 63. Put another way, where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*.

In sum, because the Application at issue here concerns only the production of call detail records or "telephony metadata" belonging to a telephone company, and not the contents of communications, Smith v. Maryland compels the conclusion that there is no Fourth Amendment impediment to the collection. Furthermore, for the reasons stated in [redacted] and discussed above, this Court finds that the volume of records being acquired does not alter this conclusion. Indeed, there is no legal basis for this Court to find otherwise.

III. Section 215.

Section 215 of the USA PATRIOT Act created a statutory framework, the various parts of which are designed to ensure not only that the government has access to the information it needs for authorized investigations, but also that there are protections and prohibitions in place to safeguard U.S. person information. It requires the government to demonstrate, among other things, that there is "an investigation to

obtain foreign intelligence information ... to [in this case] protect against international terrorism," 50 U.S.C. § 1861(a)(1); that investigations of U.S. persons are "not conducted solely upon the basis of activities protected by the first amendment to the Constitution," id.; that the investigation is "conducted under guidelines approved by the Attorney General under Executive Order 12333," id. § 1861(a)(2); that there is "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to the investigation, id. § 1861(b)(2)(A);[14] that there are adequate minimization procedures "applicable to the retention and dissemination" of the information requested, id. § 1861(b)(2)(B); and, that only the production of such things that could be "obtained with a subpoena *duces tecum*" or "any other order issued by a court of the United States directing the production of records" may be ordered, id. § 1861(c)(2)(D), see infra Part III.a. (discussing Section 2703(d) of the Stored Communications Act). If the Court determines that the government has met the requirements of Section 215, it shall enter an *ex parte* order compelling production.[15]

---

[14] This section also provides that the records sought are "presumptively relevant to an authorized investigation if the applicant shows in the statement of facts that they pertain to—(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known, to, a suspected agent of a foreign power who is the subject of such authorized investigation." 50 U.S.C. § 1861(b)(2)(A)(i)-(iii). The government has not invoked this presumption and, therefore, the Court need not address it.

[15] "Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of [Section 215], the judge *shall* enter an *ex parte* order as requested, or as modified, approving the release of tangible things." Id. § 1861(c)(1) (emphasis added). As indicated, the Court may modify the Orders as necessary, and compliance issues could present situations requiring modification.

This Court must verify that each statutory provision is satisfied before issuing the requested Orders. For example, even if the Court finds that the records requested are relevant to an investigation, it may not authorize the production if the minimization procedures are insufficient. Under Section 215, minimization procedures are "specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the 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." Id. § 1861(g)(2)(A). Congress recognized in this provision that information concerning U.S. persons that is not directly responsive to foreign intelligence needs will be produced under these orders and established post-production protections for such information. As the Primary Order issued in this matter demonstrates, this Court's authorization includes detailed restrictions on the government through minimization procedures. See Primary Ord. at 4-17. Without those restrictions, this Court could not, nor would it, have approved the proposed production. This Court's Primary Order also sets forth the requisite findings under Section 215 for issuing the Orders requested by the government in its Application. Id. at 2, 4-17.

The Court now turns to its interpretation of Section 215 with regard to how it compares to 18 U.S.C. § 2703 (Stored Communications Act); its determination that "there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation," 50 U.S.C. § 1861(b)(2)(A); and, the doctrine of legislative re-enactment as it pertains to the business records provision.

a. Section 215 of FISA and Section 2703(d) of the Stored Communications Act.

It is instructive to compare Section 215, which is used for foreign intelligence purposes and is codified as part of FISA, with 18 U.S.C. § 2703 ("Required disclosure of customer communications or records"), which is used in criminal investigations and is part of the Stored Communications Act (SCA). See In Re Production of Tangible Things From [redacted], Docket No. BR 08-13, Supp. Op. (Dec. 12, 2008) (discussing Section 215 and Section 2703). Section 2703 establishes a process by which the government can obtain information from electronic communications service providers, such as telephone companies. As with FISA, this section of the SCA provides the mechanism for obtaining either the contents of communications, or non-content records of communications. See 18 U.S.C. §§ 2703(a)-(c).

For non-content records production requests, such as the type sought here, Section 2703(c) provides a variety of mechanisms, including acquisition through a court order under Section 2703(d). Under this section, which is comparable to Section 215, the government must offer to the court "*specific and articulable* facts showing that there are reasonable grounds to believe that ... the records or other information sought, are *relevant and material* to an ongoing criminal investigation." Id. § 2703(d) (emphasis added). Section 215, the comparable provision for foreign intelligence purposes, requires neither "specific and articulable facts" nor does it require that the information be "material." Rather, it merely requires a statement of facts showing that there are reasonable grounds to believe that the records sought are relevant to the investigation. See 50 U.S.C. §1861(b)(2)(A). That these two provisions apply to the production of the same type of records from the same type of providers is an indication that Congress intended this Court to apply a different, and in specific respects lower, standard to the government's Application under Section 215 than a court reviewing a request under Section 2703(d). Indeed, the pre-PATRIOT Act version of FISA's business records provision required "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." 50 U.S.C. §1862(b)(2)(B) as it read on October 25, 2001.[16] In enacting Section 215,

[16] Prior to enactment of the PATRIOT Act, the business records provision was in Section 1862 vice 1861.

Congress removed the requirements for "specific and articulable facts" and that the records pertain to "a foreign power or an agent of a foreign power." Accordingly, now the government need not provide specific and articulable facts, demonstrate any connection to a particular suspect, nor show materiality when requesting business records under Section 215. To find otherwise would be to impose a higher burden – one that Congress knew how to include in Section 215, but chose to dispense with.

Furthermore, Congress provided different measures to ensure that the government obtains and uses information properly, depending on the purpose for which it sought the information. First, Section 2703 has no provision for minimization procedures. However, such procedures are mandated under Section 215 and must be designed to restrict the retention and dissemination of information, as imposed by this Court's Primary Order. Primary Ord. at 4-17; see 50 U.S.C. §§ 1861(c)(1), (g).

Second, Section 2703(d) permits the service provider to file a motion with a court to "quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause undue burden on such provider." Id. Congress recognized that, even with the higher statutory standard for a production order under Section 2703(d), some requests authorized by a court would be "voluminous" and provided a means by which the provider could seek relief using a motion. Id. Under Section 215, however, Congress

provided a specific and complex statutory scheme for judicial review of an Order from this Court to ensure that providers could challenge both the legality of the required production and the nondisclosure provisions of that Order. 50 U.S.C. § 1861(f). This adversarial process includes the selection of a judge from a pool of FISC judges to review the challenge to determine if it is frivolous and to rule on the merits, id. § 1861(f)(2)(A)(ii), provides standards that the judge is to apply during such review, id. §§ 1861(f)(2)(B)-(C), and provides for appeal to the Foreign Intelligence Surveillance Court of Review and, ultimately, the U.S. Supreme Court, id. § 1861(f)(3).[17] This procedure, as opposed to the motion process available under Section 2703(d) to challenge a production as unduly voluminous or burdensome, contemplates a substantial and engaging adversarial process to test the legality of this Court's Orders under Section 215.[18] This enhanced process appears designed to ensure that there are additional safeguards in light of the lower threshold that the government is required to meet for production under Section 215 as opposed to Section 2703(d). To date, no holder of

[17] For further discussion on the various means by which adversarial proceedings before the FISC may occur, see Letter from Presiding Judge Walton, U.S. FISC to Chairman Leahy, Senate Judiciary Committee (Jul. 29, 2013), at 7-10, http://www.uscourts.gov/uscourts/fisc/honorable-patrick-leahy.pdf.

[18] In In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F.Supp.2d 114, 128-29 (E.D. Va. 2011), the court found that only the service provider, as opposed to a customer or subscriber, could challenge the execution of a § 2703(d) non-content records order. The court reasoned that "[b]ecause Congress clearly provided ... protections for one type of § 2703 order [content] but not for others, the Court must infer that Congress deliberately declined to permit challenges for the omitted orders." Id. The court also noted that the distinction between content and non-content demonstrates an incorporation of Smith v. Maryland into the SCA. Id. at 128 n.11. As discussed above, the operation of Section 215 within FISA represents that same distinction.

records who has received an Order to produce bulk telephony metadata has challenged the legality of such an Order. Indeed, no recipient of any Section 215 Order has challenged the legality of such an Order, despite the explicit statutory mechanism for doing so.

When analyzing a statute or a provision thereof, a court considers the statutory schemes as a whole. See Kokoszka v. Belford, 417 U.S. 642, 650 (1974) (noting that when a court interprets a statute, it looks not merely to a particular clause but will examine it within the whole statute or statutes on the same subject) (internal quotation and citation omitted); Jones v. St. Louis-San Francisco Ry. Co., 728 F.2d 257, 262 (6th Cir. 1984) ("[W]here two or more statutes deal with the same subject, they are to be read *in pari materia* and harmonized, if possible. This rule of statutory construction is based upon the premise that when Congress enacts a new statute, it is aware of all previously enacted statutes on the same subject.") (citations omitted). Here, the Court finds that Section 215 and Section 2703(d) operate in a complementary manner and are designed for their specific purposes. In the criminal investigation context, Section 2703(d) includes front-end protections by imposing a higher burden on the government to obtain the information in the first instance. On the other hand, when the government seeks to obtain the same type of information, but for a foreign intelligence purpose, Congress provided the government with more latitude at the production stage under

Section 215 by not requiring specific and articulable facts or meeting a materiality standard. Instead, it imposed post-production checks in the form of mandated minimization procedures and a structured adversarial process. This is a logical framework and it comports well with the Fourth Amendment concept that the required factual predicate for obtaining information in a case of special needs, such as national security, can be lower than for use of the same investigative measures for an ordinary criminal investigation. See United States v. United States District Court (Keith), 407 U.S. 297, 308-09, 322-23 (1972); and, In re Sealed Case, 310 F.3d 717, 745-46 (FISA Ct. Rev. 2002) (differentiating requirements for the government to obtain information obtained for national security reasons as opposed to a criminal investigation).[19] Moreover, the government's interest is significantly greater when it is attempting to thwart attacks and disrupt activities that could harm national security, as opposed to gathering evidence on domestic crimes. See In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) ("[T]he relevant government interest—the interest in national security—is of the highest order of magnitude.") (citing Haig v. Agee, 453 U.S. 280, 307 (1981)); and, In re Sealed Case, 310 F.3d at 745-46.

[19] As discussed above, there is no Fourth Amendment interest here, as per Smith v. Maryland.

b. Relevance.

Because known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, the production of the information sought meets the standard for relevance under Section 215.

As an initial matter and as a point of clarification, the government's burden under Section 215 is not to prove that the records sought are, in fact, relevant to an authorized investigation. The explicit terms of the statute require "a statement of facts showing that there are *reasonable grounds to believe* that the tangible things sought are relevant...." 50 U.S.C. § 1861(b)(2)(A) (emphasis added). In establishing this standard, Congress chose to leave the term "relevant" undefined. It is axiomatic that when Congress declines to define a term a court must give the term its ordinary meaning. See, e.g., Taniguchi v. Kan Pacific Saipan, Ltd., ___ U.S. ___, 132 S.Ct. 1997, 2002 (2012). Accompanying the government's first application for the bulk production of telephone company metadata was a Memorandum of Law which argued that "[i]nformation is 'relevant' to an authorized international terrorism investigation if it bears upon, or is pertinent to, that investigation." Mem. of Law in Support of App. for Certain Tangible

Things for Investigations to Protect Against International Terrorism, Docket No. BR 06-05 (filed May 23, 2006), at 13-14 (quoting dictionary definitions, Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351 (1978), and Fed. R. Evid. 401[20]). This Court recognizes that the concept of relevance here is in fact broad and amounts to a relatively low standard.[21] Where there is no requirement for specific and articulable facts or materiality, the government may meet the standard under Section 215 if it can demonstrate reasonable grounds to believe that the information sought to be produced has some bearing on its investigations of the identified international terrorist organizations.

This Court has previously examined the issue of relevance for bulk collections. See [redacted]

[20] At the time of the government's submission in Docket No. BR 06-05, a different version of Fed. R. Evid. 401 was in place. While not directly applicable in this context, the current version reads: "Evidence is relevant if: (a) it has *any tendency* to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." (Emphasis added.)

[21] Even under the higher "relevant and material" standard for 18 U.S.C. § 2703(d), discussed above, "[t]he government need not show actual relevance, such as would be required at trial." In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F.Supp.2d 114, 130 (E.D. Va. 2011). The petitioners had argued in that case that most of their activity for which records were sought was "unrelated" and that "the government cannot be permitted to blindly request everything that 'might' be useful...." Id. (internal quotation omitted). The court rejected this argument, noting that "[t]he probability that some gathered information will not be material is not a substantial objection," and that where no constitutional right is implicated, as is the case here, "there is no need for ... narrow tailoring." Id.

[redacted]

[redacted] While those matters involved different collections from the one at issue here, the relevance standard was similar. See 50 U.S.C. § 1842(c)(2) ("[R]elevant to an ongoing investigation to protect against international terrorism...."). In both cases, there were facts demonstrating that information concerning known and unknown affiliates of international terrorist organizations was contained within the non-content metadata the government sought to obtain. As this Court noted in 2010, the "finding of relevance most crucially depended on the conclusion that bulk collection is *necessary* for NSA to employ tools that are likely to generate useful investigative leads to help identify and track terrorist operatives." [redacted]

[redacted] Indeed, in [redacted] this Court noted that bulk collections such as these are "necessary to identify the much smaller number of [international terrorist] communications." [redacted]

As a result, it is this showing of necessity that led the Court to find that "the entire mass of collected metadata is relevant to investigating [international terrorist groups] and affiliated persons." [redacted]

This case is no different. The government stated, and this Court is well aware, that individuals associated with international terrorist organizations use telephonic systems to communicate with one another around the world, including within the United States. Ex. A. at 4. The government argues that the broad collection of telephone company metadata "is necessary to create a historical repository of metadata that enables NSA to find or identify known *and unknown* operatives ..., some of whom may be in the United States or in communication with U.S. persons." App. at 6 (emphasis added). The government would use such information, in part, "to detect and prevent terrorist acts against the United States and U.S. interests." Ex. A. at 3. The government posits that bulk telephonic metadata is necessary to its investigations because it is impossible to know where in the data the connections to international terrorist organizations will be found. Id. at 8-9. The government notes also that "[a]nalysts know that the terrorists' communications are located somewhere" in the metadata produced under this authority, but cannot know where until the data is aggregated and then accessed by their analytic tools under limited and controlled queries. Id. As the government stated in its 2006 Memorandum of Law, "[a]ll of the metadata collected is thus relevant, because the success of this investigative tool depends on bulk collection." Mem. of Law at 15, Docket No. BR 06-05.

The government depends on this bulk collection because if production of the information were to wait until the specific identifier connected to an international terrorist group were determined, most of the historical connections (the entire purpose of this authorization) would be lost. See Ex. A. at 7-12. The analysis of past connections is only possible "if the Government has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related." Mem. of Law at 2, Docket No. BR 06-05. Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity.

The government must demonstrate "facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." 50 U.S.C. 1861(b)(2)(A). The fact that international terrorist operatives are using telephone communications, and that it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, is sufficient to meet the low statutory hurdle set out in Section 215 to

obtain a production of records. Furthermore, it is important to remember that the relevance finding is only one part of a whole protective statutory scheme. Within the whole of this particular statutory scheme, the low relevance standard is counter-balanced by significant post-production minimization procedures that must accompany such an authorization and an available mechanism for an adversarial challenge in this Court by the record holder. See supra Part III.a. Without the minimization procedures set out in detail in this Court's Primary Order, for example, no Orders for production would issue from this Court. See Primary Ord. at 4-17. Taken together, the Section 215 provisions are designed to permit the government wide latitude to seek the information it needs to meet its national security responsibilities, but only in combination with specific procedures for the protection of U.S. person information that are tailored to the production and with an opportunity for the authorization to be challenged. The Application before this Court fits comfortably within this statutory framework.

c. Legislative Re-enactment or Ratification.

As the U.S. Supreme Court has stated, "Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change." Lorillard v. Pons, 434 U.S. 575, 580 (1978) (citing cases and authorities); see also Forest Grove Sch. Dist. v. T.A., 557 U.S. 230, 239-40 (2009) (quoting Lorillard, 434 U.S. at 580). This doctrine of legislative re-enactment,

also known as the doctrine of ratification, is applicable here because Congress re-authorized Section 215 of the PATRIOT Act without change in 2011. "PATRIOT Sunsets Extension Act of 2011," Pub. L. No. 112-14, 125 Stat. 216 (May 26, 2011).[22] This doctrine applies as a presumption that guides a court in interpreting a re-enacted statute. See Lorillard, 434 U.S. at 580-81 (citing cases); NLRB v. Gullett Gin Co., 340 U.S. 361, 365-66 (1951) ("[I]t is a fair assumption that by reenacting without pertinent modification ... Congress accepted the construction ... approved by the courts."); 2B Sutherland on Statutory Construction § 49:8 and cases cited (7th ed. 2009). Admittedly, in the national security context where legal decisions are classified by the Executive Branch and, therefore, normally not widely available to Members of Congress for scrutiny, one could imagine that such a presumption would be easily overcome. However, despite the highly-classified nature of the program and this Court's orders, that is not the case here.

Prior to the May 2011 congressional votes on Section 215 re-authorization, the Executive Branch provided the Intelligence Committees of both houses of Congress with letters which contained a "Report on the National Security Agency's Bulk

---

[22] The Senate and House of Representatives voted to re-authorize Section 215 for another four years by overwhelming majorities. See http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=112&session=1&vote=00084 (indicating a 72-23 vote in the Senate); and, http://clerk.house.gov/evs/2011/roll376.xml (indicating a 250-153 vote in the House). President Obama signed the re-authorization into law on May 26, 2011.

Collection Programs for USA PATRIOT Act Reauthorization" (Report). Ex. 3 (Letter to Hon. Mike Rogers, Chairman, and Hon. C.A. Dutch Ruppersberger, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives (HPSCI), from Ronald Weich, Asst. Attorney General (Feb. 2, 2011) (HPSCI Letter); and, Letter to Hon. Dianne Feinstein, Chairman, and Hon. Saxby Chambliss, Vice Chairman, Select Committee on Intelligence, U.S. Senate (SSCI), from Ronald Weich, Asst. Attorney General (Feb. 2, 2011) (SSCI Letter)). The Report provided extensive and detailed information to the Committees regarding the nature and scope of this Court's approval of the implementation of Section 215 concerning bulk telephone metadata.[23] The Report noted that "[a]lthough these programs have been briefed to the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about th[is] ... program[] when considering reauthorization of the

[23] Specifically, the Report provided the following information: 1) the Section 215 production is a program "authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls ... but not the content of the calls ...." Ex. 3, Report at 1 (emphasis in original); 2) this Court's "orders generally require production of the business records (as described above) relating to *substantially all of the telephone calls* handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States," id. at 3 (emphasis added); 3) "Although the program[] collect[s] a large amount of information, the vast majority of that information is never reviewed by any person, because the information is not responsive to the limited queries that are authorized for intelligence purposes," id. at 1; 4) "The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the FISA Court and Congress," id.; 5) "Although there have been compliance problems in recent years, the Executive Branch has worked to resolve them, subject to oversight by the FISA Court," id.; 6) "Today, under FISA Court authorization pursuant to the 'business records' authority of the FISA (commonly referred to as 'Section 215'), the government has developed a program to close the gap" regarding a terrorist plot, id. at 2; 7) "NSA collects and analyzes large amounts of transactional data obtained from certain telecommunications service providers in the United States," id.; and, 8) that the program operates "on a very large scale." Id.

expiring PATRIOT Act provisions." Id. Report at 3. Furthermore, the government stated the following in the HPSCI and SSCI Letters: "We believe that making this document available to all Members of Congress is an effective way to inform the legislative debate about reauthorization of Section 215...." Id. HPSCI Letter at 1; SSCI Letter at 1. It is clear from the letters that the Report would be made available to *all* Members of Congress and that HPSCI, SSCI, and Executive Branch staff would also be made available to answer any questions from Members of Congress.[24] Id. HPSCI Letter at 2; SSCI Letter at 2.

In light of the importance of the national security programs that were set to expire, the Executive Branch and relevant congressional committees worked together to ensure that *each* Member of Congress knew or had the opportunity to know how

[24] It is unnecessary for the Court to inquire how many of the 535 individual Members of Congress took advantage of the opportunity to learn the facts about how the Executive Branch was implementing Section 215 under this Court's Orders. Rather, the Court looks to congressional action on the whole, not the preparatory work of individual Members in anticipation of legislation. In fact, the Court is bound to presume regularity on the part of Congress. See City of Richmond v. J.A. Croson Co., 488 U.S. 469, 500 (1989) ("The factfinding process of legislative bodies is generally entitled to a presumption of regularity and deferential review by the judiciary." (citing cases)). The ratification presumption applies here where each Member was presented with an opportunity to learn about a highly-sensitive classified program important to national security in preparation for upcoming legislative action. Furthermore, Congress as a whole may debate such legislation in secret session. See U.S. Const. art. I, Sec. 5. ("Each House may determine the Rules of its Proceedings, ... Each House shall keep a Journal of its Proceedings, and from time to time publish the same *excepting such Parts as may in their Judgment require Secrecy*; ....") (emphasis added.). In fact, according to a Congressional Research Service Report, both Houses have implemented rules for such sessions pursuant to the Constitution. See "Secret Sessions of the House and Senate: Authority, Confidentiality, and Frequency" Congressional Research Service (Mar. 15, 2013), at 1-2 (citing House Rules XVII, cl. 9; X, cl. 11; and, Senate Rules XXI; XXIX; and, XXXI). Indeed, both Houses have entered into secret session in the past decade to discuss intelligence matters. See id. at 5 (Table 1. Senate "Iraq war intelligence" (Nov. 1, 2005); Table 2. House of Representatives "Foreign Intelligence Surveillance Act and electronic surveillance" (Mar. 13, 2008)).

Section 215 was being implemented under this Court's Orders.[25] Documentation and personnel were also made available to afford each Member full knowledge of the scope of the implementation of Section 215 and of the underlying legal interpretation.

The record before this Court thus demonstrates that the factual basis for applying the re-enactment doctrine and presuming that in 2011 Congress intended to ratify Section 215 as applied by this Court is well supported. Members were informed that this Court's "orders generally require production of the business records (as described above) relating to *substantially all of the telephone calls* handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States." Ex. 3, Report at 3 (emphasis added). When Congress subsequently re-authorized Section 215 without change, except as to expiration date, that re-authorization carried with it this Court's interpretation of the statute, which permits the bulk collection of telephony metadata under the restrictions that are in place. Therefore, the passage of the PATRIOT Sunsets Extension Act

---

[25] Indeed, one year earlier when Section 215 was previously set to expire, SSCI Chairman Feinstein and Vice Chairman Bond sent a letter to every Senator inviting "each Member of the Senate" to read a very similar Report to the one provided in the 2011 Letters, and pointing out that this would "permit each Member of Congress access to information on the nature and significance of intelligence authority on which they are asked to vote." Ex. 7 ("Dear Colleague" Letter from SSCI Chairman Dianne Feinstein and Vice Chairman Christopher Bond (Feb. 23, 2010)). The next day, HPSCI Chairman Reyes sent a similar notice to each Member of the House that this information would be made available "on important intelligence collection programs made possible by these expiring authorities." Ex. 2 ("Dear Colleague" Notice from HPSCI Chairman Silvestre Reyes (Feb. 24, 2010)). This notice also indicated that the HPSCI Chairman and Chairman Conyers of the House Judiciary Committee would "make staff available to meet with any member who has questions" along with Executive Branch personnel. Id.

provides a persuasive reason for this Court to adhere to its prior interpretations of Section 215.

IV. Conclusion.

This Court is mindful that this matter comes before it at a time when unprecedented disclosures have been made about this and other highly-sensitive programs designed to obtain foreign intelligence information and carry out counter-terrorism investigations. According to NSA Director Gen. Keith Alexander, the disclosures have caused "significant and irreversible damage to our nation." Remarks at "Clear and Present Danger: Cyber-Crime; Cyber-Espionage; Cyber-Terror; and Cyber-War," Aspen, Colo. (Jul. 18, 2013). In the wake of these disclosures, whether and to what extent the government seeks to continue the program discussed in this Memorandum Opinion is a matter for the political branches of government to decide.

As discussed above, because there is no cognizable Fourth Amendment interest in a telephone company's metadata that it holds in the course of its business, the Court finds that there is no Constitutional impediment to the requested production. Finding no Constitutional issue, the Court directs its attention to the statute. The Court concludes that there are facts showing reasonable grounds to believe that the records sought are relevant to authorized investigations. This conclusion is supported not only by the plain text and structure of Section 215, but also by the statutory modifications

and framework instituted by Congress. Furthermore, the Court finds that this result is strongly supported, if not required, by the doctrine of legislative re-enactment or ratification.

For these reasons, for the reasons stated in the Primary Order appended hereto, and pursuant to 50 U.S.C. § 1861(c)(1), the Court has GRANTED the Orders requested by the government.

Because of the public interest in this matter, pursuant to FISC Rule 62(a), the undersigned FISC Judge requests that this Memorandum Opinion and the Primary Order of July 19, 2013, appended herein, be published, and directs such request to the Presiding Judge as required by the Rule.

ENTERED this 29th day of August, 2013.

Claire V Eagan

CLAIRE V. EAGAN
Judge, United States Foreign
Intelligence Surveillance Court

[redacted]

~~TOP SECRET//SI//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR 13-109

PRIMARY ORDER

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

~~TOP SECRET//SI//NOFORN~~

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

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number BR 13-80 and its predecessors. [50 U.S.C. § 1861(c)(1)]

Accordingly, and as further explained in a Memorandum Opinion to follow, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

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

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"[1] created by [redacted]

B. The Custodian of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

[1] For purposes of this Order "telephony metadata" includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer. Furthermore, this Order does not authorize the production of cell site location information (CSLI).

thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by [redacted] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [redacted]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.[2] The BR metadata shall carry unique markings such

[2] The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.[3] Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms[4] that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

---

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

[3] The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.

[4] [redacted]

but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through queries of the BR metadata to obtain contact chaining information as described in paragraph 17 of the Declaration of [redacted] attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.[5] NSA shall ensure, through

[5] For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.

adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.[6]

(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [redacted]

[6] This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[redacted]

[redacted] provided, however, that NSA's Office of General Counsel (OGC)

[redacted]

shall first determine that any selection term reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [redacted] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. The preceding sentence shall not apply to selection terms under surveillance

[redacted]

pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated [redacted] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.[9,10]

---

[9] The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the selection term is or was associated with a Foreign Power shall be specified. The automated query process described in the [redacted] Declaration limits the first hop query results to the specified time frame. Analysts conducting manual queries using that selection term shall continue to properly minimize information that may be returned within query results that fall outside of that timeframe.

[10] The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to this Orde[redacted]

(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.[11] This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns the hop-limited results from those queries to a "corporate store." The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms. The specifics of the automated query process, as described in the [redacted] Declaration, are as follows:

[redacted]

[11] This automated query process was initially approved by this Court in its November 8, 2012 Order amending docket number BR 12-178.

[12] As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms have not expired. This step does not use expired RAS-approved selection terms to create the list of "authorized query terms" (described below) regardless of whether the list of RAS-approved selection terms is up-to-date.

[redacted]

D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first

[redacted]

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.[15] NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.[16] Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch

---

[15] In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

[16] In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.[17] OGC shall provide NSD/DoJ with copies

[17] The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.

(vii) Other than the automated query process described in the [redacted] Declaration and this Order, prior to implementation of any new or modified automated query processes, such new or modified processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of NSA's application of the RAS standard, as well as NSA's implementation and operation of the automated query process. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials

authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

This authorization regarding [redacted] expires on the 11th day of October, 2013, at 5:00 p.m., Eastern Time.

Signed _____ Eastern Time
Date Time

Claire V. Eagan

CLAIRE V. EAGAN
Judge, United States Foreign
Intelligence Surveillance Court

[redacted]

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE DIRECTIVES TO YAHOO!, INC. Docket Number 105B(g): 07-01

PURSUANT TO SECTION 105B OF THE

FOREIGN INTELLIGENCE SURVEILLANCE

ACT

MEMORANDUM OPINION

Background

This case comes before the Court on the government's motion to compel compliance with directives it issued to Yahoo!, Inc. (Yahoo) pursuant to the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (PAA), which was enacted on August 5, 2007. The PAA amended the Foreign Intelligence Surveillance Act (FISA) (which, in its present form, can be found at 50 U.S.C.A. §§ 1801-1871 (West 2003, Supp. 2007 & Oct. 2007)), by creating a new framework for the collection of foreign intelligence information concerning persons reasonably believed to be outside of the United States. Under the PAA, the Attorney General and the Director of National Intelligence may authorize the acquisition of such information for periods of up to one year

pursuant to a "certification" that satisfies specific statutory criteria, and may direct third parties to assist in such acquisition. 50 U.S.C.A. §§ 1805a - 1805c.

Subsequent to the passage of the PAA, the Attorney General and the Director of National Intelligence, pursuant to 50 U.S.C.A. § 1805b(a), executed [redacted] certifications that authorized the acquisition of certain types of foreign intelligence information concerning persons reasonably believed to be outside the United States.[1] In furtherance of these acquisitions, in [redacted] 2007, the Attorney General and the Director of National Intelligence issued [redacted] directives to Yahoo. Feb. 2008 Classified Appendix at [redacted].[2] Yahoo refused to comply

[1] [redacted]

[2] Each directive states that

> [t]he Government will [redacted] pursuant to the above-referenced Certification in a mutually agreed upon format. [redacted]

(continued...)

with the directives, and on November 21, 2007, the government filed a motion asking this Court to compel Yahoo's compliance. Motion to Compel Compliance with Directives of the Director of National Intelligence and Attorney General (Motion to Compel). Yahoo responded by contending that the directives should not be enforced because they violate both the PAA and the Fourth Amendment. Yahoo also contends that the PAA violates separation of powers principles and is otherwise flawed.

Extensive briefing followed on this complicated matter of first impression. Yahoo has raised numerous statutory claims relating to the PAA, which is hardly a model of legislative clarity or precision. Yahoo's principal constitutional claim relates to the Fourth Amendment rights of its customers and other third parties, and raises complex issues relating to both standing and substantive matters. Furthermore, additional issues have arisen during the pendency of the litigation. For one thing, most of the PAA has sunset, raising the issue of whether this Court retains jurisdiction over the government's motion to compel. For another, the government filed a classified appendix with the Court in December 2007,[3] which contained the certifications and

---

[2](...continued)

[redacted] **Yahoo Inc.** . . . is hereby directed . . . to immediately provide the Government with all information, facilities, and assistance necessary to accomplish this acquisition in such a manner as will protect the secrecy of the acquisition and produce a minimum of interference with the services that **Yahoo** provides.

Feb. 2008 Classified Appendix at [redacted]

[3] This classified appendix was filed ex parte, pursuant to 50 U.S.C.A. § 1805b(k). Yahoo did not object to the ex parte filing of this initial classified appendix. Pursuant to section

(continued...)

procedures underlying the directives, but the government then inexplicably modified and added to those certifications and procedures without appropriately informing the Court or supplementing the record in this matter until ordered to do so. These changes and missteps by the government have greatly delayed the resolution of its motion, and, among other things, required this Court to order additional briefing and consider additional statutory issues, such as whether the PAA authorizes the government to amend certifications after they are issued, and whether the government can rely on directives to Yahoo that were issued prior to the amendments.[4]

For the reasons set forth below, the Court holds that it retains jurisdiction over the government's motion to compel, and that the motion is in fact meritorious. The Court also finds that the directives issued to Yahoo comply with the PAA and with the Constitution. A separate Order granting the government's motion is therefore being issued together with this Opinion.

Part I of this Opinion explains why the expiration of much of the PAA does not deprive the Court of jurisdiction over the government's motion. Part II of this Opinion rejects the statutory challenges advanced by Yahoo, and concludes that the directives in this case comply with the PAA and are still in effect pursuant to the amended certifications. Part II also rejects Yahoo's separation of powers challenge to the PAA. Part III of the Opinion holds that Yahoo

---

[3](...continued)
1805b(k), the Court subsequently allowed the government to file, ex parte, the updated, February 2008 classified appendix. Although Yahoo requested a copy of that appendix redacted to the level of the security clearance held by Yahoo's counsel, section 1805b(k) does not require, and the Court did not order, the government to provide such a document to Yahoo.

[4] The Court's February 29, 2008 Order Directing Further Briefing on the Protect America Act lays out in greater detail the circumstances that required the additional briefing.

may in fact raise the Fourth Amendment rights of its customers and other third parties, but further holds that the directives to Yahoo comply with the Fourth Amendment because they fall within the foreign intelligence exception to the warrant requirement and are reasonable.

Analysis

I. The Court Retains Jurisdiction Over the Motion to Compel Notwithstanding the Lapse of the PAA.

As originally enacted, the PAA had a "sunset" provision, under which its substantive terms would "cease to have effect 180 days after the date of the enactment" of the PAA, subject to exceptions discussed below. PAA § 6(c). On January 31, 2008, Congress extended this period to "195 days after the date of the enactment of [the original PAA]." See Pub. L. 110-182, § 1, 122 Stat. 605. Congress took no further action, and this 195-day period expired on February 16, 2008. Yahoo argues that this statutory lapse deprives this Court of jurisdiction to entertain the government's motion to compel. Yahoo's Supplemental Briefing on PAA Statutory Issues (Yahoo's Supp. Brief. on Stat. Issues) at 13-16. For the following reasons, the Court finds that it retains jurisdiction by virtue of section 6(c) of the PAA.

Section 2 of the PAA amended FISA by adopting additional provisions, codified at 50 U.S.C.A. §§ 1805a and 1805b. One of the provisions added to FISA by section 2 of the PAA states as follows:

> In the case of a failure to comply with a directive issued pursuant to subsection (e), the Attorney General may invoke the aid of the [Foreign Intelligence Surveillance Court (FISC)] to compel compliance with the directive. The court shall issue an order requiring the person to comply with the directive if it finds that the directive was issued in accordance with subsection (e) and is otherwise lawful.

PAA § 2 (codified at 50 U.S.C.A. § 1805b(g)). Unquestionably, this provision gave the Court jurisdiction over the government's motion prior to February 16, 2008.

> Section 6 of the PAA, as amended, states in relevant part:
>
> (c) SUNSET.–Except as provided in subsection (d), sections 2, 3, 4, and 5 of this Act, and the amendments made by this Act, shall cease to have effect 195 days after the date of the enactment of this Act.
>
> (d) AUTHORIZATIONS IN EFFECT.–Authorizations for the acquisition of foreign intelligence information pursuant to the amendments made by this Act, and directives issued pursuant to such authorizations, shall remain in effect until their expiration. Such acquisitions shall be governed by the applicable provisions of such amendments and shall not be deemed to constitute electronic surveillance as that term is defined in [50 U.S.C.A. § 1801(f)].

PAA § 6, as amended by Pub. L. 110-182, § 1, 122 Stat. 605 (emphasis added). Yahoo concedes that under the first sentence of § 6(d), the directives remain in effect. Yahoo's Supp. Brief. on Stat. Issues at 14. However, Yahoo contends that § 6(d) does not preserve this Court's jurisdiction over the government's motion to compel compliance with the directives it received. On the other hand, the government posits that the second sentence of § 6(d) – providing that "[s]uch acquisitions shall be governed by the applicable provisions of such amendments" – preserves the Court's jurisdiction. United States of America's Supplemental Brief on the Fourth Amendment (Govt.'s Supp. Brief on the Fourth Amend.) at 10 n.8.

The Court begins its analysis of the parties' conflicting views by examining the controlling statutory text. In the second sentence of § 6(d), the phrase "[s]uch acquisitions" plainly refers to acquisitions conducted pursuant to the "[a]uthorizations for the acquisition of foreign intelligence information pursuant to the amendments made" by the PAA, "and directives issued pursuant to such authorizations," both which "remain in effect" under the immediately

preceding sentence. The second sentence of § 6(d) provides that those acquisitions "shall be governed by the applicable provisions of such amendments." Here too, the phrase "such amendments" refers to the "amendments" in the immediately preceding sentence – i.e., the amendments made by the PAA, pursuant to which the acquisition of foreign intelligence information has been authorized. Thus, acquisitions that remain authorized under the first sentence of § 6(d) shall, by virtue of the second sentence, be governed by the "applicable" provisions of those amendments.

The relevant question under § 6(d) therefore becomes whether the provision of the PAA codified at § 1805b(g) is fairly understood to be part of those PAA amendments pursuant to which the relevant acquisitions were authorized, and which are "applicable" to those acquisitions. If so, then section 6(d) operates to maintain the applicability of § 1805b(g) with regard to the directives issued to Yahoo, thereby preserving the Court's jurisdiction to enforce those directives. The structure and logic of the amendments enacted by the PAA strongly support the conclusion that section 6(d) has this effect.

Section 2 of the PAA added to FISA all of the provisions codified at 50 U.S.C.A. §§ 1805a and 1805b in the form of a single, comprehensive amendment.[5] Section 1805b (which is titled "Additional Procedure for Authorizing Certain Acquisitions Concerning Persons Located Outside of the United States") provides a comprehensive framework for the authorization and conduct of certain acquisitions of foreign intelligence information. In addition to § 1805b(g),

---

[5] "The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after [50 U.S.C.A. § 1805] the following: [the full text of §§ 1805a and 1805b follows]." PAA § 2.

this framework includes a grant of authority to the Attorney General and the Director of National Intelligence, "[n]othwithstanding any other law," to authorize such acquisitions, subject to specified procedural and substantive requirements (i.e., § 1805b(a), (c), (d)); authority to "direct" a person, such as Yahoo, to assist in such acquisition (i.e., § 1805b(e)); immunity from civil liability for providing assistance in accordance with such a directive (i.e., § 1805b(l)); a mechanism by which a person who has received such a directive may challenge its legality before the FISC (i.e., § 1805b(h)), with an ability to appeal to the Foreign Intelligence Surveillance Court of Review (i.e., § 1805b(i)); and procedural and security requirements for judicial proceedings under § 1805b (i.e., § 1805b(j), (k)). Thus, § 1805b(g) constitutes one part of the integrated statutory framework codified by § 1805b for authorizing the acquisition of foreign intelligence information. It is therefore no stretch to regard § 1805b(g) as included within "the amendments" pursuant to which the relevant acquisitions were authorized, and as "applicable" to those acquisitions. Indeed, that is the natural construction of the terms of § 6(d) as applied to § 1805b(g).

Yahoo takes the view that § 6(d) does not preserve the efficacy of § 1805b(g) with regard to directives that had not been complied with at the time that the PAA expired. Yahoo's Supp. Brief. on Stat. Issues at 14. But as explained above, nothing in the language of § 6(d) supports this result. The phrase "[s]uch acquisitions" in the second sentence of § 6(d) plainly refers to the description, in the immediately preceding sentence, of acquisitions authorized pursuant to amendments made by the PAA. And, the preserving language in the second sentence is not

limited to acquisitions both authorized pursuant to amendments made by the PAA and actually occurring before the PAA's expiration date.

However, assuming arguendo that this statutory language might also reasonably bear the interpretation that § 1805b(g) is not preserved by § 6(d) for purposes of the directives issued to Yahoo, the Court would then have to assess which interpretation would serve the purposes envisioned by Congress.[6] Without doubt, Congress intended for the FISC to have jurisdiction over § 1805b(g) actions to compel compliance with directives prior to the expiration date for the PAA specified in § 6(c). It is equally clear that, even after that expiration date, the challenged directives "remain in effect until their expiration." § 6(d). There is no discernible reason why Congress would have chosen to dispense with the forum and process that it specifically established to compel compliance with lawfully issued directives, while providing that the directives themselves remain in effect. And the particular interpretation advanced by Yahoo yields the inexplicable outcome that recipients who have never complied with directives are now beyond the reach of § 1805b(g)'s enforcement mechanism, but recipients who were compliant as of February 16, 2008, would still be subject to it. The "illogical results of applying such an interpretation . . . argue strongly against the conclusion that Congress intended" such divergent

---

[6] See, e.g., Jones v. R.R. Donnelley & Sons Co., 541 U.S. 369, 377 (2004) (ambiguous statute interpreted in view of "the context in which it was enacted and the purposes it was designed to accomplish").

results when it enacted § 6(d). Western Air Lines, Inc. v. Board of Equalization of the State of South Dakota, 480 U.S. 123, 133 (1987).[7]

In support of its interpretation, Yahoo cites authority which concludes that the repeal of a jurisdiction-conferring statute deprives a court of jurisdiction over pending cases, in the absence of a clause in the repealing statute that preserves jurisdiction.[8] But the PAA includes a preservation clause, see § 6(d), and the issue in this case is how broadly or narrowly that clause should be construed. The authority cited by Yahoo does not shed light on that issue.

Yahoo also suggests that De La Rama S.S. Co. v. United States, 344 U.S. 386 (1953), requires that Congress employ "plain terms" to preserve jurisdiction over pending cases when the statute previously conferring jurisdiction is repealed. Yahoo's Supp. Brief. on Stat. Issues at 15. But De La Rama does not enunciate an unqualified "plain statement" requirement. Instead, in

---

[7] Yahoo cites several statements from congressional debate on the PAA that emphasize that the PAA was a temporary statute, set to expire in six months (subsequently extended by 15 days, as noted above). Yahoo's Supp. Brief. on Stat. Issues at 16 (quoting, e.g., 153 Cong. Rec. H9958-59 (daily ed. Aug. 4, 2007) (statement of Rep. Issa) ("[W]hat we're doing is passing a stopgap 6-month, I repeat, 6-month bill. This thing sunsets in 6 months."). But the statements cited by Yahoo, of which Rep. Issa's statement is illustrative, shed no light on the interpretative issue presented, which is the intended scope of §6(d)'s exception from the general sunset provision. Indeed, the statements quoted by Yahoo do not even acknowledge the existence of any exceptions to the PAA's sunset provision.

[8] Yahoo's Supp. Brief. on Stat. Issues at 15 (citing Bruner v. United States, 343 U.S. 112, 116-17 (1952); Santos v. Guam, 436 F.3d 1051, 1052 (9th Cir. 2006); United States v. Stromberg, 227 F.3d 903, 907 (5th Cir. 1955)).

the context of interpreting the general savings statute in 1 U.S.C. § 109 (2000),[9] the De La Rama Court observed:

> The Government rightly points to the difference between the repeal of statutes solely jurisdictional in their scope and the repeal of statutes which create rights and also prescribe how the rights are to be vindicated. In the latter statutes, "substantive" and "procedural" are not disparate categories; they are fused components of the expression of a policy. When the very purpose of Congress is to take away jurisdiction, of course it does not survive, even as to pending suits, unless expressly reserved . . . But where the object of Congress was to destroy rights in the future while saving those which have accrued, to strike down enforcing provisions that have special relation to the accrued right and as such are part and parcel of it, is to mutilate that right and hence to defeat rather than further the legislative purpose.

344 U.S. at 390 (emphasis added). Applying this principle, the De La Rama Court found that jurisdiction over pending cases was preserved, despite the repeal of the statute originally conferring jurisdiction. Id. at 390-91.

---

[9] This provision, which has not been amended since 1947, states:

> The repeal of any statute shall not have the effect to release or extinguish any penalty, forfeiture, or liability incurred under such statute, unless the repealing Act shall so expressly provide, and such statute shall be treated as still remaining in force for the purpose of sustaining any proper action or prosecution for the enforcement of such penalty, forfeiture, or liability. The expiration of a temporary statute shall not have the effect to release or extinguish any penalty, forfeiture, or liability incurred under such statute, unless the temporary statute shall so expressly provide, and such statute shall be treated as still remaining in force for the purpose of sustaining any proper action or prosecution for the enforcement of such penalty, forfeiture, or liability.

1 U.S.C. § 109. Because the Court finds that § 6(d), the PAA's specific savings clause, serves to preserve jurisdiction over the government's action to enforce the directives issued to Yahoo, it is not necessary to consider whether this general savings clause would support the same conclusion.

In this case, the jurisdictional, procedural, and substantive provisions of § 1805b are fairly regarded as "fused components of the expression of a policy" that Congress adopted when it enacted the PAA. To the extent De La Rama bears on this case, it counsels against the interpretation advanced by Yahoo.

For the above-described reasons, the Court finds that it retains jurisdiction over the government's motion to compel compliance with the directives issued to Yahoo, by virtue of § 6(d)'s preservation of § 1805b(g) with regard to the directives that the government seeks to enforce against Yahoo.

II. The Yahoo Directives Comply With the PAA and Can Be Enforced Without Violating the Constitutional Separation of Powers Doctrine.

A. Compelling Compliance With the Directives Under the PAA Does Not Violate Separation of Powers Principles.

Yahoo argues that the PAA is unconstitutional on separation of powers grounds because its "limitations on judicial review impose[] constitutionally impermissible restrictions on the judicial branch." Yahoo's Memorandum in Opposition to Motion to Compel (Yahoo's Mem. in Opp'n) at 21. In particular, Yahoo objects that, in proceedings under 50 U.S.C.A. § 1805c, judicial review is confined to the government's determination that its procedures are reasonably designed to ensure that acquisitions do not constitute "electronic surveillance," as defined at 50 U.S.C.A. §§ 1801(f) and 1805a, and that the FISC applies a "clear error" standard in reviewing that determination. Yahoo's Mem. in Opp'n at 21-22. Yahoo contends that these limitations are inconsistent with the scope and nature of the inquiry necessary for a court to determine, under

prior judicial decisions, whether a surveillance[10] comports with the Fourth Amendment. Id. at 21-23.

As authority for its separation of powers objection, Yahoo cites Doe v. Gonzales, 500 F. Supp. 2d 379 (S.D.N.Y. 2007), which involved First Amendment challenges to non-disclosure obligations imposed on the recipient of a national security letter (NSL) under 18 U.S.C.A. § 2709 (West 2000 & Supp. 2007). In Doe, the separation of powers concerns derived from 18 U.S.C.A. § 3511(b) (West Supp. 2007), which governs the scope and standard of review to be applied by a district court when the recipient of an NSL petitions for relief from the non-disclosure obligations. 500 F. Supp. 2d at 409, 411-13.[11] Employing one of the quintessential tenets of separation of powers jurisprudence – that "Congress cannot legislate a constitutional standard of review that contradicts or supercedes what the courts have determined to be the standard applicable under the First Amendment for that purpose," Doe, 500 F. Supp. 2d at 411 (citing Dickerson v. United States, 530 U.S. 428, 437 (2000); Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803)) – the Doe court invalidated certain aspects of § 3511(b).[12]

[redacted]

[11] The Doe court entertained facial challenges to sections 2709 and 3511 because those statutory provisions "are broadly written and certainly have the potential to suppress constitutionally protected speech." 500 F. Supp. 2d at 396.

[12] See Doe, 500 F. Supp. 2d at 405-06 (under Freedman v. Maryland, 380 U.S. 51 (1965), government must bear burden of proving need for restriction on speech); id. at 409 (§ 3511(b)(2)'s limitations on judicial review of government's certification of need for non-disclosure was "plainly at odds with First Amendment jurisprudence which requires that courts strictly construe content-based restrictions and prior restraints to ensure they are narrowly

(continued...)

Assuming arguendo that this separation of powers principle was correctly applied in Doe, it does not apply to the situation presented in this case. The limitations on judicial review legislated in § 1805c apply only to the ex parte review of the government's procedures submitted to the FISC under § 1805c(a). Here, the challenged event involves an effort by the Attorney General, under 50 U.S.C.A. § 1805b(g), to "invoke the aid of the [FISC] to compel compliance" with his directives. Under § 1805b(g), the FISC is to determine whether "the directive[s were] issued in accordance with [50 U.S.C.A. § 1805b(e)] and [are] otherwise lawful." The recipient of a directive, such as Yahoo, may raise Fourth Amendment challenges in response to a motion to compel compliance, see infra Part III.A, triggering an assessment by the FISC of whether acquisitions pursuant to the directive would violate the Fourth Amendment. The limitations on judicial review imposed on the separate, ex parte proceeding under § 1805c do not apply to the Court's analysis of Fourth Amendment issues in this case. Thus, the PAA does not intrude on the Court's "power to . . . decide what constitutional rule of law must apply" in this case. Doe, 500 F. Supp. 2d at 411.

B. Yahoo's Other Non-Fourth Amendment Objections to the PAA Are Not Persuasive.

Yahoo argues next that the PAA is "defective" or "problematic" in three other respects. Yahoo's Mem. in Opp'n at 23-24. First, it notes that 50 U.S.C.A. § 1805b(a)(1) and 50 U.S.C.A. § 1805c(b) use divergent language to describe the procedures to be adopted by the government and reviewed by the FISC, such that "it is unclear what should be submitted to, and reviewed by,

---

[12](...continued)
tailored to advance a compelling government interest").

this Court." Yahoo's Mem. in Opp'n at 23.[13] Another judge of the FISC acknowledged this ambiguity when reviewing the government's procedures under § 1805c(b). See In re DNI/AG Certifications [redacted] Memorandum Opinion and Order entered January 15, 2008 (In re DNI/AG Certifications) at 6-8. However, that judge, after applying ordinary principles of statutory construction, concluded that for the types of acquisition pertinent to this case, the statute should be understood to require that the procedures be "reasonably designed to ensure that the users of tasked facilities[14] are reasonably believed to be outside of the United States." Id. at 15. This understanding of the statutory requirement is also adopted here, for the reasons stated in In re DNI/AG Certifications.[15] Because this ambiguity can be resolved by such

---

[13] Compare § 1805b(a)(1) (requiring "reasonable procedures . . . for determining that the acquisition of foreign intelligence information . . . concerns persons reasonably believed to be located outside the United States" and providing that "such procedures will be subject to review" by the FISC under § 1805c) with § 1805c(b) (the FISC shall review for clear error "the Government's determination" that the § 1805b(a)(1) procedures "are reasonably designed to ensure that acquisitions . . . do not constitute electronic surveillance"). These procedures are separate from the "minimization procedures" required by § 1805b(a)(5).

[14] In the context of the challenged directives here, the "tasked facilities" are those [redacted] identified by the government to Yahoo for acquisition.

[15] In reaching this conclusion, Judge Kollar-Kotelly reasoned as follows:

> [T]he statute describes the subject matter of the Court's review under § 1805c using varying and ambiguous language. Section 1805b(a)(1) sets out the relevant executive branch "determination" as follows: that "there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States." § 1805b(a)(1) (emphasis added). However, § 1805c(b) states that the Court "shall assess the Government's determination under [§ 1805b(a)(1)] that those procedures are reasonably designed to ensure that acquisitions conducted pursuant to [§ 1805b] do not constitute electronic

(continued...)

interpretative analysis, there is no force to Yahoo's argument that it renders the challenged directives unlawful.

Second, Yahoo raises a separate argument that challenges the propriety of enforcing the directives while judicial review of these procedures under 50 U.S.C.A. § 1805c(b) has not been

---

[15](...continued)
surveillance." § 1805c(b) (emphasis added). One provision focuses on the location of persons implicated by the acquisitions of foreign intelligence information, while the other provision focuses on whether the acquisitions constitute electronic surveillance.

This seeming disconnect between the language of § 1805b(a)(1) and § 1805c(b) is bridged in part by the PAA's amendment to the definition of "electronic surveillance" to exclude "surveillance directed at a person reasonably believed to be located outside of the United States." § 1805a (emphasis added). Section 1805a arguably harmonizes § 1805b(a)(1) and § 1805c(b), to the extent that the acquisition of foreign intelligence information concerning persons reasonably believed to be outside of the United States (per § 1805b(a)(1)), will often, and perhaps usually, be accomplished through surveillance directed at persons reasonably believed to be outside of the United States. In that event, such surveillance will not constitute "electronic surveillance" by virtue of § 1805a. But at first glance, at least, this harmonization is imperfect. For example, an acquisition of foreign intelligence information that concerns a person outside of the United States might not necessarily be understood to involve surveillance directed at a person outside of the United States. The concepts are related and overlapping, but not necessarily co-extensive under the terms of the statute.

Despite these interpretative difficulties, it seems clear that procedures will satisfy the relevant statutory requirements if they are reasonably designed to ensure both
(1) that such acquisitions do not constitute "electronic surveillance," because they are surveillance directed at persons reasonably believed to be outside of the United States, and
(2) that the acquisitions of foreign intelligence information concern persons reasonably believed to be located outside of the United States.

In re DNI/AG Certifications at 6-8 (footnotes omitted).

completed. Yahoo's Mem. in Opp'n at 23. A brief explanation of the procedures involved in this case will be useful before addressing the merits of this argument.

This case involves multiple sets of procedures that, separately from this proceeding, have been submitted by the government to the FISC for review under § 1805c(b). The first set of procedures is implemented by the National Security Agency (NSA) and was the subject of the In re DNI/AG Certifications decision discussed above.[16] After that decision, the government submitted the second set of procedures, which applies to [redacted] acquisitions involving [redacted] the Federal Bureau of Investigation (FBI).[17] As related to this case, the NSA procedures apply to [redacted] but for accounts identified for [redacted] the FBI procedures [redacted] apply.[18] In other words, all accounts identified for acquisition are screened [redacted] If an account passes this screening and is identified for [redacted] then it is subject to [redacted] With this background, the Court returns to Yahoo's second argument.

---

[16] More precisely, there are [redacted] closely similar sets of NSA procedures, one for each of the certifications at issue in this case. These NSA procedures can be found in the Feb. 2008 Classified Appendix at [redacted]

[17] There are also [redacted] closely similar sets of FBI procedures, one for each of the [redacted] certifications at issue in this case. These FBI procedures can be found in the Feb. 2008 Classified Appendix at [redacted] They were adopted on January 31, 2008, pursuant to amendments to each of the [redacted] certifications, which may be found in the Feb. 2008 Classified Appendix at [redacted] The legal effect of these amendments is discussed later in this Opinion. See infra Part II.D.

[18] See Feb. 2008 Classified Appendix at [redacted]

Yahoo claims that it "should not be required to comply with the Directives until this Court has approved the government's procedures" under 50 U.S.C.A. § 1805c(b). Yahoo's Mem. in Opp'n at 23. With regard to the NSA procedures, this argument is mooted by the intervening In re DNI/AG Certifications decision, which found that the NSA procedures satisfy the applicable review for clear error under § 1805c(b). However, FISC review of the FBI procedures under § 1805c(b) has not been completed, although as noted above, the FBI procedures [redacted] the NSA procedures that [redacted]

With regard to the FBI procedures, the Court finds that the terms of the PAA foreclose Yahoo's suggestion that the completion of judicial review under § 1805c(b) is a prerequisite to a directive's having compulsive effect. Upon the effective date of the PAA, see § PAA 6(a), the Attorney General and the Director of National Intelligence were empowered to authorize acquisitions of foreign intelligence information under § 1805b(a), and to issue directives "[w]ith respect to an authorization of an acquisition" under § 1805b(e). The recipient of a directive is obligated to "immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition." § 1805b(e)(1) (emphasis added). In contrast, Congress envisioned that judicial review of the government's procedures under § 1805c(b) could take up to 180 days after the effective date of the PAA to complete. See § 1805c(b). Congress plainly

intended that directives could take effect before the § 1805c(b) process was completed.[19] Thus, Yahoo's second argument must also be rejected.

Third, Yahoo challenges the directives, arguing that, under section 6(c)-(d) of the PAA, it remains obligated to comply with the directives for up to one year, even though the protection of immunity provided to it by the legislation may not apply by virtue of the lapse of 50 U.S.C.A. § 1805b(l). Yahoo's Mem. in Opp'n at 24. In response, the government asserts that the immunity provision remains in effect throughout the life of the directives. Memorandum in Support of Government's Motion to Compel (Mem. in Support of Gov't Motion) at 24 n.22. For essentially the same reasons that support the Court's holding that § 1805b(g) remains in effect with regard to the directives at issue by operation of § 6(d) of the PAA, see supra Part I, the Court finds that § 6(d) also preserves the operability of the immunity provision of § 1805b(l). Not only does § 1805b(l) fit comfortably within the preserving language of § 6(d), but it would be wholly illogical for Congress to have initially afforded civil immunity to the recipients of directives, only to have it subsequently extinguished even though the obligation to comply with the directives remains in effect.[20]

---

[19] Yahoo's argument regarding the timing of judicial review under § 1805c(b) is also unpersuasive if construed as a Fourth Amendment challenge. As explained below, the Court finds that authorized acquisitions pursuant to the directives issued to Yahoo comport with the Fourth Amendment jurisprudence. See infra Part III.B-C. And, as part of the Court's assessment of compliance with the reasonableness requirement of the Fourth Amendment, the Court has reviewed the procedures in question, which seek to ensure that acquisitions will be directed at [redacted] used by persons reasonably believed to be overseas. See infra note 83 and accompanying text.

[20] Moreover, in Yahoo's case, any assistance rendered will be pursuant to this Court's

(continued...)

C. The PAA Does Not Require Certifications or Directives to Identify Each Individual Target.

Yahoo also argues that the directives do not comply with the terms of the PAA, because they require Yahoo to assist in surveillance of persons who are not known to the government at the time of the certification, but rather become known to the government after the certification is made. Yahoo's Mem. in Opp'n at 24-25. Yahoo advances this argument despite its acknowledgment that 50 U.S.C.A. § 1805b(b) expressly states that a certification "is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed." Yahoo opines that there is an implicit requirement that the government identify each person at whom the surveillance will be directed when a certification is made, and that the government can target persons identified thereafter only pursuant to a subsequent certification. Yahoo bases this argument on 50 U.S.C.A. § 1805b(a)(2), which requires the Attorney General and the Director of National Intelligence to issue a certification if they "determine, based on the information provided to them, that . . . the acquisition does not constitute electronic surveillance." Yahoo's Mem. in Opp'n at 24. Yahoo notes that 50 U.S.C.A. § 1805b(a)(1) separately requires the Attorney General and the Director of National Intelligence, before issuing a certification, to determine that "there are reasonable procedures in place for determining that the acquisition of foreign information . . . concerns

---

[20](...continued)
Order requiring compliance with the directives. And, failure to obey the Order "may be punished . . . as contempt of court." § 1805b(g). Under such circumstances, Yahoo would likely have recourse to some form of immunity, even apart from the express language of § 1805b(l). Cf. Rodriques v. Furtado, 950 F.2d 805, 814-16 (1st Cir. 1991) (qualified immunity for physician assisting in search authorized by warrant).

persons reasonably believed to be located outside the United States." Yahoo's Mem. in Opp'n at 24-25. Yahoo argues that in order for § 1805b(a)(2) to have any independent effect, this provision must require the Attorney General and the Director of National Intelligence to determine, on an individualized basis, that each person at whom surveillance will be directed is outside of the United States, such that surveillance directed at them will not constitute "electronic surveillance" by virtue of 50 U.S.C.A. § 1805a. Yahoo's Mem. in Opp'n at 25. Otherwise, the argument continues, the determination under § 1805b(a)(2) would merely (and redundantly) rely on the efficacy of the procedures, which are already the subject of the determination under § 1805b(a)(1), in ensuring that new persons at whom the surveillance is later directed are outside of the United States. Yahoo's Mem. in Opp'n at 25.

In response, the government essentially inverts Yahoo's argument by contending that, if § 1805b(a)(2) required individualized determinations by the Attorney General and the Director of National Intelligence regarding the location of each person at whom surveillance will be directed, then it would be superfluous for § 1805b(a)(1) to require procedures to ensure that the surveillance is directed at persons reasonably believed to be outside of the United States. Mem. in Support of Gov't Motion at 23.

This appears to be another occasion where the PAA is not a model of clear and concise legislative drafting. See supra notes 13-15 and accompanying text. Nonetheless, for the reasons described below, the Court concludes that the government's interpretation of § 1805b(a)(1) and (a)(2) better serves the canon of statutory construction which requires that statutes be construed in a manner that promotes a "symmetrical and coherent regulatory scheme, and fit[s], if possible,

all parts [of a statute] into an harmonious whole," such that the terms of the statute are "read in their context and with a view to their place in the overall statutory scheme." Food & Drug Admin. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000) (internal quotations and citations omitted).

Under the PAA, both the Attorney General and the Director of National Intelligence must make determinations "in the form of a written certification, under oath, [and] supported as appropriate by affidavit" of Presidentially-appointed and Senate-confirmed national security officials or the head of an agency within the intelligence community. 50 U.S.C.A. § 1805b. However, in circumstances where "immediate action by the Government is required and time does not permit the preparation of a certification, . . . the determination of the Director of National Intelligence and the Attorney General shall be reduced to a certification as soon as possible but in no event more than 72 hours after the determination is made." Id. These requirements for senior executive branch official participation are generally comparable to the involvement required by 50 U.S.C.A. § 1804, when application is made to the FISC for an order authorizing electronic surveillance.[21]

Requiring the executive branch to meet these procedural requirements every time it identifies a new person (or group of persons) at whom it intends to direct surveillance would substantially burden and very likely impede the intelligence gathering efforts authorized under

---

[21] See § 1804(a) (requiring approval of the Attorney General based upon his finding that the application satisfies applicable statutory criteria); § 1804(a)(7) (requiring certification by "the Assistant to the President for National Security Affairs" or a Presidentially-appointed, Senate-confirmed national security official).

the PAA, compared to an interpretation that permits surveillance of newly-identified persons under a previously issued certification, assuming that the other requirements for conducting surveillance are satisfied. It is true that based on Yahoo's interpretation, surveillance of a newly-identified account could commence immediately if the user of the newly-identified account also used a separate account already covered by a prior certification. But, in many instances, it will not be self-evident whether that is the case, and the analytical effort devoted to this question would constitute an additional burden on intelligence agencies.[22]

Imposing such burdens is contrary to the congressional intent of easing the procedural requirements for targeting persons reasonably believed to be outside of the United States, in order to allow intelligence agencies to pursue new overseas targets with greater expediency and effectiveness.[23] This objective is reflected in § 1805b(b)'s express statement that a certification need not "identify the specific facilities, places, premises, or property at which the acquisition of

[22] [redacted]

[23] See 153 Cong. Rec. H9954 (daily ed. Aug. 4, 2007) (statement of Rep. Smith) (PAA "adopts flexible procedures to collect foreign intelligence from foreign terrorists overseas," and "does not impose unworkable, bureaucratic requirements that would burden the intelligence community"); see also 153 Cong. Rec. S10,869 (daily ed. Aug. 3, 2007) (statement of Sen. Bond) (PAA meets "the needs that were identified . . . to clear up the backlog because there is a huge backlog," resulting from "the tremendous amount of paperwork" involved in the pre-PAA FISA process).

foreign intelligence information will be directed." In view of the evident purpose for enacting the PAA, the Court declines to find an implicit requirement that certifications specify the persons at whom surveillance will be directed. If Congress had intended a limitation of this magnitude on the flexibility it otherwise intended to confer when it passed into law the PAA, one would expect a much clearer statement of such intent.

The Court therefore concludes that certifications and directives do not have to specify the persons at whom surveillance will be directed in order to comply with the PAA. This construction of the PAA – wherein the Attorney General and the Director of National Intelligence determine that there are "reasonable procedures in place" regarding the overseas location of targeted persons under § 1805b(a)(1), the FISC reviews those procedures under § 1805c(b),[24] and intelligence agency personnel make reasonable assessments of the location of persons to be targeted in conformance with those procedures – provides a framework more conducive to the congressional purpose of enabling intelligence agencies to identify and pursue overseas targets with greater speed and efficacy.

D. The Directives Issued to Yahoo Survive the Amendment of the Government's Certifications.

As explained above, see supra notes 3-4 and accompanying text, the government purported to amend each of the [redacted] certifications relevant to this proceeding prior to the

[24] The only judicial review that is necessarily mandated under the PAA is the FISC's review of these procedures under § 1805c(b); other modes of judicial review occur only in response to contingent decisions by parties, such as the government's decision to bring the instant motion to compel under § 1805b(g). The decision of Congress to single out the § 1805b(a)(1) procedures for mandatory judicial review suggests that Congress expected these procedures to be especially important in properly implementing the PAA.

expiration of the PAA on February 16, 2008. The government contends that these amendments are effective, and that the government may use the directives that were issued to Yahoo prior to these amendments as the means for conducting acquisitions under the amended certifications. Government's Response to the Court's Order of February 29, 2008 (Govt.'s Resp. to Feb. 29 Order) at 6-12, 16-20. Yahoo, on the other hand, argues that the issuance of new directives is required to effectuate material amendments to certifications. Yahoo's Supp. Brief. on Stat. Issues at 6-12.

Now that the PAA has expired, it is by no means clear that the government could issue new directives at this time, or otherwise take additional steps to effectuate the changes it intended to implement by the amendments. See PAA § 6(c), (d). For this reason, the impact of the government's actions prior to the expiration of the PAA has assumed greater importance.

1. Certifications May Be Amended and Such Amendments Do Not Necessarily Require the Issuance of New Directives.

The PAA does not expressly address whether and how certifications may be amended, or what effect such amendments have on previously issued directives. Nevertheless, the following general principles can be gleaned from the text of the statute:

> (1) The Attorney General and the Director of National Intelligence must make a written certification in order to authorize acquisitions of foreign intelligence information under § 1805b(a).[25]

---

[25] As noted earlier, in emergency situations, the Attorney General and the Director of National Intelligence may make the determinations in support of an acquisition less formally, and then make the written certification within 72 hours. § 1805b(a). This emergency provision does not apply to this case because the authorizations in question have at all relevant times been supported by written certifications.

(2) Acquisitions may only be conducted in accordance with the applicable certification. § 1805b(d).

(3) "With respect to an authorization of an acquisition," the Attorney General and the DNI may direct a person to provide assistance in the acquisition. § 1805b(e).

These principles do not foreclose the possibility that the Attorney General and the Director of National Intelligence could amend previous certifications. Indeed, the government argues that the authority to make a certification logically implies the ability to modify a certification in response to changed circumstances, see Govt.'s Resp. to Feb. 29 Order at 8, a principle courts have recognized in other contexts.[26] The FISC's practice of entertaining motions to amend previously issued orders could be seen as illustrating a similar principle, since (as noted by the government, see Govt.'s Resp. to Feb. 29 Order at 9) FISA does not explicitly provide for the amendment of FISC orders. Yahoo, for its part, does not object to the general proposition that the government could amend certifications while the PAA was in effect. Yahoo's Supp. Brief. on Stat. Issues at 6. Accordingly, the Court concludes that, prior to the PAA's expiration, the Attorney General and the Director of National Intelligence were not categorically prohibited from amending certifications previously made under § 1805b. The more difficult issue, however, is whether an amendment to a certification required the issuance of a new (or appropriately amended) directive, or instead whether the previously issued directive was a proper and effective

---

[26] See, e.g., Belville Min. Co. v. United States, 999 F.2d 989, 997-98 (6th Cir. 1993) ("Even if an agency lacks express statutory authority to reconsider an earlier decision, an agency possesses inherent authority to reconsider administrative decisions, subject to certain limitations."); Gun South, Inc. v. Brady, 877 F.2d 858, 862-63 (11th Cir. 1989) (recognizing "an implied authority in . . . agencies to reconsider and rectify errors even though the applicable statute and regulations do not expressly provide for such reconsideration").

means to obtain assistance for acquisitions conducted in accordance with the post-amendment terms of the certification. To that issue the Court now turns.[27]

The government analogizes the relationship between certifications and directives to the relationship between primary and secondary orders issued by the FISC pursuant to 50 U.S.C.A. §§ 1804-1805. See Govt.'s Resp. to Feb. 29 Order at 9-11; see also Yahoo's Supp. Brief. on Stat. Issues at 4 (certifications are comparable in effect to court orders authorizing surveillance). In the latter context, the "order" by which the FISC "approv[es] the electronic surveillance" under 50 U.S.C.A. § 1805(a), and makes the findings, directions, and specifications necessary under § 1805(a) and (c), is customarily referred to as the "primary order." If the surveillance requires assistance from a third party under § 1805(c)(2)(B)-(D), the FISC also issues a separate "secondary order," which the government serves on the third party.[28] The secondary order does

---

[27] The government also argues that, on these questions of statutory interpretation, the Attorney General's and the Director of National Intelligence's decisions are entitled to deference under Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984). See Govt.'s Resp. to Feb. 29 Order at 8. Indeed, the government argues that an especially heightened version of Chevron deference is due in this case because the statute to be interpreted concerns foreign affairs. See id. (citing Springfield Indus. Corp. v. United States, 842 F.2d 1284, 1286 (Fed. Cir. 1988), and Population Inst. v. McPherson, 797 F.2d 1062, 1070 (D.C. Cir. 1986)). However, the government does not explain why, in this case, the conditions for according any level of Chevron deference are satisfied. See, e.g., Gonzales v. Oregon, 546 U.S. 243, 255-56 (2006) (Chevron deference applies only when agency interpretation of statute was promulgated pursuant to statutorily-delegated "authority to the agency . . . to make rules carrying the force of law") (internal quotations omitted). In any case, because the Court finds that the amended certifications are valid and may be effectuated through the previously-issued directives without according Chevron deference, it is unnecessary to decide whether Chevron applies to this case.

[28] Congress used nearly identical language to describe third-party assistance under a PAA directive and under a FISC order to assist in an electronic surveillance authorized under § 1805.

(continued...)

not include all of the required elements of the primary order, but instead is limited to information that the third party needs to know in order to provide the required assistance.

The government correctly observes that the FISC has granted motions by the government to amend a previously issued primary order – for example, to approve modified minimization procedures. Govt.'s Resp. to Feb. 29 Order at 9-11 (discussing, e.g., [redacted] In such cases, the FISC has sometimes amended primary orders without amending secondary orders, see, e.g., [redacted] based on the implicit understanding that the efficacy of previously issued secondary orders was not undermined by the amendment. As a general rule, the FISC has issued new or amended secondary orders to a third party who is already subject to an extant secondary order in the same docket only when the primary order has been amended in a way that changes the nature or scope of the assistance to be provided – for example, when the amendment authorizes surveillance of a new facility that was beyond the scope of the original orders. See, e.g., [redacted]

---

[28](...continued)
See § 1805b(e)(1)-(3) (PAA directive); § 1805(b)(2)(B)-(D) (FISC order).

The government's analogy to this motions practice is on point. Under § 1805, the primary order issued by the FISC is the means of authorization required by the statute in non-emergency situations,[29] and must include certain findings and specifications identified in § 1805(a) and (c). Surveillance authorized by the FISC under § 1805 must be conducted in accordance with the primary order.[30] Under § 1805b(a), the certification made by the Attorney General and the Director of National Intelligence is the means of authorization required by the PAA in non-emergency situations, and must include certain determinations identified in § 1805b(a)(1)-(5). Acquisitions authorized by the Attorney General and the Director of National Intelligence under § 1805b must be conducted in accordance with the applicable certification (except under an emergency authorization, after which a written certification must be made within 72 hours under § 1805b(a)).[31] On the other hand, secondary orders issued by the FISC are the means of compelling third parties to assist in an authorized surveillance pursuant to §

---

[29] In cases of emergency, the Attorney General may authorize electronic surveillance, provided that a FISC order approving such surveillance is obtained "as soon as practicable, but not more than 72 hours" after the Attorney General's authorization. § 1805(f).

[30] See § 1805(c)(2)(A) (order "shall direct . . . that the minimization procedures be followed"); FISC Rule 10(c) (government must immediately inform FISC when "any authority granted by the Court has been implemented in a manner that did not comply with the Court's authorization"). The FISC's rules are available online at: <http://www.uscourts.gov/rules/FISC_Final_Rules_Feb_2006.pdf>.

[31] The government suggests that there is also a non-emergency exception to this requirement, i.e., when the government has modified procedures that were originally adopted under § 1805b(a)(1) in response to an adverse ruling by the FISC under § 1805c(c), it may follow the new procedures even if that results in an acquisition that is not in accordance with the certification. See Govt.'s Resp. to Feb. 29 Order at 17. But those hypothetical circumstances are not presented here and the Court expresses no opinion on whether the government's view is correct.

1805(b)(2)(B)-(D). They are only issued when the FISC, in a primary order, has made the findings and specifications necessary to authorize the surveillance under § 1805(a) and (c). So, too, the Attorney General and the Director of National Intelligence issue directives, pursuant to § 1805b(e), to compel third parties to assist in acquisitions that have been authorized under § 1805b(a). Directives may be issued only after the Attorney General and the Director of National Intelligence have made the determinations specified in § 1805b(a)(1)-(5) and, except in emergencies, those determinations must take the form of a written certification under § 1805b(a).

Given these similarities, the practice under § 1805 of amending primary orders, while implicitly relying on the continued efficacy of secondary orders issued prior to the amendment, supports the conclusion that a certification may be amended without undermining the effectiveness of a previously issued directive, at least in some circumstances. Yahoo acknowledges that this is the case for "purely ministerial amendments." Yahoo's Supp. Brief. on Stat. Issues at 9 n.10. However, Yahoo contends that amendments that modify minimization procedures under § 1805b(a)(5) or "targeting" procedures under § 1805b(a)(1) are "material," Yahoo's Supp. Brief. on Stat. Issues at 8-9, and that materially amended certifications are tantamount to new certifications that require new directives. Id. at 9-10. But Yahoo's approach is difficult to reconcile with the motions practice described above. For example, the FISC has granted motions to amend primary orders to approve modified minimization procedures (and those amendments are fairly regarded as material). But those amendments were not understood to vitiate secondary orders that the FISC had issued prior to the amendment.

Moreover, as a matter of logic, it does not follow that any material amendment to the terms of an authorization – whether they are embodied in a FISC order under § 1805 or an executive branch certification under § 1805b(a) – necessarily vitiates the obligation of third parties to assist in the authorized surveillance. The fact of an amendment does not imply that the pre-amendment authorization had been invalid. For example, an amendment that modifies minimization procedures may replace one legally sufficient set of procedures with another. In such a case, there is an equally valid authorization for surveillance, both before and after the amendment, and the amendment has no effect whatsoever on the nature of the assistance to be provided by a third party. Therefore, there is no reason why the amendment should necessarily extinguish a third party's obligation to assist the surveillance, whether that obligation arises under a FISC secondary order or a directive under § 1805b(e). And if that obligation is not extinguished, then there is no reason to require the government to issue and serve a new directive (or an amendment to the prior directive), provided that the prior directive still appropriately describes the obligations of the third party to assist surveillance conducted pursuant to the amended authorization.[32]

2. Requiring the Government to Issue New Directives Would Not Appreciably Enhance Judicial Review of Directives Under the PAA.

The Court has carefully considered whether, and to what extent, the issuance of new directives whenever a certification is materially amended would further the purposes of the PAA

---

[32] In addition, Yahoo's approach involves practical disadvantages. As the government correctly contends, see Govt.'s Resp. to Feb. 29 Order at 23, the issuance of multiple directives would involve at least a marginal increase in the risk of improper disclosure of classified information.

by facilitating judicial review of directives in the context of government actions to enforce compliance under § 1805b(g), or challenges to directives brought by recipients under § 1805b(h). As explained below, the Court concludes that any such furtherance of congressional intent based on Yahoo's position is illusory, and accordingly provides no basis for construing the PAA to require the issuance of new or amended directives in all cases where there has been a material amendment of a certification.

Yahoo makes three arguments regarding the availability of meaningful judicial review of directives. Yahoo's Supp. Brief. on Stat. Issues at 9-12. Although only the third of these arguments directly pertains to the impact of amendments, all three are considered below.

The first argument contends that the PAA violates the Fourth Amendment because there is no mechanism for judicial review of the reasonableness of surveillance under § 1805b, unless and until a directive is challenged under § 1805b(h) or becomes the subject of an enforcement action under § 1805b(g). Yahoo's Supp. Brief. on Stat. Issues at 9-12. But the directives at issue in this case are the subject of such an enforcement action, and for reasons discussed below, see infra Part III.B-C, the Court determines that the requirements of the Fourth Amendment are satisfied.

Secondly, Yahoo notes that the recipient of a directive does not have access to the underlying certification and procedures. Yahoo's Supp. Brief. on Stat. Issues at 10.[33] Yahoo

---

[33] The directives issued to Yahoo recite, in language tracking the terms of § 1805b(a)(1)-(5), that the Attorney General and the Director of National Intelligence have made the determinations required for them to authorize acquisition under the PAA, but Yahoo is correct that they do not provide any information about the basis for these determinations. See Feb. 2008 (continued...)

objects that this lack of access puts the recipient in the position of deciding whether to comply with the directive, and whether to seek judicial review, without the information necessary for a full assessment of the directive's lawfulness. Id. at 10-11. The Court appreciates this conundrum, but it has nothing to do with whether a second, post-amendment directive needs to be issued. Even in circumstances where there is no amendment, the recipient will not necessarily have access to the underlying certification and procedures. Indeed, the PAA specifically provides that, even when a recipient is a party to litigation involving the lawfulness of a directive under § 1805b(g) or (h), "the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information." § 1805b(k). With this provision, Congress created an opportunity for the government to provide a full record to the Court, without disclosing sensitive information to non-governmental parties.[34] Under other provisions of FISA, it is the norm for federal district courts

---

[33](...continued)
Classified Appendix at [redacted]

[34] On February 20, 2008, the government filed a motion for leave, pursuant to § 1805b(k), to submit ex parte for the Court's in camera review a classified appendix containing a complete set of the certifications, amendments, and procedures pertaining to the directives to Yahoo. See Response to Ex Parte Order to Government and Motion for Leave to File Classified Appendix for the Court's Ex Parte and In Camera Review, filed Feb. 20, 2008. As referenced above, see supra note 3, Yahoo filed a motion for disclosure of that submission, as well as of the Memorandum Opinion and Order in In re DNI/AG Certifications. See Motion for Disclosure of Filings, filed Feb. 20, 2008. On February 28, 2008, the Court granted the government's motion and denied Yahoo's motion. See Order entered on Feb. 28, 2008. Under the circumstances of this case, the Court has been able to assess the lawfulness of the directives without the benefit of a more fully informed adversarial process.

to conduct an ex parte in camera review in assessing the basis for a prior authorization of surveillance.[35]

If the recipient of a directive is not entitled to information about the basis for the underlying authorization, it follows logically that a rule requiring that any material amendment to a certification be supported by the issuance of new directives would not appreciably enhance the recipient's ability to litigate the lawfulness of a directive. Service of a new directive might put the recipient on notice that a certification has been amended, but it would not inform the recipient of the nature of the amendment. Thus, from the perspective of judicial review, the recipient would scarcely be better-equipped to contest the lawfulness of the underlying authorization by virtue of having received a second, post-amendment directive.

---

[35] For example, under 50 U.S.C.A. § 1806(f), federal district courts have jurisdiction over challenges to the lawfulness of electronic surveillance conducted pursuant to FISC orders issued under § 1805. In such cases, the district court

> shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary proceeding would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.

§ 1806(f). After the filing of such an affidavit, materials may be disclosed to the aggrieved person "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." Id. "In practice, the government has filed an affidavit from the Attorney General in every case in which a defendant has sought to suppress FISA evidence," David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 28:7 (2007), and "no court has ever ordered the disclosure to a defendant or the public of a FISA application or order." Id. § 29:3. Moreover, courts have found that such ex parte proceedings do not violate the constitutional rights of criminal defendants seeking to suppress the evidentiary use of FISA information. See, e.g., United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982); United States v. Nicholson, 955 F. Supp. 588, 592 (E.D. Va. 1997).

Yahoo's third argument is that permitting the amendment of certifications without issuing new directives complicates judicial review by potentially presenting the FISC with a "moving target." Yahoo's Supp. Brief. on Stat. Issues at 11-12. It is true in this matter that the "target" has been displaced, and that the Court was only belatedly made aware of this fact. See supra notes 3-4 and accompanying text. And, the government now acknowledges:

> While litigation is pending before this Court regarding the legality of directives under the Protect America Act, the Government has an obligation to alert this Court to any material changes made to an authorization, an accompanying certification, or the procedures the Government uses in the course of its acquisition of foreign intelligence information. The Government's obligations to keep the Court informed of changes that may inform its analysis are amplified where as here the materials at issue are filed ex parte.

Govt.'s Resp. to Feb. 29 Order at 21. The Court agrees with this assessment, subject to the modification that, because they are so central to the case, the Court should be apprised immediately of any change to an authorization, certification, or set of procedures that pertains to a directive that is the subject of either (1) pending litigation under § 1805b(g) or (h); or (2) a FISC order compelling compliance with such directive. The Order accompanying this Opinion therefore directs the government to notify the Court forthwith of any such changes pertaining to the directives issued to Yahoo.[36]

With these corrective measures in place, the "moving target" concern becomes manageable from the perspective of judicial review. Moreover, the alternative of requiring the government to issue new directives after a certification has been amended would not necessarily

---

[36] In issuing this requirement, the Court expresses no opinion on whether or to what extent the government now has the authority to make such changes, given the expiration of the PAA.

simplify judicial review. Rather, the pending litigation regarding the lawfulness of the prior, superseded directives would presumably be mooted, therefore requiring the institution of a new challenge to the lawfulness of the new directives. This is hardly a desirable result from the Court's perspective.

For these reasons, the Court concludes that the efficacy of judicial review would not be enhanced by requiring the government to issue new directives following a material amendment to a certification.

3. The Particular Amendments in Question Do Not Require New Directives.

Based on the foregoing analysis, see supra Part II.D.1-2, the Court concludes, as a general matter,[37] that the amendment of a certification does not require the issuance of a new (or amended) directive to replace a previously issued directive when the following conditions are present:

> (1) The directive, when issued (i.e., pre-amendment), was supported by a valid authorization;
>
> (2) After the amendment, a valid (albeit modified) authorization remains in effect; and
>
> (3) The previously issued directive accurately describes the obligations of the recipient regarding the assistance of acquisitions pursuant to the amended authorization.

The Court now applies these criteria to the amendments at issue in this case.

Prior to any amendments, the [redacted] certifications at issue contained each of the determinations specified in § 1805b(a)(1)-(5), and otherwise conformed with the requirements of

---

[37] With respect to amendments to procedures adopted under § 1805b(a)(1), the impact of the statutory timetable for submission to, and review by, the FISC under § 1805c(a) and (b) merits a separate evaluation. See infra Part II.D.4.

the PAA. See Feb. 2008 Classified Appendix at [redacted] Moreover, each of the [redacted] Yahoo directives corresponded with its underlying certification, both in duration and in the nature of the information and assistance to be provided.[38] Therefore, as to all of the amendments, the first of the three above-stated conditions is satisfied.

The first amendment in question pertained only to Certification [redacted] This amendment modified the applicable minimization procedures to permit the [redacted] See Feb. 2008 Classified Appendix at 119-33. Pursuant to § 1801b(a)(5), the Attorney General and the Director of National Intelligence determined that these modified minimization procedures satisfy the definition of "minimization procedures" under 50 U.S.C.A. § 1801(h). See Feb. 2008 Classified Appendix at 116. Accordingly, after this amendment, a valid (albeit modified) authorization was still in effect, so the second of the conditions is also present as to the first amendment. In addition, this amendment entirely concerned the government's handling of information once

[38] Compare [redacted] Each directive states that it encompasses information [redacted] The directives provide a more detailed description of the information sought from Yahoo than the certifications do, but the information described by the directives does not extend beyond the authorization in each certification to obtain "foreign intelligence information from or with the assistance of communications service providers . . . who have access to communications, [redacted]

acquired, and had no bearing on the nature of Yahoo's assistance in acquiring the information in the first place. Therefore, the directive still appropriately described Yahoo's post-amendment obligations, and accordingly the third condition as to the first amendment was also satisfied.

As described above, see supra notes 17-18 and accompanying text, the government also amended all [redacted] certifications to adopt additional procedures under § 1801b(a)(1) for the acquisition of [redacted] by the FBI. See Feb. 2008 Classified Appendix at [redacted] These amendments also approved, under § 1801b(a)(5), the minimization procedures to be followed by the FBI, the CIA, and the NSA under the amended certifications.[39] Pursuant to § 1801b(a)(1) and (5), the Attorney General and the Director of National Intelligence made the required determinations with regard to each of these procedures. See Feb. 2008 Classified Appendix at [redacted] Accordingly, after these amendments, valid (albeit modified) authorizations were still in effect under all [redacted] certifications, and therefore the second of the above-stated conditions is present. As to the third condition, these amendments pertained to the government's internal processes for identifying accounts for [redacted] acquisition, and to the government's handling of information once acquired. Neither type of amendment altered the nature of the assistance to be rendered by Yahoo.[40] Therefore, each directive still appropriately

---

[39] The minimization procedures for [redacted]

[40] Yahoo has submitted a sworn statement indicating that, prior to serving the directives on Yahoo, representatives of the government "indicated that, at the outset, it only would expect (continued...)

described Yahoo's obligations pursuant to these amended authorizations, so the third above-stated condition is satisfied.

Accordingly, the Court finds that all three conditions are satisfied as to each of the amendments in this case. However, amendments to procedures under § 1805b(a)(1) also require consideration of the potential impact of the statutory timetable for the government to submit, and the FISC to review, such procedures under § 1805c(a) and (b). The Court's analysis of that issue follows.

4. The Timetables for Submission and Review of Procedures Under § 1805c(a) and (b) Do Not Foreclose the Government from Amending Procedures Under § 1805b(a)(1).

Section § 1805b(a)(1) requires "reasonable procedures . . . for determining that the acquisition of foreign intelligence information . . . concerns persons reasonably believed to be located outside of the United States," and these procedures are "subject to review of the [FISC] pursuant to" section 1805c. § 1805b(a)(1). The Attorney General was required to submit such procedures to the FISC "[n]o later than 120 days after the effective date" of the PAA. § 1805c(a). The FISC was required to complete its review of those procedures by "[n]o later than 180 days after the effective date" of the PAA. § 1805c(b). The statute expressly provides that those procedures "shall be updated and submitted to the Court on an annual basis." § 1805c(a).

---

[10](...continued)

[redacted]

Presumably, the purpose of these annual submissions is for the Court to review the updated procedures under the standards provided by § 1805c(b) and (c), although no timetable for such Court review is statutorily provided.[41]

The 120-day and 180-day timetables were followed with regard to the original [redacted] sets of procedures adopted under § 1805b(a)(1). See In re DNI/AG Certifications. The PAA does not expressly provide for the submission and review of procedures after these 120-day and 180-day intervals, but before an annual submission would become due. The government advances a construction of these provisions under which the 120-day and 180-day intervals would apply to the procedures initially adopted by the government, but would not preclude the government from adopting and submitting new or revised procedures at any time thereafter. Govt.'s Resp. to Feb. 29 Order at 23-28. The Court agrees that this construction is in accord with the purpose and structure of the PAA, because the alternative construction, under which the government could not submit new or revised procedures after 120 days, except as part of an "annual" update, would produce anomalous results.

Under the terms of § 1805b(a), the Attorney General and the Director of National Intelligence were empowered to authorize acquisitions while the PAA was in effect. To do so, they were required to make determinations, including a determination that the procedures adopted under § 1805b(a)(1) "will be subject to review of the [FISC] pursuant to [§ 1805c]." §

---

[41] However, when one takes into account that the PAA was originally enacted for a term of only 180 days (later extended to 195 days), see § 6(c), and that authorizations may be authorized "for periods up to one year," see § 1805b(a), the purpose of requiring submissions "on an annual basis" is less clear.

1805b(a)(1). If the government could not submit procedures to the FISC for review after 120 days, then any authorizations after that time would necessarily have to rely on previously submitted procedures. But there is no apparent reason why Congress would have desired to prohibit the government from revising procedures, or adopting new ones, as warranted by new authorizations, or for that matter, other changed circumstances.[42] For example, previously submitted procedures might not be as well-suited for new authorizations, which could involve new classes of targets or new means of acquisition. Indeed, previously submitted procedures might not satisfy the requirements of § 1805b(a)(1) at all, when transplanted to the circumstances of a new authorization. In such a case, the inability to adopt new or revised procedures would prevent the Attorney General and the Director of National Intelligence from making the determination that is required by § 1805b(a)(1) in order to authorize otherwise valid acquisitions of foreign intelligence information.

Yahoo, for its part, contends that the timing of the government's submission of procedures must not have the effect of avoiding judicial review under § 1805c. Yahoo's Supp. Brief. on Stat. Issues at 12-13. Indeed, judicial review of the procedures relevant to this case under § 1805c has not been avoided. FISC review under § 1805c of the § 1805b(a)(1) procedures adopted by the original, pre-amendment certifications has been completed. See In re DNI/AG Certifications. On the other hand, judicial review of the § 1805b(a)(1) procedures

---

[42] Indeed, Congress perceived a need to examine § 1805b(a)(1) procedures periodically, as evidenced by the requirement to update them annually under § 1805c(a). It would be inexplicable for Congress to have required annual review and updating, but to have prohibited such efforts on a more frequent basis when circumstances so required.

adopted by the amended certifications has not been completed; however, the 180-day timetable for completion of the FISC review established by § 1805c(b) is properly subject to the same construction as the 120-day timetable for government submission of procedures established by § 1805c(a), i.e., that the 180-day timetable applies to the procedures initially submitted by the government. It is only natural to construe these parallel provisions in a similar matter. Thus, the Court concludes that the 180-day timetable applies to the completion of FISC review of procedures initially submitted by the government, and that the FISC may and should review procedures subsequently submitted by the government, even if such review cannot be completed within 180 days of the effective date of the PAA.

Moreover, the Court finds that, by virtue of § 6(d) of the PAA, the judicial review provisions of § 1805c remain operative with regard to the § 1805b(a)(1) procedures adopted under the amended certifications. The amendments adopting new § 1805b(a)(1) procedures were made on January 31, 2008, see Feb. 2008 Classified Appendix at [redacted] while the PAA was still in effect. Those amendments modified authorizations under the PAA. Despite the subsequent lapse of the PAA, those authorizations "remain in effect until their expiration," and acquisitions made thereunder "shall be governed by the applicable provisions of . . . amendments" enacted by the PAA. PAA § 6(d).[43] The judicial review provisions of § 1805c were enacted by § 3 of the PAA and, by their terms, those provisions are "applicable" to the acquisitions conducted pursuant to the procedures in question. Thus, the Court finds that these procedures remain subject to judicial review under § 1805c.

---

[43] A more thorough analysis of § 6(d) is provided above. See supra Part I.

For these reasons, the Court concludes that the government's amendments to the § 1805b(a)(1) procedures do not conflict with the judicial review provisions of § 1805c.

Accordingly, based on the analysis set out in this Part of the Opinion (Part II), the Court finds that (1) the directives issued to Yahoo comply with the PAA and – subject to the Court's analysis of Fourth Amendment issues, see infra Part III – remain in effect pursuant to the amended certifications; and (2) enforcement of the directives in this proceeding does not violate separation of powers principles.

III. The Directives to Yahoo Comply with the Fourth Amendment.

A. Yahoo's Fourth Amendment Arguments Are Properly Before the Court.

Having disposed of most of Yahoo's arguments, the Court now turns to whether Yahoo can raise its claim that the directives at issue violate the Fourth Amendment rights of third parties.

In its memorandum in opposition to the government's motion to compel, Yahoo argued that implementation of the directives would violate the Fourth Amendment rights of United States citizens whose communications would be intercepted. The government filed a reply that not only responded to Yahoo's Fourth Amendment arguments on the merits, but also disputed Yahoo's right to raise them, since Yahoo was not claiming that its own Fourth Amendment rights would be violated if it complied with the directives. The Court then ordered further briefing on the issue of whether Yahoo's Fourth Amendment arguments were properly before the Court. For the reasons set forth below, the Court agrees with Yahoo that it can challenge the directives as violative of the Fourth Amendment rights of third parties.

The Court starts its analysis of this issue with three basic propositions. First, Yahoo's attempt to assert the Fourth Amendment rights of others as a defense to the government's motion to compel does not raise any Article III standing concerns. See Warth v. Seldin, 422 U.S. 490, 500 n.12 (1975) (a litigant's attempt to assert the rights of third parties defensively, as a bar to judgment against him, does not raise any Article III standing problem). Second, prudential standing rules frequently (though not always) prevent litigants from asserting the rights of third parties. See Kowalski v. Tesmer, 543 U.S. 125, 129 (2004) (a party generally must assert its own legal rights and interests, and cannot base its claim for relief on the legal rights or interests of third parties, but also noting exceptions to this rule); Warth, 422 U.S. at 500 n.12 (litigants who assert the rights of third parties defensively are also subject to prudential standing rules). Third, prudential limitations on standing do not apply where Congress has spoken and conferred standing to seek relief or raise defenses on the basis of the legal rights and interests of third parties. See Raines v. Byrd, 521 U.S. 811, 820 n.3 (1997); Warth, 422 U.S. at 501; Alderman v. United States, 394 U.S. 165, 174-75 (1969) (a Fourth Amendment case discussed further below). As to this third proposition, the Court concludes that Congress has indeed spoken here, and that Yahoo therefore may assert the Fourth Amendment rights of third parties as a defense to the government's motion to compel.

The Court's analysis begins with the specific language of 50 U.S.C.A. § 1805b(g), which provides in pertinent part: "In the case of a failure to comply with a directive . . . , [t]he court shall issue an order requiring the person to comply with the directive if it finds that the directive

was issued in accordance with subsection (e) and is otherwise lawful." Id. (emphasis added),[44] The plain reading of this language leads the Court to the conclusion that a government directive to Yahoo that violates the Fourth Amendment is not "otherwise lawful," regardless of whose Fourth Amendment rights are being violated.[45]

Moreover, in the context of a statute that authorizes the government to acquire the contents of communications to and from United States persons[46] without their knowledge or consent, the protections provided by the Fourth Amendment are critically important. See, e.g., United States v. United States District Court, 407 U.S. 297 (1972); Katz v. United States, 389 U.S. 347 (1967). In this context especially, the expansive language that Congress used to

---

[44] Cf. 50 U.S.C.A. § 1805b(h)(2), which is a similar provision that would have applied if Yahoo had affirmatively filed a petition challenging the directive. Subsection (h)(2) provides, in pertinent part, that "[a] judge considering a petition to modify or set aside a directive may grant such petition only if the judge finds that such directive does not meet the requirements of this section or is otherwise unlawful." (emphasis added).

[45] Indeed, the government implicitly acknowledged as much in its opening motion to compel, where, prior to any filing by Yahoo, the government argued that the directives in question were "otherwise lawful" precisely because they comported with any Fourth Amendments rights of third parties. Motion to Compel at 3-7.

[46] Yahoo's arguments focus on the Fourth Amendment rights of United States citizens. The government, however, focuses on "United States persons," of whom United States citizens are a subset. Govt.'s Supp. Brief on the Fourth Amend. at 1, n.1. This Court agrees with the government's assertion that, "in general, the Fourth Amendment rights of non-citizen U.S. persons are substantially coextensive with the rights of U.S. citizens." Id. The phrase "United States person" is a term of art in the intelligence community that is defined in similar but not identical terms in FISA, 50 U.S.C.A. § 1801(i); Exec. Order No. 12,333, 3 C.F.R. 200 (1982), reprinted as amended in 50 U.S.C. § 401 (2000 & Supp. V 2005) (E.O. 12333); and the Department of Defense Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, DoD 5240.1-R (1982), Appendix A, definition 25. This Court will use the phrase "United States person" in referring to those persons who enjoy the protections of the Fourth Amendment.

describe the Court's inquiry is difficult to reconcile with an intent to exclude the central question of whether compliance with a challenged directive would transgress the Fourth Amendment rights of United States persons whose communications would be acquired.[47]

Despite the broad and unqualified nature of the statutory language (and notwithstanding what the government stated in its initial filing, see supra note 45), in subsequent filings the government is now urging the Court to conclude that Congress intended for the term "otherwise lawful" to preclude challenges to the legality of its directives based on the Fourth Amendment rights of third parties. See Mem. in Support of Gov't Motion at 5-7; Reply to Yahoo Inc.'s Sur-Reply. The government relies primarily on Supreme Court caselaw as support for its current position, in which the Court held that litigants could not raise the Fourth Amendment claims of others. The government also asserts that allowing Yahoo to raise the Fourth Amendment rights of others would lead to adjudication of those rights without sufficient concrete factual context.[48]

---

[47] The scant legislative history on the statutory provision at issue does not undermine its plain meaning. In the House, one proponent of the bill simply noted without further elaboration that, "[w]ith this new legislation . . . [t]he Court may also issue orders to assist the Government in obtaining compliance with lawful directives to provide assistance under the bill, and review challenges to the legality of such directives." See 153 Cong. Rec. H9965 (daily ed. Aug. 4, 2007) (statement of Rep. Wilson). In the Senate, one opponent of the bill charged that "[i]n effect, the only role for the court under this bill is as an enforcement agent – it is to rubberstamp the Attorney General's decisions and use its authority to order telephone companies to comply. The court would be stripped of its authority to serve as a check and to protect the privacy of people within the United States." See 153 Cong. Rec. S10,867 (daily ed. Aug. 3, 2007) (statement of Sen. Leahy). However, the remarks by an opponent of the legislation carry little weight. See United States v. Andrade, 135 F.3d 104, 108 (1st Cir. 1998).

[48] The government cites South Dakota v. Opperman, 428 U.S. 364, 375 (1976) for this proposition, where the Supreme Court stated that, "as in all Fourth Amendment cases, we are obliged to look to all the facts and circumstances of this case." This Court is obviously obliged

(continued...)

However, these arguments do not persuade the Court to adopt the strained reading of the statutory language advocated by the government.

The Court will assume, arguendo, that there is some validity to the government's argument that allowing Yahoo to assert the Fourth Amendment rights of third parties could be problematic because of inadequate factual context. But this is the type of prudential standing consideration that can be outweighed by countervailing considerations even in the absence of congressional action. See Kowalski v. Tesmer, 543 U.S. 125, 129-30 (2004) (discussing circumstances in which third parties may be granted standing to assert the rights of others). Here, however, Congress has spoken, and nothing absurd or outlandish will result from adhering to the natural meaning of its words. See generally Akio Kawashima v. Gonzales, 503 F.3d 997, 1000 (9th Cir. 2007) (plain meaning of statute controls absent an absurd or unreasonable result). The reality is that third parties whose communications are acquired pursuant to the government's directives will generally not be in a position to vindicate their own Fourth Amendment rights. It is unlikely that they will receive notice that the government is seeking or has already acquired their communications under the PAA unless the acquisitions are going to be used against them in an official proceeding within the United States, see 50 U.S.C.A. § 1805b(e)(1); 50 U.S.C.A. § 1806, and such proceedings will probably be rare given the foreign intelligence nature of the acquisitions and the fact that such acquisitions must concern persons reasonably believed to be outside the United States. See 50 U.S.C.A. § 1805b(a). Thus, allowing the recipient of a

---

[48](...continued)
to adhere to the directives of the Supreme Court, and will do so by examining all the facts and circumstances of this case, as reflected in the record before it, in rendering its decision.

directive such as Yahoo to contest its constitutionality under the Fourth Amendment will generally be the only possible means to protect the Fourth Amendment rights of third parties, albeit on a relatively undeveloped factual record in some situations. Although Congress could have chosen a different path, the one reflected in the wording of the statute is far from absurd, and gives no cause to stray from the plain meaning of what Congress said.

Furthermore, giving the "otherwise lawful" language its plain and obvious meaning is consistent with the Supreme Court precedent cited by the government concerning the assertion of Fourth Amendment rights. The government cites several cases, including Alderman v. United States, 394 U.S. 165 (1969), Rakas v. Illinois, 439 U.S. 128 (1978), and Minnesota v. Carter, 525 U.S. 83 (1998), in which the Supreme Court rejected attempts by criminal defendants to suppress evidence allegedly obtained in violation of others' Fourth Amendment rights. The government also cites a civil case, California Bankers Association v. Shultz, 416 U.S. 21 (1974), in which the Court stated that a bank could not challenge a provision of the Bank Secrecy Act on the grounds that the provision violated the Fourth Amendment rights of bank customers. None of these cases, however, support the government's position.

In California Bankers, a bank, a bankers association, and individual bank customers challenged the Bank Secrecy Act of 1970, Pub.L. 91-508, 84 Stat. 1114, on Fourth Amendment grounds. In rejecting a challenge to the domestic reporting requirements of the Act and its implementing regulations, the Court held that the requirements did not violate the banks' own Fourth Amendment rights. California Bankers, 416 U.S. at 66. The Court also held that the depositor plaintiffs lacked standing to challenge the regulations, since they had failed to allege

any transactions that would necessitate the filing of a report. Id. at 68. The Court then made the following statement without further explanation: "Nor do we think that the California Bankers Association or the Security National Bank can vicariously assert such Fourth Amendment claims on behalf of bank customers in general." Id. at 69.

Although the unexplained nature of this last statement makes it difficult to know what the Court's rationale was for making it, one important point to note for purposes of this case is that there is no suggestion in the Supreme Court's opinion that the Bank Secrecy Act contained any language that even arguably conferred standing on a bank to assert the Fourth Amendment rights of its depositors. Thus, at most, California Bankers stands for the proposition that the banks in that case lacked prudential standing to assert the Fourth Amendment rights of their customers, in the absence of a congressional enactment affirmatively authorizing the banks to do so. See Haitian Refugee Center v. Gracey, 809 F.2d 794, 808-10 (D.C. Cir. 1987) (analyzing California Bankers as falling within the prudential standing rule that the plaintiff generally must assert his own legal rights and interests, while also noting that Congress may expressly confer third party standing so long as Article III is satisfied).[49] In the instant case, unlike California Bankers, Congress has enacted a provision that does appear to permit Yahoo to rely on the Fourth Amendment rights of others as a defense to a motion to compel.

---

[49] It is also possible that California Bankers was decided on a narrower ground entirely, i.e., that the plaintiff banks had failed to show that they had business with depositors whose transactions would require the filing of reports. See National Cottonseed Products Association, 825 F.2d 482, 491 n.11 (D.C. Cir. 1987) ("the Solicitor General's brief in California Bankers, however, suggested that depositors affected by the regulation in question were not so common as to make their business with the plaintiff banks predictable").

Turning now to the criminal cases cited by the government, in Alderman, the defendants were convicted prior to becoming aware that allegedly illegal electronic surveillance had been conducted. Alderman, 394 U.S. at 167. On appeal, they demanded a retrial if any of the evidence used to convict them was obtained in violation of the Fourth Amendment, regardless of whose Fourth Amendment rights had been violated. Id. at 171. The Court rejected that demand, and instead "adhere[d] . . . to the general rule that Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted." Id. at 174. The Court noted, however, that special circumstances that might justify expanded standing were not present. Id. And the Court specifically stated that "[o]f course, Congress or state legislatures may extend the exclusionary rule and provide that illegally seized evidence is inadmissible against anyone for any purpose." Id. at 175 (emphasis added).

As Alderman demonstrates, it is perfectly consistent for the Supreme Court to hold that, in the absence of congressional action, Fourth Amendment rights (at least in the criminal suppression context) are "personal rights" that may not be asserted vicariously, while also envisioning that Congress might calibrate a different balance and confer expanded authority for third-party Fourth Amendment challenges as a matter of legislative prerogative. Thus, Alderman provides no support for a strained reading of the "otherwise lawful" legislative language.

In Rakas, the Supreme Court reaffirmed the holding of Alderman that (at least in the criminal suppression context) Fourth Amendment rights are personal rights that cannot be vicariously asserted. Rakas, 439 U.S. at 133-34. The Rakas Court also determined that it served no useful analytical purpose to consider this principle as a matter of "standing." Thus, what had

been analyzed as "standing" in Alderman and other earlier cases was now to be considered a substantive Fourth Amendment question, so that the suppression analysis would "forthrightly focus[] on the extent of a particular defendant's rights under the Fourth Amendment." Rakas, 439 U.S. at 139.

This shift in analytical framework for criminal suppression motions does not support the government's position that Yahoo is barred from arguing that the directives to it are unlawful because they violate the Fourth Amendment rights of third parties. As the Court itself explained, its shift in Rakas from the rubric of "standing" to a pure "Fourth Amendment" analysis was not intended to affect the outcome of any cases. Id.[50] Furthermore, Rakas did not address a federal statute which affirmatively confers to a party the ability to assert another's Fourth Amendment rights, and nothing in Rakas undermined the statement in Alderman that Congress could "of course" confer what at the time was characterized as "standing" through legislative enactment.

---

[50] In this regard, the Court noted that "[r]igorous application of the principle that the rights secured by this Amendment are personal, in the place of a notion of 'standing,' will produce no additional situations in which evidence must be excluded. The inquiry under either approach is the same." Rakas, 439 U.S. at 139 (emphasis added); see also Rawlings v. Kentucky, 448 U.S. 98, 106 (1980).

As this Court understands Rakas, the Supreme Court's "standing" analysis in Alderman and in other earlier cases, and the substantive analysis in Rakas itself, make clear that what had been called Fourth Amendment "standing" principles, properly applied, inexorably lead to the conclusion that a defendant in a criminal case seeking to suppress probative evidence on Fourth Amendment grounds could only assert his own Fourth Amendment rights, and not the Fourth Amendment rights of others. See Rakas, 439 U.S. at 132-39. It therefore made sense, in future cases, for courts to dispense with the "standing" nomenclature and proceed directly to the question of whether the defendant could make out a violation of his own Fourth Amendment rights. Rakas, 439 U.S. at 139. But as the Supreme Court made clear, no substantive change in the law was intended.

Thus, nothing in Rakas requires this Court to read the "otherwise lawful" language in the manner suggested by the government.

Finally, the government cites Minnesota v. Carter, 525 U.S. 83 (1998), a criminal suppression case in which the Supreme Court held that the Fourth Amendment rights of two criminal defendants were not violated by a police officer who looked through a drawn window blind into an apartment they were using to package cocaine. Id. at 85. There, the Supreme Court chastised the state courts in that case for using the discarded rubric of "standing,"[51] and reiterated that a criminal defendant seeking suppression had to demonstrate a violation of his own Fourth Amendment rights. Id. at 87-88. In analyzing whether the defendants' own Fourth Amendment rights had been violated, the Court stated that the text of the Fourth Amendment (which protects persons against unreasonable searches of "their" persons and houses) "indicates that the Fourth Amendment is a personal right that must be invoked by an individual." Id. at 88. Further, the Court noted, under Rakas, the individual seeking protection had to have a legitimate expectation of privacy in the invaded place. Id. The Court concluded that the defendants in that case had no legitimate expectation of privacy in the apartment they were temporarily using to package cocaine, and accordingly could not successfully challenge the seizure of the drugs. Id. at 89-91.

Like Rakas, nothing in Carter suggests that this Court should read the congressional enactment at issue in a manner contrary to its most natural meaning. Rather, Carter merely

---

[51] The Carter Court stated that the shift in Rakas from standing to substantive Fourth Amendment law was "central" to the Court's analysis in Rakas. 525 U.S. at 88. This Court does not think, however, that this characterization of the analytical shift in Rakas undermines this Court's interpretation of Rakas, as set forth above.

follows and applies Rakas, which precludes the assertion of another's rights in the absence of a federal statute authorizing one defendant to assert another defendant's Fourth Amendment rights. The language in those cases concerning the "personal" nature of Fourth Amendment rights echoes similar language in Alderman, but, as already noted, Alderman saw no inconsistency between such language and a congressional enactment that would extend the reach of the exclusionary rule. Furthermore, unlike the defendants in Carter, Yahoo is not "claim[ing] the protection of the Fourth Amendment," id. at 88; rather, Yahoo is claiming the protection of a federal statute that entitles it not to comply with an unlawful directive. Nothing in the text of the Fourth Amendment affirmatively precludes Congress from extending such protection to Yahoo, and Carter is not to the contrary.

Finally, none of the courts of appeals cases cited by the government are apposite. In Ellwest Stereo Theatres, Inc. v. Wenner, 681 F.2d 1243, 1248 (9th Cir. 1982) (alternative holding), a movie arcade was deemed to lack standing to assert the Fourth Amendment rights of its customers. But, again, there is no hint of any legislative enactment that would have conferred upon the arcade the ability to make the challenge. Similarly, cases cited by the government that were brought under 42 U.S.C. § 1983 (2000) or Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics, 403 U.S. 388 (1971),[52] do not support the government's argument

[52] See Hollingsworth v. Hill, 110 F.3d 733, 738 (10th Cir. 1997) (Fourth Amendment rights are personal rights which may not be vicariously asserted in section 1983 action); Pleasant v. Lovell, 974 F.2d 1222, 1228-29 (10th Cir. 1992) ("To recover for a Fourth Amendment violation in a Bivens action plaintiffs must show that they personally had an expectation of privacy in the illegally seized items or the place illegally searched"); Shamaeizadeh v. Cunigan, 338 F.3d 535, 544-45 (6th Cir. 2003) (plaintiff in section 1983 action had no standing to assert (continued...)

in regards to the particular statute at issue here. The Court's holding in this situation is based on the specific wording of 50 U.S.C.A. § 1805b(g). And this language compels the conclusion that 50 U.S.C.A. § 1805b(g) confers upon Yahoo the ability to raise the Fourth Amendment rights of third parties whose rights would allegedly be violated if Yahoo complied with the directives issued to it, and that Yahoo's arguments on this score are properly before the Court.

B. Yahoo's Fourth Amendment Arguments Fail on the Merits.

The Court turns next to the merits of the Fourth Amendment issue. The crux of Yahoo's Fourth Amendment argument is that the directives are unconstitutional because they allow the government to acquire the communications of United States citizens without first obtaining a particularized warrant from a disinterested judicial officer. See Yahoo's Mem. in Opp'n at 10-13. Yahoo contends that there is no foreign intelligence exception to the Fourth Amendment's warrant requirement, but that even if such an exception exists, it does not apply to the directives issued to it under the PAA. See id. at 13-17. Finally, Yahoo asserts that even if a Fourth Amendment warrant is not required, the directives are still "unreasonable" under the Fourth Amendment. See id. at 19-21.

The government counters by arguing that there is a foreign intelligence exception to the Warrant Clause of the Fourth Amendment, and that the exception is applicable to this case. See Mem. in Support of Gov't Motion at 8-12. The government further contends that surveillance of

---

[52](...continued)
the Fourth Amendment rights of his lessees); but see Heartland Academy Community Church v. Waddle, 427 F.3d 525, 532 (8th Cir. 2005) (cited by Yahoo) (statement that Fourth Amendment rights are personal and may not be vicariously asserted was made in context of exclusionary rule in criminal cases and is not controlling in a case under 42 U.S.C. § 1983).

United States persons pursuant to the challenged directives is reasonable under the Fourth Amendment because the directives advance a compelling government interest; are limited in scope and duration; and are accompanied by substantial safeguards specifically designed to protect the privacy of United States persons. See id. at 13-20.

The Court begins its analysis with the text of the Fourth Amendment, which provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Yahoo contends[53] (and the government has not argued to the contrary) that "the people" protected by the Fourth Amendment include not only United States citizens located within the country's boundaries, but also United States citizens abroad as well, see United States v. Bin Laden, 126 F. Supp. 2d 264, 270-71 (S.D.N.Y. 2000) (Fourth Amendment protects American citizen in Kenya), and that the directives may sweep up communications to which a United States citizen is a party.[54] The Court assumes that United States citizens (and other United States persons, as well) will have a reasonable expectation of privacy in at least some of these communications, even though the scope of Fourth Amendment protection for email communications is not a settled

---

[53] See Yahoo's Mem. in Opp'n at 6-8.

[54] In particular, Yahoo notes that its accounts with United States citizens reasonably believed to be abroad could be targeted directly under the directives, see Yahoo's Mem. in Opp'n at 7-8, and, in addition, communications between non-targeted United States citizens (who may be within the boundaries of the United States) and targeted accounts would also be acquired. See id. at 9.

legal issue.[55] Indeed, the government has conceded the point.[56] Nevertheless, for the reasons stated below, the Court agrees with the government that the Fourth Amendment's Warrant Clause is inapplicable, because the government's acquisition of foreign intelligence under the PAA falls within the foreign intelligence exception to the warrant requirement.[57]

1. There is a Foreign Intelligence Exception to the Warrant Clause and It is Applicable Here.

Yahoo correctly notes that the Supreme Court has never recognized a foreign intelligence exception to the warrant requirement. See United States v. United States District Court, 407 U.S. 297, 321-22 & n.20 (1972) (expressing no view as to whether warrantless electronic surveillance may be constitutional with respect to foreign powers or their agents, even as the Court held that there is no exception to the Fourth Amendment's warrant requirement for electronic surveillance conducted to protect national security against purely domestic threats). Nevertheless, the Court

---

[55] See David S. Kris & J. Douglas Wilson, National Security Investigations & Prosecutions at § 7:28.

[56] See Govt.'s Supp. Brief on the Fourth Amend. at 2 ("U.S. Persons Abroad and U.S. Persons Communicating with Foreign Intelligence Targets Have a Reasonable Expectation of Privacy in the Content of Certain Communications Acquired Pursuant to the Directives") (emphasis in original); id. at 4 ("[redacted] with respect to electronic communications of U.S. persons while [redacted], the Government does not contest that the acquisition contemplated by the directives would implicate the reasonable expectation of privacy of U.S. persons").

[57] This conclusion does not end the Court's Fourth Amendment inquiry, as the warrantless searches must also be "reasonable" upon consideration of all pertinent factors. See In re Sealed Case, 310 F.3d 717 (FISCR 2002) (discussed below); United States v. Bin Laden, 126 F. Supp. 2d at 277-82, 284-86 (conducting bifurcated Fourth Amendment inquiry into (1) whether the foreign intelligence exception to the warrant requirement was satisfied; and (2) whether the warrantless electronic surveillance at issue was reasonable). The Court resolves the reasonableness inquiry in the government's favor in Part III.B.2 of this Opinion.

is not without appellate guidance on this issue. In addition to being bound by decisions of the Supreme Court, the FISC must also adhere to decisions issued by the Foreign Intelligence Surveillance Court of Review (FISCR), the relationship of the FISC and the FISCR being akin to that of a federal district court and its circuit court of appeals. See, e.g., 50 U.S.C.A. § 1803(a) & (b); 50 U.S.C.A. § 1805b(i); cf. Springer v. Wal-Mart Associates' Group Health Plan, 908 F.2d 897, 900 n.1 (11th Cir. 1990) (district court bound by court of appeals precedent in its circuit). The FISCR has issued only one decision during its existence, but that decision bears directly on the existence of a foreign intelligence exception to the warrant requirement.

In In re Sealed Case, 310 F.3d 717 (FISCR 2002), the FISCR considered the constitutionality of electronic surveillance applications under FISA, as amended in 2001 by the USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001), but prior to enactment of the PAA. Under the individualized application procedure that was before the FISCR, the government submits an application for "electronic surveillance," as defined in 50 U.S.C.A. § 1801(f), to a FISC judge either prior to initiating surveillance or, under emergency procedures, shortly after such initiation. In order to approve such surveillance, the FISC judge must make a number of findings, including a probable cause finding that the target of the surveillance is a "foreign power" or an "agent of a foreign power," as defined in 50 U.S.C.A. § 1801(a) & (b). Furthermore, a high ranking executive branch official must certify, among other things, that "a significant purpose" of the surveillance is to obtain "foreign intelligence information," as defined in 50 U.S.C.A. § 1801(e). See generally 50 U.S.C.A. §§ 1801, 1803-1805.

The FISCR held that the pre-PAA version of FISA was constitutional under the Fourth Amendment "because the surveillances it authorizes are reasonable." 310 F.3d at 746. In so holding, the FISCR expressly declined to decide whether an electronic surveillance order issued by a FISC judge constituted a "warrant" under the Fourth Amendment. In re Sealed Case, 310 F.3d at 741-42 ("a FISA order may not be a 'warrant' contemplated by the Fourth Amendment . . . We do not decide the issue"); id. at 744 ("assuming *arguendo* that FISA orders are not Fourth Amendment warrants, the question becomes, are the searches constitutionally reasonable"). But if the Warrant Clause of the Fourth Amendment had been deemed applicable, it would have been necessary for the FISCR to decide whether a FISC electronic surveillance order under 50 U.S.C.A. § 1805 constituted a "warrant" under the Fourth Amendment. The FISCR did not feel compelled to decide that issue because it concluded that the President has inherent authority to conduct warrantless searches to obtain foreign intelligence information, so long as those searches are "reasonable" under the Fourth Amendment, noting:

> The *Truong* court,[58] as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. . . . We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power. The question before us is the reverse, does FISA amplify the President's power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable.

---

[58] United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

In re Sealed Case, 310 F.3d at 742 (emphasis added). Thus, it is this Court's view that binding precedent requires recognition of a foreign intelligence exception to the Fourth Amendment's warrant requirement.

The Court turns next to the contours of the exception. Caselaw indicates that two criteria must be satisfied in order for the foreign intelligence exception to the warrant requirement to apply. The first criterion, naturally, is that the government's actual purpose, or a sufficient portion thereof (and there is some dispute as to what degree is sufficient), be the acquisition of foreign intelligence. Second, a sufficiently authoritative official must find probable cause to believe that the target of the search or electronic surveillance is a foreign power or its agent. See United States v. Truong Dinh Hung, 629 F.2d at 915-16 (laying out criteria for the exception);[59] United States v. Bin Laden, 126 F. Supp. 2d at 277 (same); see also United States v. United States District Court, 407 U.S. at 321-22 (expressing no view on "the issues which may be

[59] In re Sealed Case was extremely critical of Truong's assessment that obtaining foreign intelligence must be the government's primary purpose in order to qualify for this exception from the warrant requirement. See infra pp. 61-62. However, there is nothing in In re Sealed Case that undermines or is otherwise inconsistent with the two criteria set forth in Truong and Bin Laden and applied herein. Certainly there is no suggestion in In re Sealed Case that there are additional criteria that need to be met before a court may conclude that the warrant exception is applicable and that a reasonableness analysis must therefore be undertaken. Furthermore, neither Yahoo nor the government has argued that there are some other, additional criteria that need be met for the foreign intelligence exception to apply.

involved with respect to activities of foreign powers or their agents") (emphasis added).[60] The Court therefore focuses on whether these two criteria are satisfied in this case.

As to the first criterion, Yahoo cites Truong and United States v. Butenko, 494 F.2d 593 (3d Cir. 1974), for the proposition that any foreign intelligence exception to the warrant requirement can only apply where the "primary" (or even exclusive) purpose of the search is for foreign intelligence purposes. See Yahoo's Mem. in Opp'n at 16. If those cases were followed on this point, then the first criterion would not be satisfied here, because the Attorney General and the Director of National Intelligence are required by the PAA to certify, and have certified, only that a "significant" purpose of the acquisition is to acquire foreign intelligence information.

Relying, once again, on the controlling authority of In re Sealed Case, this Court rejects the proposition that the foreign intelligence exception to the warrant requirement is only applicable if the primary or exclusive purpose of an acquisition is to acquire foreign intelligence information. In fact, under the FISCR opinion, a "significant purpose" to obtain foreign intelligence information is sufficient.

In In re Sealed Case, the FISCR focused on the meaning and constitutionality of 50 U.S.C.A. § 1804(a)(7), which was amended by Congress in section 218 of the USA Patriot Act (115 Stat. at 291) to require an executive branch certification that a "significant purpose" of an

---

[60]In the context of this case, where the acquisitions are targeted against persons reasonably believed to be abroad, and in light of United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), which indicates that foreigners abroad generally have no Fourth Amendment rights, the probable cause finding presumably need not be made as to targeted non-United States persons. Indeed, Yahoo "does not dispute that the Fourth Amendment does not apply to non-U.S. persons located outside the United States." Yahoo's Mem. in Opp'n at 6 n.7.

electronic surveillance is to obtain foreign intelligence information. The FISCR construed this "significant purpose" amendment, together with a related amendment,[61] as "clearly disapprov[ing] the primary purpose test." In re Sealed Case, 310 F.3d at 734. The FISCR further noted that "as a matter of straightforward logic, if a FISA application can be granted even if 'foreign intelligence' is only a significant – not a primary – purpose, another purpose can be primary." Id.[62]

The FISCR then held that the "significant purpose" test in section 1804 comports with the Fourth Amendment. Id. at 736-46. As noted above, this holding rested in part on the foreign intelligence exception to the warrant clause. Thus, the FISCR necessarily concluded that an electronic surveillance that had a "significant purpose" of obtaining foreign intelligence information, qualified under this exception. Moreover, in conducting its Fourth Amendment analysis, the FISCR extensively criticized the conclusion in Truong, 629 F.2d at 908 -- "the case that set forth the primary purpose test as constitutionally required" -- as "rest[ing] on a false

---

[61] See 50 U.S.C.A. § 1806(k) (authorizing consultation and coordination for specified purposes between law enforcement officers and officers conducting electronic surveillance to acquire foreign intelligence information, and stating that such activities shall not preclude the "significant purpose" certification under section 1804), which was added by section 504 of the USA Patriot Act, 115 Stat. at 364.

[62] The FISCR added, however, based on FISA's legislative history, that the primary objective of an electronic surveillance application could not be criminal prosecution for ordinary crimes that are unrelated to foreign intelligence crimes such as sabotage or international terrorism. In re Sealed Case, 310 F.3d at 735-36. Furthermore, based again on legislative history, the FISCR held that a significant foreign intelligence purpose had to exist apart from any criminal prosecutive purpose, including criminal prosecution for foreign intelligence crimes. Id. at 735.

premise," and drawing a line that "was inherently unstable, unrealistic, and confusing." In re Sealed Case, 310 F.3d at 742-43 (emphasis in original).

The FISCR having seemingly concluded that an electronic surveillance can fall within the foreign intelligence exception to the warrant requirement even if it merely has as a "significant purpose" the collection of foreign intelligence information, this Court rejects the proposition that the exception is inapplicable to acquisitions under the PAA because the pertinent officials are required to certify (and have certified in this case) merely that a "significant purpose" of an acquisition is to obtain foreign intelligence information.

That brings the Court to the question of whether the acquisitions at issue satisfy the second prong of the foreign intelligence exception to the warrant requirement, which, as set forth above, would require a probable cause finding by an appropriate official that a United States person targeted for acquisition is a foreign power or an agent of a foreign power. Yahoo contends that this condition is not satisfied, because the PAA in fact authorizes surveillance directed at U.S. citizens abroad, whether or not they are agents of any foreign power.

Yahoo's description of the PAA is correct. See 50 U.S.C.A. § 1805b. However, the government counters Yahoo's argument by citing the original certifications, each of which provides that "[a]ny time NSA seeks to acquire foreign intelligence information against a U.S. person abroad in the above-referenced matter, NSA must first obtain Attorney General authorization, using the procedures under Executive Order 12333, section 2.5." Feb. 2008 Classified Appendix at [redacted] The government maintains that this language requires the Attorney General to find probable cause that any U.S. person targeted under the certifications is a

foreign power or an agent of a foreign power. See Mem. in Support of Gov't Motion at 12 n.10 & 15-16.

As noted above, the government subsequently filed amended certifications, which the Court has concluded encompass the directives issued to Yahoo. The amended certifications provide that "[a]ny time the acquisition of foreign intelligence information against a U.S. person abroad is sought pursuant to the above-referenced certification, Attorney General authorization, pursuant to the procedures under Executive Order 12333, section 2.5, must first be obtained." Feb. 2008 Classified Appendix at [redacted] Although the language in both the original and amended certifications is similar, the original certifications specify that it is "NSA" that must obtain the authorization from the Attorney General. The amendment was made presumably because the original certifications envisioned that the acquisitions would be accomplished by the NSA, while under the amended certifications the FBI also plays a role in securing some acquisitions. In any event, it seems reasonably clear that, under both the original and amended certifications, Attorney General authorization is required for all acquisitions targeting U.S. persons abroad, pursuant to "the procedures" under section 2.5 of E.O. 12333.[63]

The Court agrees with the government that the language in the certifications concerning the applicability of the section 2.5 procedures is of significant importance. The issue before this Court is not what the PAA might authorize in the abstract; rather, the issue is the lawfulness of

---

[63] Of course, there may be cases in which there is significant doubt or lack of clarity about whether the target is a United States person or not. However, the Court assumes that the government will follow the section 2.5 procedures whenever it is reasonable to believe that the target is a United States person.

the particular directives issued to Yahoo. The scope of each directive issued to Yahoo is determined and limited by the applicable certification. See 50 U.S.C.A. § 1805b(d) (an acquisition of foreign intelligence information under section 1805b may only be conducted in accordance with the certification by the DNI and AG, or in accordance with their oral instructions if time does not permit a certification). The Court therefore turns to the requirement in the certifications for Attorney General authorization pursuant to the section 2.5 procedures.

Section 2.5 of E.O. 12333 is a delegation to the Attorney General from the President to approve the use of certain techniques for intelligence collection purposes, "provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power." E.O. 12333, § 2.5.[64] As for "the procedures" under section 2.5 referenced in the certifications, the government's memorandum in support of its motion to compel identifies the Department of Defense Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, DoD 5240.1-R (1982) (DoD Procedures), as the applicable procedures.

---

[64] Within the four corners of the Executive Order, section 2.5 specifically applies to the use for intelligence collection purposes "of any technique for which a warrant would be required if undertaken for law enforcement purposes." However, there is nothing in the certification language that incorporates this limitation. Rather, the fair import of the certification language is that Attorney General authorization is required for all acquisitions undertaken pursuant to these certifications that target a United States person abroad, and that the existing procedures for Attorney General authorization under section 2.5 shall be followed with regard to all such acquisitions.

Although the certifications could describe in clearer terms what is intended by their reference to "the procedures," the Court accepts the government's representation as to what is being referenced. The DoD Procedures by their terms apply to the NSA, which is a DoD intelligence component, see DoD Procedures, Appendix A, definition 8(a), and, as discussed below, individual procedures contained therein require Attorney General approval of proposed DoD intelligence activities in a manner consistent with section 2.5 of E.O. 12333. Furthermore, even under the amended certifications providing authority to the FBI [redacted] Exhibit F of those amended certifications envisions FBI reliance on [redacted] Feb. 2008 Classified Appendix at [redacted] Thus, the DoD Procedures are central to the Court's analysis.

In its memorandum in support of its motion to compel (filed prior to the submission of the amended certifications), the government cites specifically to Procedure 5, Part 2.C, which envisions, as a general rule,[65] that DoD intelligence components cannot direct "electronic

[65] There is a temporary emergency exception set forth in the procedures, but it is not relevant here. The language of both the original and amended certifications specifically require that Attorney General authorization must "first" be obtained "[a]ny time" (i.e., every time) acquisition of foreign intelligence information against a United States person abroad is sought under a certification. For purposes of acquisitions under the certifications and directives at issue here, this language in the certifications overrides the exception language in the procedures. Also, although Procedure 5, Part 2 by its terms does not require Attorney General approval where the United States person target has no reasonable expectation of privacy, under the language of the certifications Attorney General approval is always required for acquisitions pursuant to the certifications when United States persons abroad are targeted.