IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA
(Pittsburgh Division)

ELLIOTT SCHUCHARDT, individually and d/b/a the Schuchardt Law Firm, Plaintiff, v. BARACK H. OBAMA, President of the United States, *et al*., Defendants.	)	Case No. 2:14-cv-0705-CB

DEFENDANTS' MOTION TO DISMISS
PLAINTIFF'S SECOND AMENDED COMPLAINT

Pursuant to Rule 12 of the Federal Rules of Civil Procedure, Defendants Barack H. Obama, President of the United States; James. R. Clapper, Director of National Intelligence; Admiral Michael S. Rogers, Director of the National Security Agency; and James B. Comey, Director of the Federal Bureau of Investigation; all in their official capacities, respectfully move the Court to dismiss Plaintiff's Second Amended Complaint (ECF No. 19). The Second Amended Complaint should be dismissed under Fed. R. Civ. P. 12(b)(1) for lack of subject-matter jurisdiction, and under Fed. R. Civ. P. 12(b)(6) for failure to state a claim upon which relief can be granted.

The reasons for Defendants' Motion to Dismiss are set forth in the accompanying Brief in Support of Defendants' Motion to Dismiss Plaintiff's Second Amended Complaint. A proposed order is filed herewith.

Dated: December 11, 2014

Respectfully submitted,

JOYCE R. BRANDA
Acting Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel

/s/ Marcia Berman
MARCIA BERMAN
Senior Trial Counsel
RODNEY PATTON
Trial Attorney
JULIA A. BERMAN
Trial Attorney
U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7132
Washington, D.C. 20001
Phone: (202) 514-2205
Fax: (202) 616-8470
Email: Marcia.berman@usdoj.gov

Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA
(Pittsburgh Division)

ELLIOTT SCHUCHARDT, individually and d/b/a the Schuchardt Law Firm, Plaintiff, v. BARACK H. OBAMA, President of the United States, *et al*., Defendants.	)	Case No. 2:14-cv-0705-CB

[PROPOSED] ORDER

AND NOW, having considered Defendants' Motion to Dismiss Plaintiff's Second Amended Complaint and any response and reply thereto, it is hereby ORDERED that the motion is GRANTED and Plaintiff's Second Amended Complaint is DISMISSED.

So ORDERED this _____ day of _____, 2015.

_____
HON. CATHY BISSOON
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA
(Pittsburgh Division)

ELLIOTT SCHUCHARDT, individually and d/b/a the Schuchardt Law Firm, Plaintiff, v. BARACK H. OBAMA, President of the United States, *et al.*, Defendants.	Case No. 2:14-cv-0705-CB

BRIEF IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS PLAINTIFF'S SECOND AMENDED COMPLAINT

Dated: December 11, 2014

JOYCE R. BRANDA
Acting Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
RODNEY PATTON
Trial Attorney
JULIA A. BERMAN
Trial Attorney

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7132
Washington, D.C. 20001
Phone: (202) 514-2205
Email:marcia.berman@usdoj.gov

Counsel for Defendants

TABLE OF CONTENTS

PAGE

TABLE AUTHORITIES ii

INTRODUCTION 1

ARGUMENT 1

I. THE SECOND AMENDED COMPLAINT FAILS TO ESTABLISH PLAINTIFF'S STANDING 1

II. PLAINTIFF'S FIRST AMENDMENT CLAIM SHOULD BE DISMISSED 6

A. Good-Faith Investigatory Conduct Not Intended to Deter or Punish Protected Speech or Association Does Not Violate the First Amendment 6

B. Plaintiff's First Amendment Claim Must Also Be Dismissed for Failure to Allege a Direct and Substantial Burden on his Freedom of Speech or Association 9

CONCLUSION 13

TABLE OF AUTHORITIES

CASES **PAGE(S)**

ACLU v. Barr,
952 F.2d 457 (D.C. Cir. 1991) 6, 7

ACLU v. Clapper,
959 F. Supp. 2d 724 (S.D.N.Y. 2013) ..... passim

Ashcraft v. Iqbal,
556 U.S. 662 (2009) ..... passim

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007) 2, 11

Clapper v. Amnesty Int'l USA,
133 S. Ct. 1138 (2013) 5, 12, 13

In re Directives,
551 F.3d 1004 (FISC Ct. Rev. 2008) 8

Fighting Finest, Inc. v. Bratton,
95 F.3d 224 (2d Cir. 1996) 10

Gordon v. Warren Consol. Bd. of Educ.,
706 F.2d 778 (6th Cir. 1983) 6, 7

Gross v. Taylor,
1997 WL 535872 (E.D. Pa. Aug. 5, 1997) 12

Haig v. Agee,
453 U.S. 280 (1981) 8

Hayes v. Wal-Mart Stores, Inc.,
725 F.3d 349 (3d Cir. 2013) 5

Holder v. Humanitarian Law Project,
561 U.S. 1 (2010) 8

Hollingsworth v. Perry,
133 S. Ct. 2652 (2013) 3

Jewel v. NSA,
673 F.3d 902 (9th Cir. 2011) 3, 4

Jewel v. NSA,
2010 WL 235075 (N.D. Cal. Jan. 21, 2010) 3

Kerchner v. Obama,
612 F.3d 204 (3d Cir. 2010) 6

Laird v. Tatum,
408 U.S. 1 (1972) 6, 11, 12

Lance v. Coffman,
549 U.S. 437 (2007) 3

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 3, 4, 13

Lyng v. UAW,
485 U.S. 360 (1988) 10

McNair v. Synapse Group, Inc.,
672 F.3d 213 (3d Cir. 2012) 5

Paton v. La Prade,
524 F.2d 862 (3d Cir. 1975) 12

Philadelphia Yearly Meeting of Religious Soc'y of Friends v. Tate,
519 F.2d 1335 (3d Cir. 1975) 12

Redd v. City of Enterprise,
140 F.3d 1378 (11th Cir. 1998) 6

Reporters Comm. for Freedom of the Press v. AT&T,
593 F.2d 1030 (D.C. Cir. 1978) 6, 7, 10

In re Schering Plough Corp. Intron/Temodar Consumer Class Action,
678 F.3d 235 (3d Cir. 2012) 1, 3, 4

Tabbaa v. Chertoff,
509 F.3d 89 (2d Cir. 2007) 10

United States v. Mayer,
503 F.3d 740 (9th Cir. 2007) 6, 7

United States v. U.S. Dist. Ct. (Keith),
407 U.S. 297 (1972) 6, 9

United States v. Verdugo-Urquidez,
494 U.S. 259 (1990) 8

Williams v. Price,
25 F. Supp. 2d 623 (W.D. Pa. 1998) 11

Zurcher v. Stanford Daily,
436 U.S. 547 (1978) 6, 7

STATUTES

50 U.S.C. § 1801(e) 8

50 U.S.C. § 1801(h) 13

50 U.S.C. § 1861(a)(1) 8

50 U.S.C. § 1861(a)(2)(B) 7

50 U.S.C. § 1881a(a) 8

50 U.S.C. § 1881a(b) 8

50 U.S.C. § 1861(g)(2) 13

50 U.S.C. § 1881a(e) 13

INTRODUCTION

Like its forerunners, Plaintiff's Second Amended Complaint (ECF No. 19) ("2d Am. Compl.") contains insufficient allegations of injury to establish his standing, and fails to state viable claims for relief. In sum, the Second Amended Complaint reprises the allegations and claims already set forth in Plaintiff's prior complaints, and to them adds (1) new "background" allegations about NSA intelligence-gathering activities made in another pending case, *see* 2d Am. Compl. ¶¶ 1-23; (2) class action allegations, *id.* ¶¶ 76-84; and (3) a new claim alleging violation of the First Amendment, *id.* ¶¶ 132-39. Plaintiff's prior claims and allegations remain legally deficient for the reasons explained in the Government's Brief in Support of Defendants' Motion to Dismiss (ECF No. 6) ("Gov't Br."), and Brief in Support of Defendants' Motion to Dismiss Plaintiff's First Amended Complaint (ECF No. 14) ("Gov't 2d Br."), which are incorporated herein by reference. For the reasons set forth below, Plaintiff's new claim and allegations also fail to establish his entitlement to any relief. Accordingly, the Second Amended Complaint must also be dismissed.

ARGUMENT

I. THE SECOND AMENDED COMPLAINT FAILS TO ESTABLISH PLAINTIFF'S STANDING.

As the Government demonstrated in support of its motions to dismiss Plaintiff's two prior iterations of his complaint, Gov't Br. at 9-12; Gov't 2d Br. at 5-10, neither contained well-pleaded allegations of fact "that affirmatively and plausibly suggest" that Plaintiff's online communications have ever been acquired under the NSA's PRISM program, or that records about his telephone calls have ever been collected under the NSA's bulk telephony metadata program. *See In re Schering Plough Corp. Intron/Temodar Consumer Class Action*, 678 F.3d 235, 243-44 (3d Cir. 2012), citing *Ashcraft v. Iqbal*, 556 U.S. 662, 678 (2009). Plaintiff predicates his standing to challenge these foreign-intelligence programs on the claim that the

NSA collects the online communications, and records about the telephone calls, of all Americans, including, therefore, his. But notwithstanding the new wave of "background" allegations he has added to the complaint, 2d Am. Compl. ¶¶ 1-23, Plaintiff still has not plausibly alleged this to be the case.

Principally, Plaintiff embellishes his own allegations with claims made by the plaintiffs (and several of their declarants) in *Jewel v. NSA*, 08-cv-4373 (JSW) (N.D. Cal.). 2d Am. Compl. ¶¶ 8-23. *Jewel* is a self-described "challenge[to] an [alleged] illegal and unconstitutional program of dragnet communications surveillance conducted by the [NSA] and other Defendants …." *Jewel*, Complaint for Constitutional & Statutory Violations (ECF No. 1) ("*Jewel* Compl.") ¶ 2. Plaintiff incorporates into his complaint the allegation in *Jewel* that the NSA uses a "nationwide network of … surveillance devices" "to acquire the content of a significant portion of the phone calls, emails … and other [online] communications … of practically every American who uses the phone system or the Internet …." *Id.* ¶¶ 8, 9; *see* 2d Am. Compl. ¶ 15.

But the *Jewel* complaint (like Plaintiff's) lacks the "factual enhancement" required to support this "naked assertion," and it is therefore not entitled to the presumption of truth. *Iqbal*, 556 U.S. at 678, 681; *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 554-55 (2007). The *Jewel* complaint alleges only that the NSA collects Internet-based communications at AT&T facilities located in four states—California, Washington, Georgia, and Missouri—and records, stored in AT&T databases, that pertain to the telecommunications of AT&T customers. *Jewel* Compl. ¶¶ 55, 68, 82-83. Regardless of whether the *Jewel* complaint adequately pleads the standing of the plaintiffs there, who allegedly are AT&T subscribers, *see id.* ¶¶ 20-24, it contains no well-pleaded allegations from which it could plausibly be concluded that the NSA collects information about the telecommunications of "practically every American," including persons, such as Plaintiff, who are not subscribers to services provided by AT&T. *See* 2d Am. Compl.

¶ 87 (listing telecommunications services to which Plaintiff subscribes). Plaintiff's burden here is to set forth well-pleaded, non-conclusory allegations of fact that affirmatively and plausibly suggest he has suffered a concrete and particularized injury that is traceable to the Government's alleged conduct. *Iqbal*, 556 U.S. at 678-79; *Schering Plough*, 678 F.3d at 243-44. It does him no good simply to repeat the conclusory allegations contained in other litigants' complaints.

Plaintiff also cites the Ninth Circuit's decision in *Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2011), as support for his standing. 2d Am. Compl. ¶ 22. But that decision is of no assistance to Plaintiff because it concerned a standing issue different from the one presented here. In *Jewel* the district court dismissed the complaint for lack of standing on the basis that the harm alleged by the plaintiffs was not "sufficiently particular to [them]," and was instead "a generalized grievance shared in substantially equal measure by all or a large class of citizens" — an argument the Government had not made. *Jewel v. NSA*, 2010 WL 235075, at *1 (N.D. Cal. Jan. 21, 2010).[1] The Ninth Circuit reversed, holding that the injuries asserted by the *Jewel* plaintiffs were not "abstract, generalized grievances and instead me[t] the constitutional standing requirement of concrete injury," because (contrary to the district court's conclusion) the plaintiffs' allegations "'specifically link[ed] [them] to the alleged surveillance activities.'" *Jewel*, 673 F.3d at 905, 907 (quoting *Jewel*, 2010 WL 235075, at *5); *see id.* at 910.

The Government's motion in this case, however, does not present the question whether Plaintiff's claimed injury is sufficiently concrete and particularized. The question is whether Plaintiff's claim that he has been injured at all is supported by sufficient well-pleaded and non-

[1] *See Hollingsworth v. Perry*, 133 S. Ct. 2652, 2662 (2013) (explaining that "raising only a generally available grievance about government—claiming only harm to [the plaintiff's] and every citizen's interest in proper application of the Constitution and laws, and seeking relief that no more directly and tangibly benefits him than it does the public at large"—does not state a concrete and particularized injury that confers Article III standing) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 573-74 (1992)); *Lance v. Coffman*, 549 U.S. 437, 439 (2007).

conclusory allegations of fact to meet the plausibility requirement of *Iqbal* and *Schering Plough*. The answer is no, because neither Plaintiff's own allegations, nor those he has imported from *Jewel*, plausibly link him to the alleged intelligence-gathering activities he purports to challenge. *See Defenders of Wildlife*, 504 U.S. at 563 (Article III requires "that the party seeking [judicial] review" of allegedly unlawful conduct "be himself among the injured").[2]

The declarations that Plaintiff cites from the *Jewel* case also fail to establish that critical link, as none of them supports the allegation that the NSA collects information about the telecommunications of all Americans. Plaintiff cites the statement of former NSA employee William Binney that, following the September 11, 2001, terrorist attacks, he "learned" that the NSA had begun using a "data-min[ing] program" to "collect and analyze domestic e-mail, without a warrant." 2d Am. Compl. ¶¶ 9-12, 19; *see Jewel*, Declaration of William E. Binney (ECF No. 88) ("Binney Decl.") ¶¶ 5-6. But nothing in these allegations—which are based on hearsay (*see* Binney Decl. ¶ 5)—even purports to describe the scope or scale of these supposed surveillance activities, or supports the conclusion that they involved collection of information about all Americans' communications.

In addition to the Binney Declaration, Plaintiff cites the declarations of two other former NSA employees, *Jewel*, Declaration of J. Kirk Wiebe (ECF No. 86) ("Wiebe Decl."); *id.*, Declaration of Thomas A. Drake (ECF No. 87) ("Drake Decl."); *see* 2d Am. Compl. ¶¶ 20, 21, who express agreement with Mr. Binney's assertion that the NSA today "has the capability to seize and store most electronic communications passing through its U.S. intercept centers," which Mr. Binney "estimate[s]" to number between ten and twenty. Binney Decl. ¶¶ 7-9; Wiebe

[2] Whether the *Jewel* plaintiffs can prove their standing as a matter of fact, and can do so without risking or requiring impermissible disclosures of national security information protected by the state secrets privilege, remains the subject of ongoing proceedings in that case. *See, e.g.*, *Jewel*, Gov't Defs.' Opp. to Pls.' Mot. for Partial Summ. Judg. & Cross-Mot. for Partial Summ. Judg. on Pls.' Fourth Am. Claim (ECF No. 286-6) at 20-23.

Decl. ¶ 8; Drake Decl. ¶ 8. They also agree with Mr. Binney's conclusion, based on media reports about the anticipated capacity of new NSA digital storage facilities, that the NSA "is, in fact, storing all [the electronic communications] that they are collecting." Binney Decl. ¶¶ 11-13; Wiebe Decl. ¶ 9; Drake Decl. ¶ 9. But by the time these gentlemen executed their declarations in June 2012, they had not been employed by the NSA for years—in the cases of Messrs. Binney and Wiebe, for more than a decade—*see* Binney Decl. ¶ 6; Wiebe Decl. Exh. A at 2; Drake Decl. Exh. A at 2, and could only speculate about the nature, scope, and focus of the NSA's current intelligence-gathering activities. The Supreme Court has made clear that speculation about the scope and operation of the Government's foreign-intelligence surveillance programs will not support a finding, for standing purposes, that a litigant has been a subject of such surveillance. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147-51 (2013). Moreover, even assuming the NSA were "stor[ing] most electronic communications passing through its U.S. intercept centers," nothing in the Binney, Wiebe, and Drake Declarations even purports to suggest what fraction of Americans' electronic communications passes through the 10-20 "intercept centers" whose existence Mr. Binney posits, much less that they intercept the communications of all Americans, including Plaintiff's.[3]

Notwithstanding multiple attempts, Plaintiff still has not set forth well-pleaded, non-conclusory allegations from which it could plausibly be concluded that the NSA intelligence-gathering activities he purports to challenge involve the collection of information about all Americans' communications, nor any other non-speculative basis on which it could plausibly be concluded that these activities involve collection of information about his communications.

[3] Plaintiff's class-action allegations, 2d Am. Compl. ¶¶ 76-84, are immaterial to the standing analysis. Plaintiff must establish his standing regardless of whether he seeks to litigate his claims individually or on behalf of a class. *Hayes v. Wal-Mart Stores, Inc.*, 725 F.3d 349, 360-61 (3d Cir. 2013); *McNair v. Synapse Group, Inc.*, 672 F.3d 213, 223-24 (3d Cir. 2012).

Plaintiff therefore cannot establish his Article III standing, and this case must be dismissed for lack of subject matter jurisdiction. *Kerchner v. Obama*, 612 F.3d 204, 207 (3d Cir. 2010).

II. PLAINTIFF'S FIRST AMENDMENT CLAIM SHOULD BE DISMISSED.

Plaintiff's First Amendment claim, 2d Am. Compl. ¶¶ 134-39, asserts that the challenged NSA intelligence-gathering programs violate his freedom of speech and association. Under long accepted principles, discussed below, Plaintiff's First Amendment claim perishes in the wake of his Fourth Amendment claim, which fails for the reasons discussed in the Government's prior briefs. *See* Gov't Br. at 12-19; Gov't 2d Br. at 10-19. Alternatively, even if the Court were to hold that Plaintiff's First Amendment claim could survive dismissal of his Fourth Amendment claim, his allegations would still be insufficient to establish an entitlement to relief for violation of his First Amendment rights.

A. Good-Faith Investigatory Conduct Not Intended to Deter or Punish Protected Speech or Association Does Not Violate the First Amendment.

Recognizing the need to accommodate the Government's interests where prevention of crime, or, even more imperatively, potential threats to national security are concerned, *see United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297, 313 (1972), courts distinguish for purposes of First Amendment analysis between government investigations that may have an incidental effect of deterring First Amendment activity, and concrete government action of a regulatory, proscriptive, or compulsory nature that is directed against individuals based on their expressive or associational activities. *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *Laird v. Tatum*, 408 U.S. 1, 11 (1972); *United States v. Mayer*, 503 F.3d 740, 747-53 (9th Cir. 2007); *Redd v. City of Enter.*, 140 F.3d 1378, 1383-84 (11th Cir. 1998); *Gordon v. Warren Consol. Bd. of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983) (collecting cases); *ACLU v. Barr*, 952 F.2d 457, 471 (D.C. Cir. 1991); *Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1051-

53 (D.C. Cir. 1978); *[Redacted]*, Dkt. No. PR/TT [redacted], Opinion and Order, 66-69 (F.I.S.C. [date redacted]) (attached hereto as Exhibit A).

Accordingly, good faith governmental investigations conducted with "scrupulous" adherence, *Zurcher*, 436 U.S. at 564, to Fourth Amendment requirements, without the purpose of deterring or penalizing protected expression or association, do not violate the First Amendment. *See Reporters Comm.*, 593 F.2d at 1051-53; *see also Gordon*, 706 F.2d at 781 n.3 ("[S]urveillance consistent with Fourth Amendment protections . . . does not violate First Amendment rights, even though it may be directed at communicative or associative activities."); *ACLU v. Clapper*, 959 F. Supp. 2d 724, 753 (S.D.N.Y. 2013) (concluding that "[t]he Government's argument [on this point] is well-supported").[4]

Here, Plaintiff does not even purport to allege that the challenged NSA programs are directed against him (or any other individuals) based on expressive or associational activities. Indeed, as the court in *ACLU* recognized, the express terms of Section 215 (under which the bulk collection of telephony metadata is authorized) prohibit the statute's use for purposes of investigations "conducted 'solely on the basis of activities that are protected by the first amendment,'" 959 F. Supp. 2d at 753 (quoting 50 U.S.C. § 1861(a)(2)(B)), a restriction the FISC takes into account and reinforces each time it re-authorizes the bulk telephony metadata program. *See* September 11, 2014, FISC Primary Order (attached hereto as Exhibit B) at 2; *id.* at 7 n.6, 9 n.7 (prohibiting queries of the metadata using selectors chosen "solely on the basis of activities

[4] The Ninth Circuit has "clarif[ied] that good faith . . . requires" that the "government investigation" be "justified by a legitimate" purpose that "outweighs any harm to First Amendment interests." *Mayer*, 503 U.S. at 753; *see also Barr*, 952 F.2d at 471 (no "legitimate purpose" when "surveill[ing] with the intent of deterring membership in . . . an association engaged in lawful activities"). For the reasons set forth in the text, both the bulk telephony metadata program and the PRISM collection authorized by Section 702 surmount this low bar.

that are protected by the First Amendment").[5] And FISA Section 702, under which PRISM collection is conducted, authorizes targeting only of non-U.S. persons reasonably believed to be located abroad, 50 U.S.C. § 1881a(b), that is, of persons who do not have First Amendment rights to begin with, *see United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990) ("[A]liens receive constitutional protections [only] when they have come within the territory of the United States and developed substantial connections with this country.").

Indeed, Plaintiff makes no claim that the bulk telephony metadata program is conducted for any purpose other than the statutorily authorized objective of obtaining foreign intelligence information to protect against foreign terrorist attacks, *see* 50 U.S.C. § 1861(a)(1); September 11, 2014, Primary Order at 2. Nor has Plaintiff alleged that targeted PRISM collection of non-U.S. person communications is conducted for any purpose other than the authorized acquisition of foreign intelligence information to protect the Nation against such dangers as, for example, international terrorism, the international proliferation of weapons of mass destruction, and the clandestine intelligence activities of foreign powers, *see* 50 U.S.C. § 1801(e); *id.* § 1881a(a). These are not only legitimate Government interests, they represent paramount national security concerns. *Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010) ("[T]he Government's interest in combating terrorism is an urgent objective of the highest order."); *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("[N]o governmental interest is more compelling than the security of the Nation."); *In re Directives*, 551 F.3d 1004, 1012 (FISC Ct. Rev. 2008) (national-security interest in conducting acquisitions pursuant to Section 702 "is of the highest order of magnitude").

[5] Although Plaintiff's allegation that the bulk telephony metadata program collects "all 'call detail records' for calls made wholly within the United States," 2d Am. Compl. ¶ 33, is incorrect, *see* Gov't 2d Br. at 9, it underscores the point that Plaintiff does not and, due to the program's scale, cannot suggest that the program singles him out in any way, let alone on the basis of his expressive or associational activity.

Because Plaintiff has not plausibly alleged that these intelligence-gathering programs violate his Fourth Amendment rights, *see* Gov't Br. at 12-19; Gov't 2d Br. at 10-19, nor alleged at all (plausibly or otherwise) that the purposes of these programs include the suppression of free expression or association, *supra*, at 7-8, he has failed to state a claim that either of the challenged programs violates the First Amendment.[6]

B. Plaintiff's First Amendment Claim Must Also Be Dismissed for Failure to Allege a Direct and Substantial Burden on his Freedom of Speech or Association.

Even if the Court concluded that Plaintiff's First Amendment claim could in theory survive dismissal of his Fourth Amendment claim, his First Amendment claim would still fail for the independent reason that he has not alleged a direct and substantial burden on his freedom of speech or association. Rather, Plaintiff's allegations amount at most to a subjective "chill" on his First Amendment freedoms, arising solely from speculative fears that are based on his (mis)understanding of the challenged NSA programs rather than their actual operation. These misplaced fears are an insufficient basis on which to bring a First Amendment claim.

"[C]onsonant with the First Amendment," the Government "may engage" in conduct that "incidentally inhibits protected forms of association," which, though it may "make it more

[6] The Supreme Court's decision in *Keith* is not to the contrary. In that case, the Court addressed the constitutionality of warrantless surveillance targeting "domestic organizations" that sought to "attack and subvert" the Government. *Keith*, 407 U.S. at 299-300. In finding that prior judicial approval for such surveillance was necessary, *id.* at 321, the Court expressed particular concern that "domestic security surveillance" might infringe on "constitutionally protected privacy of speech" "because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent." *Id.* at 320. The concerns that animated the *Keith* Court are not implicated by the telephony metadata program or PRISM collection, because, as explained above, Sections 215 and 702 authorize only the collection of foreign intelligence, and their terms prohibit, either expressly, or in effect, the investigation of persons solely on the basis of activities protected by the First Amendment. *See Keith*, 407 U.S. at 321-22 ("emphasiz[ing]" that the "scope of [its] decision" addressed only the "domestic aspects of national security" and did "not address[]" the "issues which may be involved with respect to activities of foreign powers or their agents").

difficult for individuals to exercise their freedom of association, this consequence does not, without more, result in a violation of the First Amendment." *Fighting Finest, Inc. v. Bratton*, 95 F.3d 224, 228 (2d Cir. 1996) (citing *Lyng v. UAW*, 485 U.S. 360, 366 (1988)); *see also Reporters Comm.*, 593 F.2d at 1052 ("Not every Government action that affects, has an impact on, or indeed inhibits First Amendment activity constitutes the kind of 'abridgement' condemned by the First Amendment."). "Mere incidental burdens on the right to associate do not violate the First Amendment." *Tabbaa v. Chertoff*, 509 F.3d 89, 101 (2d Cir. 2007); *ACLU*, 959 F. Supp. 2d at 753 (stating same in finding that the "bulk [telephony] metadata collection does not burden First Amendment rights substantially"). Rather, "[t]o be cognizable, the interference with associational rights must be 'direct and substantial' or 'significant.'" *Fighting Finest, Inc.*, 95 F.3d at 228 (quoting *Lyng*, 485 U.S. at 366, 367 & n.5).

Plaintiff's allegations of a violation of his free-speech and associational rights do not meet this standard. Plaintiff claims that he is "no longer able to freely express himself by means of e-mail or in documents stored by means of internet cloud services because the Defendants are collecting and data-mining such documents." 2d Am. Compl. ¶ 136. He maintains also that the Defendants have "interfered with [his] ability to freely associate with other persons" because the Defendants have obtained "phone and internet data showing with whom [he] associates." *Id.* ¶ 138. These allegations fail to state a claim that the Government has burdened Plaintiff's First Amendment rights at all, much less in a "direct" and "substantial" manner, first because they are predicated on the assumption that the challenged NSA intelligence programs involve interception of Plaintiff's electronic communications, and acquisition of metadata associated with Plaintiff's telephone calls. As discussed above and in the Government's prior briefs, Plaintiff has not

plausibly alleged that to be the case. *See supra*, at 2-5; Gov't Br. at 9-12; Gov't 2d Br. at 5-10.[7] Plaintiff's "bare assertions," *Iqbal*, 556 U.S. at 681, in his First Amendment claim that the Government is "collecting and data-mining" his online documents, and has obtained "phone and internet data showing with whom [he] associates,'" 2d Am. Compl. ¶¶ 136, 138, are just as unaccompanied by "factual matter" raising them "above the speculative level" as are the similar "background" allegations set forth in his complaint. *Twombly*, 550 U.S. at 555-56.[8]

Second, claims that Plaintiff "is no longer able to freely express himself" or "freely associate with other persons," simply because of a fear that the Government might obtain or "data-mine" information about his communications, are insufficient to state a claim for direct and substantial interference with his First Amendment rights. It is true that a "constitutional violation[] may arise from the deterrent, or 'chilling,' effect" of government action that "fall[s] short of a direct prohibition against the exercise of First Amendment rights." *Laird*, 408 U.S. at 11. But the alleged chill on Plaintiff's First Amendment freedoms is attributable to his own speculative fears of surveillance, rather than being plausibly connected to the challenged

[7] Even presuming that the Government has collected metadata associated with Plaintiff's telephone calls under the bulk telephony metadata program, under the FISC's orders NSA analysts may only review those records within two hops of selectors (*e.g.*, telephone numbers) that the FISC has determined are reasonably suspected of association with terrorist organizations the FISC has approved for targeting. *See* September 11 Primary Order at 2, 7-8; Gov't 2d Br. at 3, 8-10. Plaintiff has made no plausible allegation that records of his calls are among the "very small percentage" of the records that are ever reviewed by NSA analysts under this standard. *See ACLU*, 959 F. Supp. 2d at 735. Hence, the Second Amended Complaint contains no "factual matter" to support Plaintiff's assertion that the Government learns "with whom [he] associates," 2d Am. Compl. ¶ 138, from bulk telephony metadata collected by the NSA. *Twombly,* 550 U.S. at 555-56; *see Iqbal*, 556 U.S. at 681.

[8] For this reason, *Williams v. Price*, 25 F. Supp. 2d 623 (W.D. Pa. 1998), provides no comfort to Plaintiff. In that case, the court found that the claimed First Amendment right of the plaintiff prisoners to confer confidentially with their counsel was chilled by the presence of correctional officers, stationed outside the meeting room, who could hear what the inmates and counsel were saying inside. *Id.* at 624-25, 630. Here, in contrast, Plaintiff has not plausibly alleged that his online communications, or telephony metadata associated with his calls, have been obtained or reviewed by the Government.

intelligence programs, because, as we have shown, the Second Amended Complaint contains no plausible allegations that information about Plaintiff's communications has been obtained, reviewed, or used in any fashion under PRISM or the telephony metadata program. *See supra*, at 2-5; Gov't Br. at 9-12; Gov't 2d Br. at 5-8. "Allegations of a subjective chill" arising from an "individual's knowledge" of the "mere existence, without more, of a governmental investigative and data-gathering activity" "are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm." *Laird*, 408 U.S. at 10, 11, 13-14.[9] Such allegations are insufficient even to confer standing, much less to state a claim for a First Amendment violation. *See Amnesty Int'l, USA,* 133 S. Ct. at 1152 (and cases cited therein); *ACLU*, 959 F. Supp. 2d at 754 ("Fear that telephony metadata relating to [plaintiffs' calls] will be queried or reviewed or further investigated 'relies on a highly attenuated chain of possibilities,'" and that "speculative fear" can neither "create standing" nor "establish a violation of an individual's First Amendment rights.") (quoting *Amnesty Int'l*, 133 S. Ct. at 1148, 1152).[10]

---

[9] *See also Paton v. La Prade*, 524 F.2d 862, 874 (3d Cir. 1975) (teacher who designed a course taken by a student, and who claimed that a resulting FBI investigation of the student "constituted an 'inhibiting force'" on his free expression, suffered only a non-cognizable "subjective chill"); *Philadelphia Yearly Meeting of Religious Soc'y of Friends v. Tate*, 519 F.2d 1335, 1137-39 (3d Cir. 1975) (plaintiffs suffered only "subjective chill" of First Amendment rights arising from police creation of "dossiers" about them based on information gathered from "public meetings," which the police shared with "other law enforcement agencies"; cognizable injury occurred only when police shared dossiers with public or "broadcast" on "network television" the names of groups and individuals "on whom such files were kept"); *Gross v. Taylor*, 1997 WL 535872, at *16 (E.D. Pa. Aug. 5, 1997) ("vague charge of chilled expression" insufficient to "sustain" a "First Amendment claim").

[10] Plaintiff's allegation he could not consult with certain persons by e-mail in preparing his Second Amended Complaint, because "the Defendants could provide such communications *directly* to the lawyers representing the [G]overnment in this lawsuit," 2d Am. Compl. ¶ 137, provides no support for his First Amendment claim. This allegation is too speculative to satisfy either the requirement of actual or imminent injury, *see Amnesty Int'l, supra*, or the plausibility standard under *Iqbal*. That is all the more so considering that both Section 215 and Section 702 require the Government to adopt minimization procedures "to prohibit the dissemination …of nonpublicly available information concerning unconsenting United States persons" except as

(footnote continued on next page)

Accordingly, Plaintiff's First Amendment claim, like the other causes of action he has attempted to plead, states no violation of legal right entitling him to relief.

CONCLUSION

For the reasons stated above, the Second Amended Complaint should be dismissed.

Dated: December 11, 2014

Respectfully submitted,

JOYCE R. BRANDA
Acting Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel

/s/ Marcia Berman
MARCIA BERMAN
Senior Trial Counsel
RODNEY PATTON
Trial Attorney
JULIA A. BERMAN
Trial Attorney
U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Rm. 7132
Washington, D.C. 20001
Phone: (202) 514-2205
Fax: (202) 616-8470
Email: Marcia.Berman@usdoj.gov

Counsel for Defendants

(footnote continued from previous page)
"consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1861(g)(2), 1881a(e); *see id.* § 1801(h). Also unavailing is Plaintiff's allegation that "it is possible that future American governments will use" information obtained under the challenged NSA intelligence programs "to blackmail or target political enemies." 2d Am. Compl. ¶ 139. Again, this type of "allegation[] of *possible* future injury [is] not sufficient" to confer standing, much less support a claim for the violation of Plaintiff's First Amendment rights, *Amnesty Int'l USA*, 133 S. Ct. at 1147, especially because Plaintiff does not even allege that he might be among the unidentified "political enemies" whom the Government could hypothetically "target." *See Defenders of Wildlife*, 504 U.S. at 563.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA
(Pittsburgh Division)

ELLIOTT SCHUCHARDT, individually and d/b/a the Schuchardt Law Firm, Plaintiff, v. BARACK H. OBAMA, President of the United States, *et al*., Defendants.	Case No. 2:14-cv-0705-CB

DECLARATION OF MARCIA BERMAN IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS PLAINTIFF'S SECOND AMENDED COMPLAINT

I, Marcia Berman, hereby declare:

1. I am a Senior Trial Counsel for the United States Department of Justice, Civil Division, Federal Programs Branch, and one of the attorneys of record for defendants in the above-captioned matter. The statements made herein are based on my personal knowledge, and on information made available to me in the course of my duties and responsibilities as counsel for defendants in this case.

2. Filed with this declaration, as Exhibits A and B in support of Defendants' Motion to Dismiss Plaintiff's Second Amended Complaint, are true and correct copies of the following documents:

a. Exhibit A, *[Redacted]*, Dkt. No. PR/TT [redacted], Opinion and Order, 66-69 (F.I.S.C. [date redacted]);

b. Exhibit B, September 11, 2014, FISC Primary Order.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on December 11, 2014, at Washington, D.C.

/s/ Marcia Berman
MARCIA BERMAN
Senior Trial Counsel
Marcia.berman@usdoj.gov
U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7132
Washington, D.C. 20001
Phone: (202) 514-2205
Fax: (202) 616-8470

EXHIBIT A

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

FILED
[redacted]
U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

Docket Number: PR/TT [redacted]

OPINION AND ORDER

This matter comes before the Court on an application of the Government for authority for the National Security Agency (NSA) to collect information regarding e-mail and certain other forms of Internet communications under the pen register and trap and trace provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States Code (U.S.C.), §§ 1801-1811, 1841-1846. This application seeks authority for a

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

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

much broader type of collection than other pen register/trap and trace applications and therefore presents issues of first impression.[1] For that reason, it is appropriate to explain why the Court concludes that the application should be granted as modified herein.

Accordingly, this Opinion and Order sets out the bases for the Court's findings that: (1) the collection activities proposed in the application involve the installation and use of "pen registers" and/or "trap and trace devices" as those terms are used in FISA, 50 U.S.C. §§ 1841-1846; (2) the application, which specifies restrictions on the retention, accessing, use, and dissemination of information obtained from these collection activities, "satisfies the requirements" of 50 U.S.C. § 1842 for the issuance of an order "approving the installation and use of a pen register or trap and trace device," id. § 1842(d)(1), subject to modifications stated herein;[2] and (3) the installation and use of these pen registers and/or trap and trace devices pursuant to

---

[1] The application was filed in two steps: an application filed on [redacted] followed by an addendum filed on [redacted] For ease of reference, the following discussion refers to both submissions collectively as the application.

[2] The Court has authority in this case to "enter an ex parte order as requested, or as modified." 50 U.S.C. § 1842(d)(1).

this Opinion and Order will comply with the First and Fourth Amendments.

In making these findings, the Court relies on factual representations made in the application, which was submitted by the Attorney General as applicant and verified by the Director of the NSA (DIRNSA); in the separate declaration of the DIRNSA (Attachment A to the application); and in the declaration of the [redacted] (Attachment B to the application). The Court has given careful consideration to the arguments presented in the Government's memorandum of law and fact (Attachment C to the application).

By letter dated [redacted] the Court directed the Government to respond to two questions necessary to its ruling on this application. The Court relies on the Government's responses to these questions, which were provided in a letter submitted on [redacted]

The Court also relies on information and arguments presented in a briefing to the Court on [redacted] which addressed the current and near-term threats posed by [redacted]

---

[3] One of these questions concerned First Amendment issues presented by the application. The other concerned the length of time that the Government expected the collected information to retain operational significance. These questions and the Government's responses are discussed more fully below.

[redacted] investigations conducted by the Federal Bureau of Investigation (FBI) to counter those threats, the proposed collection activities of the NSA (now described in the instant application), the expected analytical value of information so collected in efforts to identify and track operatives [redacted] and the legal bases for conducting these collection activities under FISA's pen register/trap and trace provisions.[4]

The principal statutory issues in this matter are whether the proposed collection constitutes the installation and use of "pen registers" and/or "trap and trace devices" and, if so, whether the certification pursuant to 50 U.S.C. § 1842(c)(2) is adequate. These issues are addressed below.

I. THE PROPOSED COLLECTION IS A FORM OF PEN REGISTER AND TRAP AND TRACE SURVEILLANCE.

For purposes of 50 U.S.C. §§ 1841-1846, FISA adopts the definitions of "pen register" and "trap and trace device" set out

---

[4] This briefing was attended by (among others) the Attorney General; [redacted] the DIRNSA; the Director of the FBI; the Counsel to the President; the Assistant Attorney General for the Office of Legal Counsel; the Director of the Terrorist Threat Integration Center (TTIC); and the Counsel for Intelligence Policy.

in 18 U.S.C. § 3127. See 50 U.S.C. § 1841(2). Section 3127 gives the following definitions:

> (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of business;
>
> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

These definitions employ three other terms – "electronic communication," "wire communication," and "contents" – that are themselves governed by statutory definitions "set forth for such terms in section 2510" of title 18. 18 U.S.C. § 3127(1). Section 2510 defines these terms as follows:

(1) "Electronic communication" is defined at 18 U.S.C. § 2510(12) as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole

or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include - (A) any wire or oral communication."[5]

(2) "Wire communication" is defined at 18 U.S.C. § 2510(1) as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

(3) "Contents" is defined at 18 U.S.C. § 2510(8) to "include[] any information concerning the substance, purport, or meaning" of a "wire, oral, or electronic communication."[6]

While the definitions of "pen register" and "trap and trace device" each contain several elements, the application of these

---

[5] The other exclusions to this definition at § 2510(12)(B)-(D) are not relevant to this case.

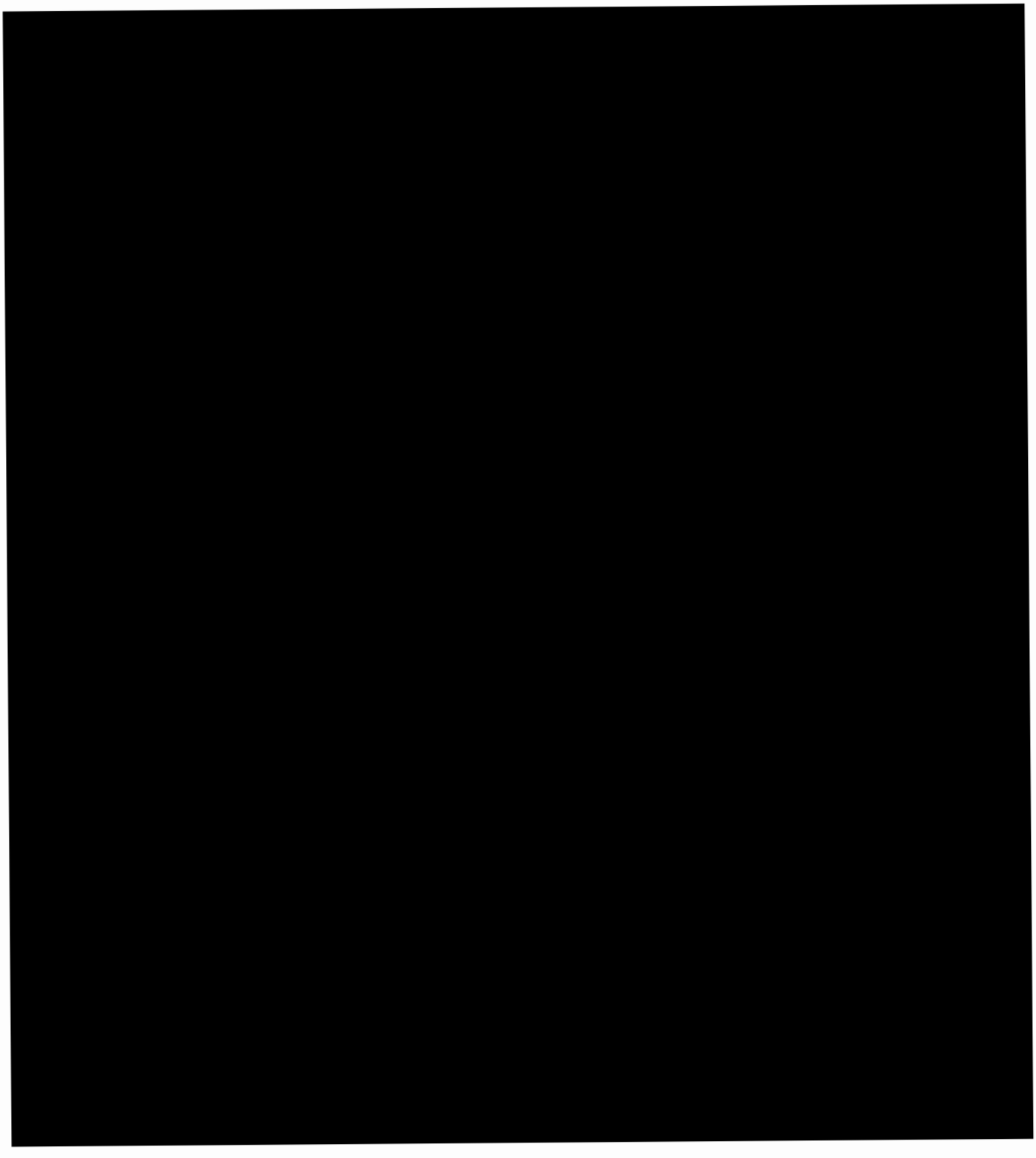
[6] Different definitions of "wire communication" and "contents" are provided at 50 U.S.C. § 1801(l), (n). However, the definitions set forth in § 1801 apply to terms "[a]s used in this subchapter," i.e., in 50 U.S.C. §§ 1801-1811 (FISA subchapter on electronic surveillance), and thus have no bearing on the meaning of "wire communication" and "contents" as used in the definitions of "pen register" and "trap and trace device" applicable to §§ 1841-1846 (separate FISA subchapter on pen registers and trap and trace devices).

definitions to the devices described in the application presents two primary questions: (1) Does the information to be obtained constitute "dialing, routing, addressing, or signaling information" that does not include the "contents" of any communication? (2) Does the means by which such information would be obtained come within the definition of "pen register" or "trap and trace device?" In addressing these questions, the Court is mindful that "when the statute's language is plain, the sole function of the courts - at least where the disposition required by the text is not absurd - is to enforce it according to its terms." Lamie v. United States Trustee, 124 S. Ct. 1023, 1030 (2004) (internal quotations and citations omitted).

A. The Information to Be Obtained Is "Dialing, Routing, Addressing, or Signaling Information" and Not "Contents."

The Government uses the umbrella term "meta data" to designate the categories of information it proposes to collect. This meta data comprises [redacted] categories:

[redacted]



[redacted]

[redacted]

Also, the address from which an e-mail was sent and [redacted] are not part of the e-mail's "contents."

---

[8] This is the first application presented to this Court for authority to [redacted] under pen register/trap and trace authority. The Court understands that FBI devices implementing prior pen register/trap and trace surveillance authorized by this Court have not obtained [redacted] See Memorandum of Law and Fact at 23-24 n.14. The fact that prior applications did not seek authority for this specific form of collection sheds no light on the merits of the instant application.

[redacted] but this isolated fact does not provide "information concerning the substance, purport, or meaning" of the e-mail. 18 U.S.C. § 2510(8).[9]

The DIRNSA Declaration mentions other types of information that are not described in the application as forms of meta data to be collected.[10] The Court understands such references to pertain to information or inferences that could be gleaned from accumulating meta data in Categories [redacted] above and/or analyzing meta data, perhaps in conjunction with information from other sources. This Opinion and Order authorizes only the collection of information in Categories [redacted]

[9] The finding that the [redacted] meta data do not constitute "content" is also supported by the assurance that meta data "does not include information from either the 'subject' or 're' line of the E-mail [redacted] DIRNSA Declaration at 3 n.1.

[10] These references in the DIRNSA Declaration include [redacted] at 12, and information said to pertain to elements of [redacted]

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]

[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]

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]

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]

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]

[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 [illegible] at . -2[illegible] & 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]

[redacted]

[redacted]

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

[redacted]

[redacted]

3. The Use of the Internet by [redacted]

[redacted]

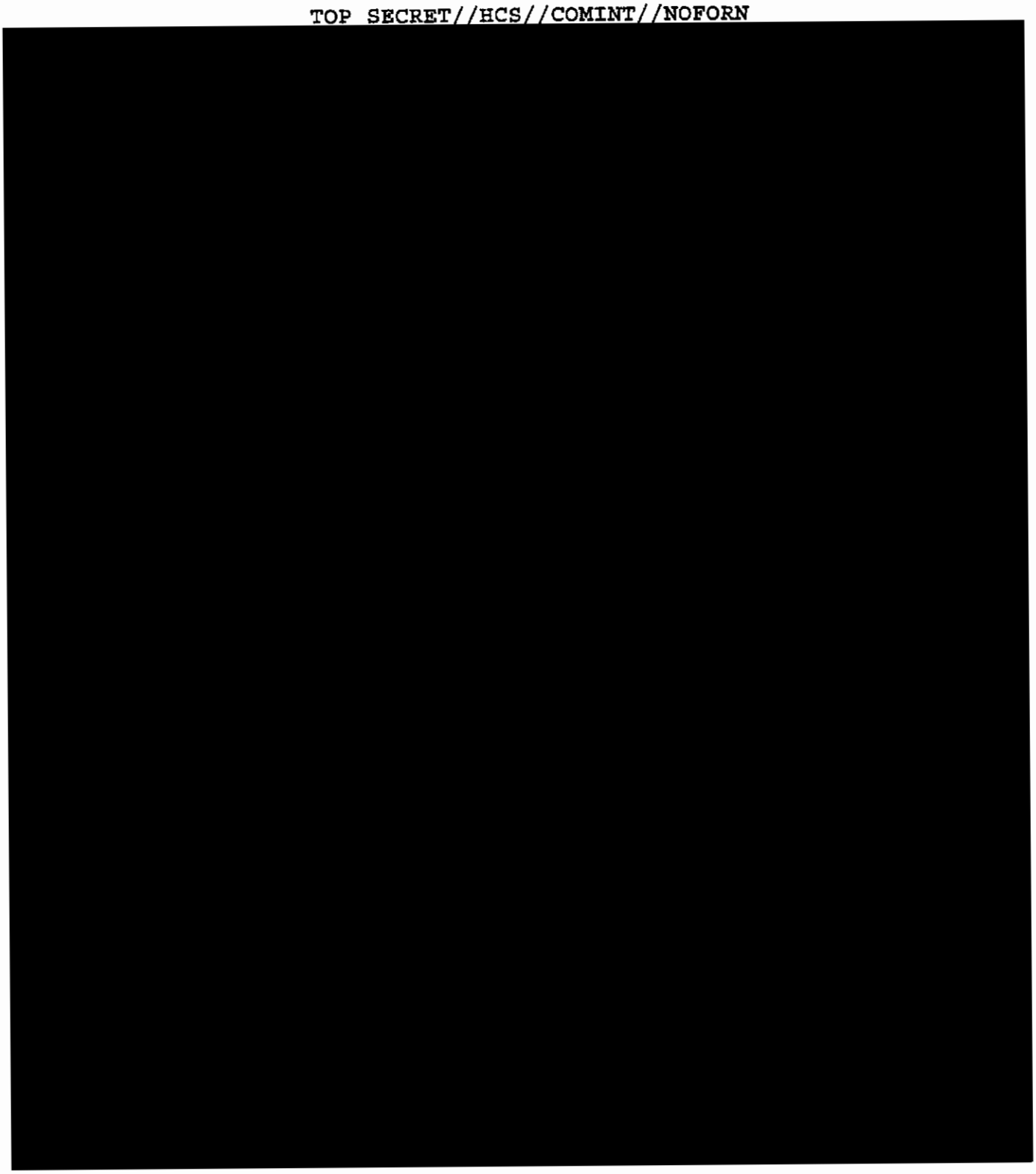
[redacted]

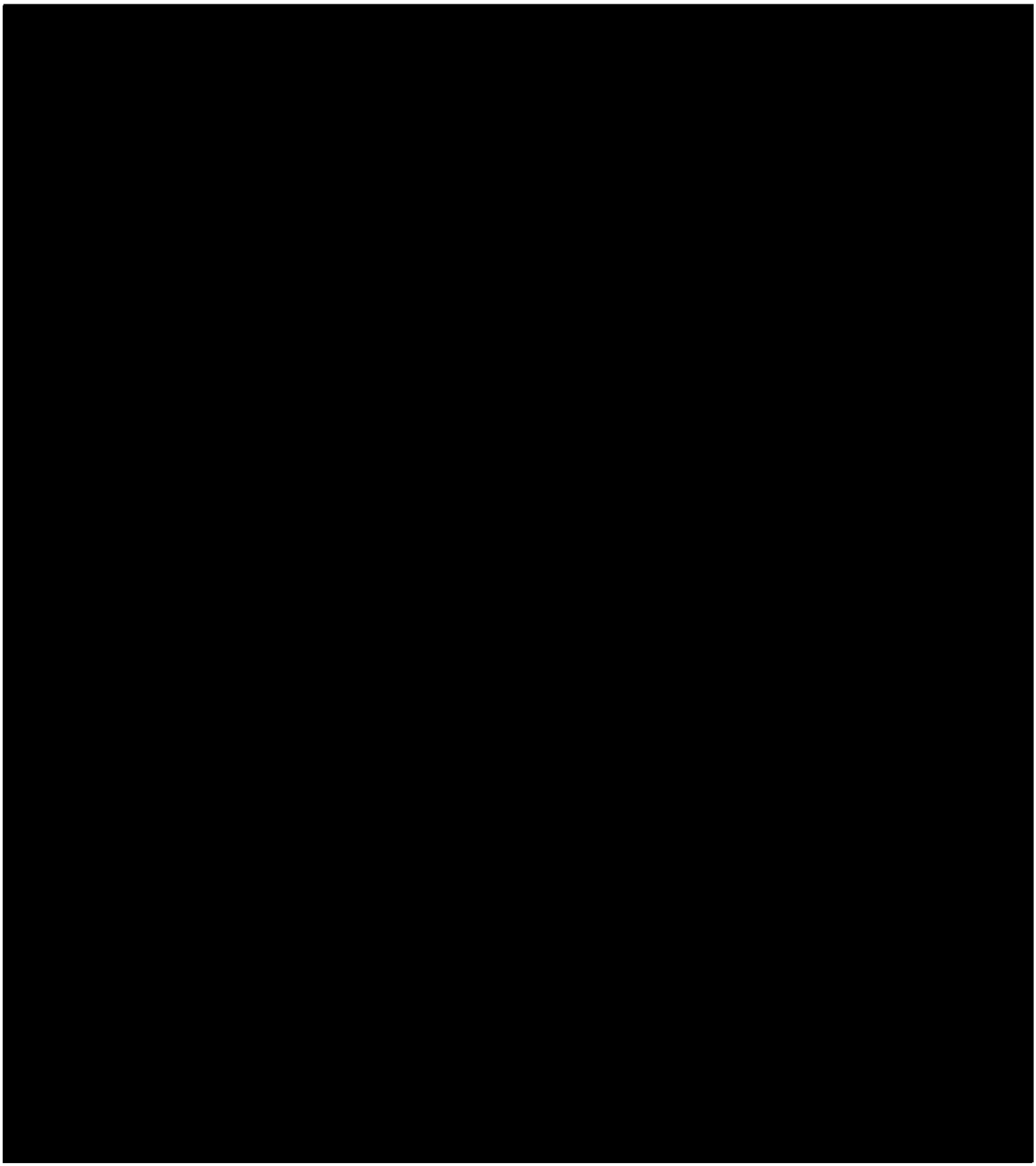
4. The Scope of the Proposed Collection of Meta Data

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]

[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. Aquilar, 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.

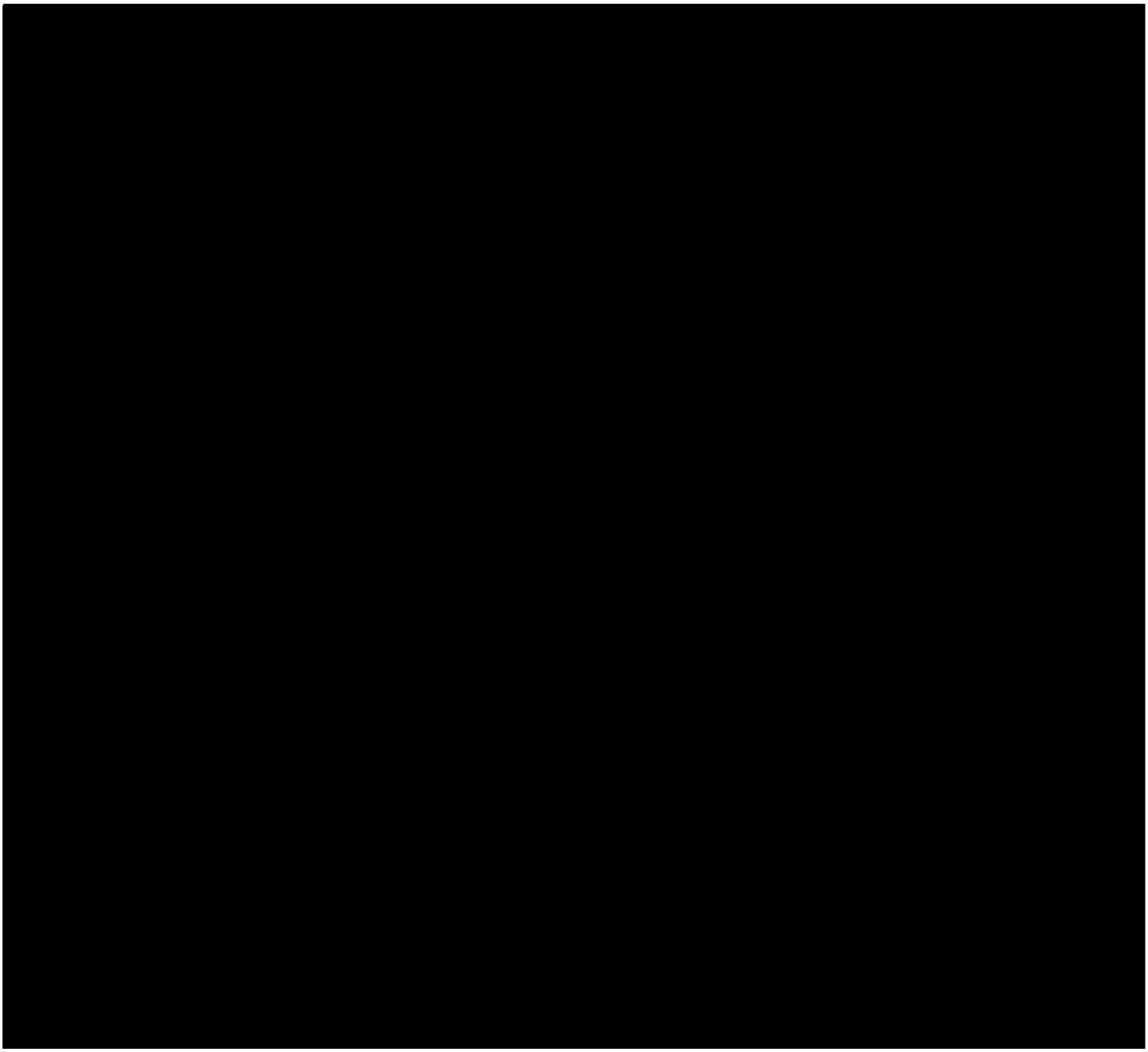
4. The pen registers and trap and trace devices [redacted]

[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]

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

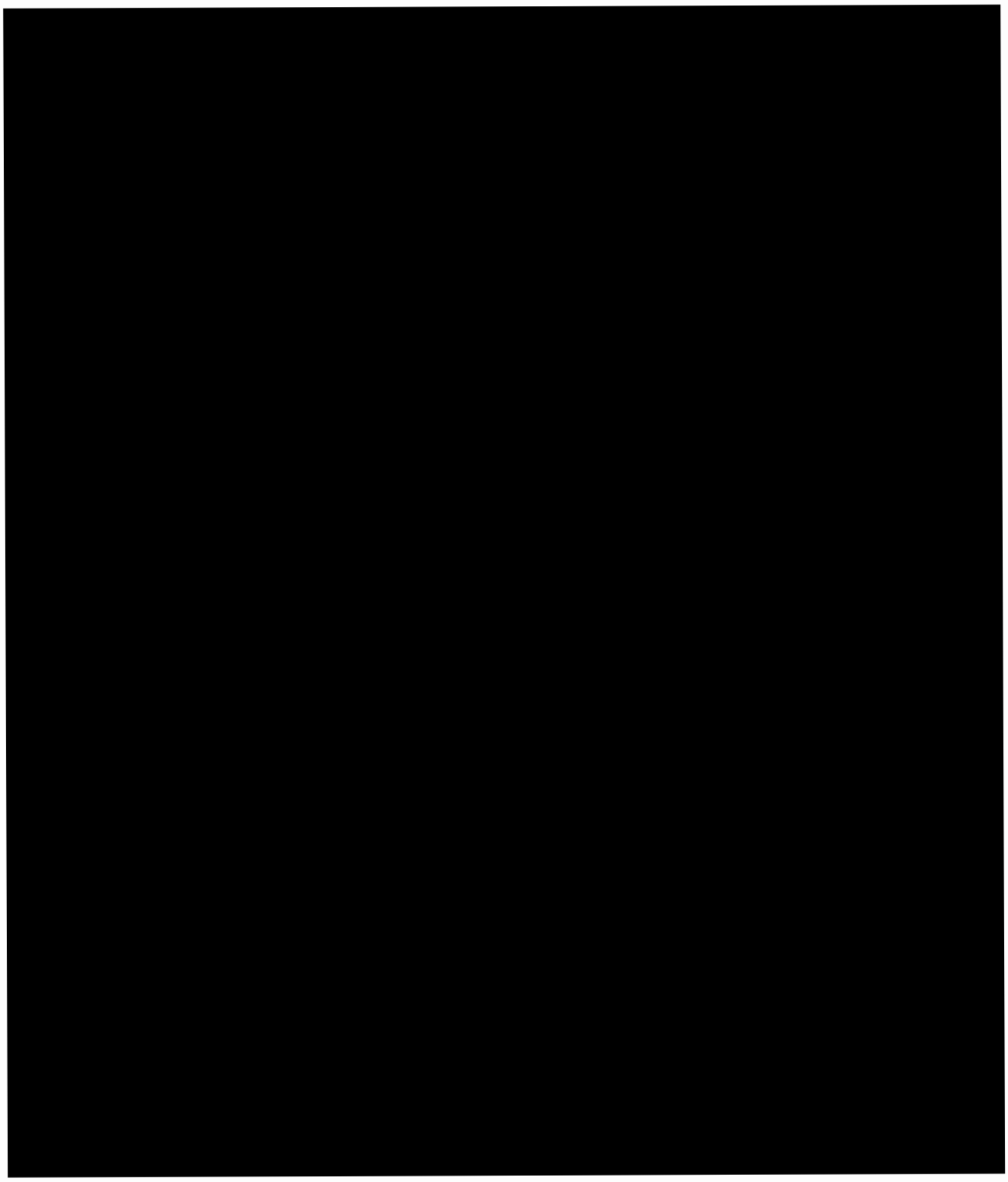


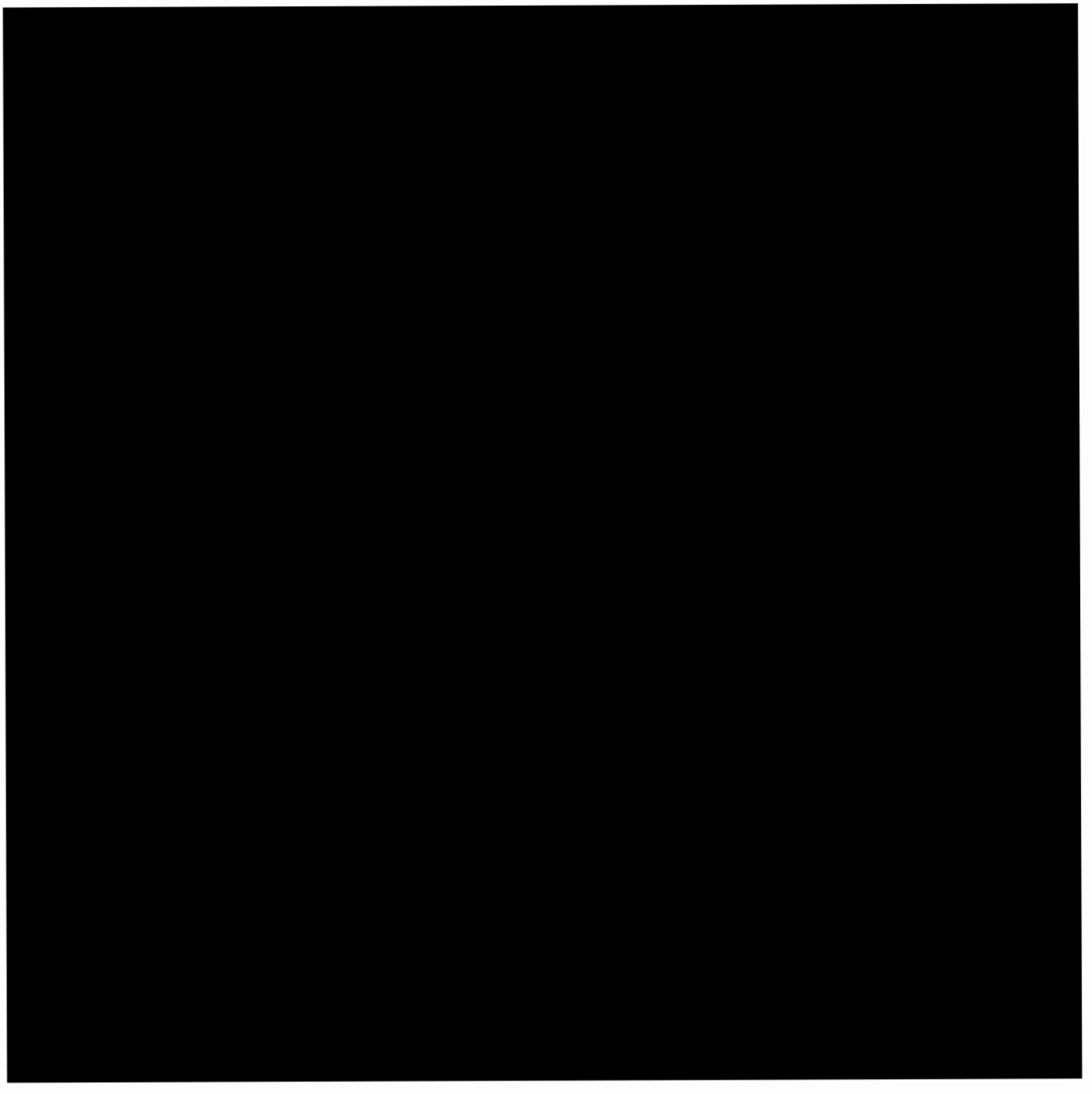


~~TOP SECRET//HCS//COMINT//NOFORN~~

[redacted]

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





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

[redacted]

[redacted]

[55] Because electronic communications will [redacted]

[redacted]

[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

EXHIBIT B

Declassified by James R. Clapper, DNI, on October 17, 2014

~~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 14-125

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: ~~12 September 2039~~

Declassified by James R. Clapper, DNI, on October 17, 2014

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 14-67 and its predecessors. [50 U.S.C. § 1861(c)(1)]

Accordingly, the Court finds that the application of the United States to obtain

Declassified by James R. Clapper, DNI, on October 17, 2014

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]

[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).

Declassified by James R. Clapper, DNI, on October 17, 2014

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 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 or has received as a result of this Order or predecessor Orders of this Court requiring the production to NSA of telephony metadata pursuant to 50 U.S.C. § 1861, NSA shall strictly adhere to the minimization procedures set out at subparagraphs A. through G. below; provided, however, that the Government may take such actions as are permitted by the Opinion

Declassified by James R. Clapper, DNI, on October 17, 2014

and Order of this Court issued on March 12, 2014, in docket number BR 14-01, subject to the conditions and requirements stated therein, including the requirement to notify this Court promptly of any material developments in civil litigation pertaining to such telephony metadata.

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

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.[2] The BR metadata shall carry unique markings such that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to 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

[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 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.

Declassified by James R. Clapper, DNI, on October 17, 2014

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, 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

[4] [redacted]

Declassified by James R. Clapper, DNI, on October 17, 2014

the requirements of subparagraph (3)C below.

C. The government may request, by motion and on a case-by-case basis, permission from the Court for NSA[5] to use specific selection terms that satisfy the reasonable articulable suspicion (RAS) standard[6] as "seeds" to query the BR metadata

[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.

[6] The reasonable articulable suspicion standard is met when, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [redacted]; provided, however, that any selection term reasonably believed to be used by a United States (U.S.) person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution. [redacted]

Declassified by James R. Clapper, DNI, on October 17, 2014

to obtain contact chaining information, within two hops of an approved "seed", for purposes of obtaining foreign intelligence information. In addition, the Director or Acting Director of NSA may authorize the emergency querying of the BR metadata

[redacted]

Declassified by James R. Clapper, DNI, on October 17, 2014

with a selection term for purposes of obtaining foreign intelligence information, within two hops of a "seed", if: (1) the Director or Acting Director of NSA reasonably determines that an emergency situation exists with respect to the conduct of such querying before an order authorizing such use of a selection term can with due diligence be obtained; and (2) the Director or Acting Director of NSA reasonably determines that the RAS standard has been met with respect to the selection term.[7] In any case in which this emergency authority is exercised, the government shall make a motion in accordance with the Primary Order to the Court as soon as practicable, but not later than 7 days after the Director or Acting Director of NSA authorizes such query.[8]

(i) Any submission to the Court under this paragraph shall, at a minimum, specify the selection term for which query authorization is sought or was granted, provide the factual basis for the NSA's belief that the reasonable articulable suspicion

---

[7] Before an emergency query is performed under this authority, NSA's Office of General Counsel (OGC), in consultation with the Director or Acting Director shall confirm 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.

[8] In the event the Court denies such motion, the government shall take appropriate remedial steps, including any steps the Court may direct.

Declassified by James R. Clapper, DNI, on October 17, 2014

standard has been met with regard to that selection term and, if such query has already taken place, a statement of the emergency necessitating such query. [9]

(ii) NSA shall ensure, through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved.[10] Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.[11]

(iii) The Court's finding that a selection term is associated with [redacted] shall be effective for: one hundred eighty days for any selection term

[9] For any selection term that is subject to ongoing Court- authorized electronic surveillance, pursuant to 50 U.S.C. § 1805, based on this Court's finding of probable cause to believe that the selection term is being used or is about to be used by agents of [redacted], including those used by U.S. persons, the government may use such selection terms as "seeds" during any period of ongoing Court-authorized electronic surveillance without first seeking authorization from this Court as described herein. Except in the case of an emergency, NSA shall first notify the Department of Justice, National Security Division of its proposed use as a seed any selection term subject to ongoing Court-authorized electronic surveillance.

[10] The Court understands that NSA has implemented technical controls, which preclude any query for intelligence analysis purposes with a non-RAS-approved seed.

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

Declassified by James R. Clapper, DNI, on October 17, 2014

reasonably believed to be used by a U.S. person; and one year for all other selection terms.[12,13]

(iv) Queries of the BR metadata using RAS-approved selection terms for purposes of obtaining foreign intelligence information may occur by manual analyst query only. Queries of the BR metadata to obtain foreign intelligence information shall return only that metadata within two "hops" of an approved seed.[14]

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

[12] The Court understands that from time to time the information available to NSA will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, the government's submission shall specify the time frame for which the selection term is or was associated with [redacted]. In the event that the RAS standard is met, analysts conducting manual queries using that selection term shall properly minimize information that may be returned within query results that fall outside of that timeframe.

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

[14] The first "hop" from a seed returns results including all identifiers (and their associated metadata) with a contact and/or connection with the seed. The second "hop" returns results that include all identifiers (and their associated metadata) with a contact and/or connection with an identifier revealed by the first "hop."

Declassified by James R. Clapper, DNI, on October 17, 2014

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 personnel (1) in order to enable them to determine whether the information contains

---

[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.

Declassified by James R. Clapper, DNI, on October 17, 2014

exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions. Notwithstanding the above requirements, NSA may share the results from intelligence analysis queries of the BR metadata, including United States person information, with Legislative Branch personnel to facilitate lawful oversight functions.

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

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

(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

Declassified by James R. Clapper, DNI, on October 17, 2014

maintain records of all such training.[17] OGC shall provide NSD/DoJ with copies of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

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

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this 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.

---

[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.

Declassified by James R. Clapper, DNI, on October 17, 2014

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

(vi) Prior to implementation of any automated query processes, such processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA, other than Executive Branch or Legislative Branch personnel receiving such results for their purposes that are exempted from the dissemination requirements of paragraph (3)D above. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call

Declassified by James R. Clapper, DNI, on October 17, 2014

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.

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

09-11-2014 P04:50

Signed _____ Eastern Time
Date Time

RAYMOND J. DEARIE
Judge, United States Foreign
Intelligence Surveillance Court