

In the
**United States Foreign Intelligence
Surveillance Court of Review**

IN RE: CERTIFICATION OF QUESTIONS OF LAW TO THE FOREIGN
INTELLIGENCE SURVEILLANCE COURT OF REVIEW

Upon Certification for Review by the United States
Foreign Intelligence Surveillance Court

AMICUS APPENDIX

PROFESSOR LAURA K. DONOHUE
AGNES N. WILLIAMS RESEARCH PROFESSOR
Georgetown University Law Center
600 New Jersey Avenue, NW
Washington, D.C. 20001
Tel: (202) 662-9455
Fax: (202) 662-9444
lkdonohue@law.georgetown.edu

February 23, 2018

TABLE OF CONTENTS TO AMICUS APPENDIX

	Tab	Page
Summary Chart	A	
Declassified & Redacted FISC/FISCR Opinions		1
Summary Chart	B	
Declassified & Redacted FISC Orders		18
Certification and En Banc Opinion and Dissent	C	
<i>Order, In re Certification of Questions of Law to the Foreign Intelligence Surveillance Court of Review, No. 18-01 (FISA Ct. Rev. Jan. 9, 2018)</i>		31
<i>Op., In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act, No. Misc. 13-08 (FISA Ct. Nov. 9, 2017)</i>		33
<i>Dissent, In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act, No. Misc. 13-08 (FISA Ct. Nov. 9, 2017)</i>		51
Collyer Opinion	D	
<i>Op. and Order, In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act, No. Misc. 13-08 (FISA Ct. Jan. 25, 2017)</i>		77
Briefs from Below	E	
<i>United States Legal Br. to the En Banc Ct., In re Opinions of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act, No. Misc. 13-08 (FISA Ct. Apr. 17, 2017)</i>		120
<i>United States' Resp. to Movant's En Banc Opening Br., In re Opinions of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act, No. Misc. 13-08 (FISA Ct. May 1, 2017)</i>		133

United States’ Opp’n to the Mot. of the ACLU et al., for the Release of Court Records, <i>In re Opinions of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act</i> , No. Misc. 13-08 (FISA Ct. Dec. 6, 2013)	140
Four Opinions to Which Access is Being Sought	F
Mem. Op., [REDACTED], No. PR/TT [REDACTED] (FISA Ct.) (Bates, J.) [Bates Mem. Op.]	149
Op. and Order, [REDACTED], No. PR/TT [REDACTED] (FISA Ct.) (Kollar-Kotelly, J.) [Kollar-Kotelly Op.]	266
Mem. Op. and Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 13-158 (FISA Ct. Oct. 11, 2013) (McLaughlin, J.) [McLaughlin Mem. Op.]	353
Amend. Mem. Op. and Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 13-109 (FISA Ct. Aug. 29, 2013) (Eagan, J.) [Eagan Mem. Op.]	376
Additional (Cited) Declassified & Redacted Opinions & Orders	G
Mem. Op., <i>In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act</i> , No. 105B(g): 07-01, (FISA Ct. Apr. 25, 2008)	422
Suppl. Op., <i>In re Production of Tangible Things From [REDACTED]</i> , No. BR 08-13 (FISA Ct. Dec. 12, 2008) [Suppl. Op. 2008]	520
Order, <i>In re [REDACTED]</i> , No. [REDACTED] (FISA Ct. May 31, 2007) (Vinson, J.)	525
Order and Mem. Op., <i>In re [REDACTED]</i> , No. [REDACTED] (FISA Ct. Apr. 3, 2007)	554
Primary Order, [REDACTED], No. PR/TT [REDACTED] (FISA Ct.) (Walton, J.)	576
Mem. Op. and Order, [REDACTED] (FISA Ct. 2009) (Hogan, J.)	591

Suppl. Op. and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things [REDACTED]</i> , No. BR 09-15 (FISA Ct. Nov. 5, 2009) (Walton, J.)	607
Suppl. Op. and Amend. to Primary Order, <i>[REDACTED]</i> (FISA Ct.) (Bates, J.)	614
Order and Mem. Op., <i>In re Proceedings Required by Section 702(i) of the FISA Amendments Act of 2008</i> , No. Misc. 08-01 (FISA Ct. Aug. 27, 2008) (McLaughlin, J.)	626
Op. on Mot. for Disclosure of Prior Decisions, <i>[REDACTED]</i> (FISA Ct. 2014) (Collyer, J.)	637
Mem. Op., <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 14-96 (FISA Ct. June 19, 2014) (Zagel, J.)	647
Op. and Order, <i>[REDACTED]</i> , Nos. <i>[REDACTED]</i> (FISA Ct. May 13, 2011) (Scullin, J.)	677

**Summary Chart: Declassified & Redacted FISC/FISCR Opinions
with Holdings, Findings, and Matters of Law**

Index No.	Doc. Date	Release Date	Document Name and Location Online	Holding, Findings, and Matters of Law
1.	Nov. 9, 2017	Nov. 9, 2017	Opinion, <i>In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act</i> , No. Misc. 13-08 (FISA Ct. Nov. 9, 2017) (En Banc Op.), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-08%20Opinion%20November%209%202017.pdf .	Holding that ACLU and Media Freedom and Information Access Clinic have standing, having sufficiently alleged the invasion of a legally cognizable interest as necessary to establish an injury-in-fact
2.	Apr. 26, 2017	May 11, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016 Cert FISC Memo Opin Order Apr 2017.pdf .	Holding that 2016 certifications, as amended by 2017 amendments, comply with 50 U.S.C. §§1881a(d)-(e) and are consistent with the Fourth Amendment
3.	Jan. 25, 2017	Jan. 25, 2017	Opinion and Order, <i>In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act</i> , No. Misc. 13-08 (FISA Ct. Jan. 25, 2017) (Collyer, J.), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-08%20Opinion%20and%20Order%200.pdf .	Dismissing motion of ACLU and Media Freedom and Access Clinic to release court records on grounds of a lack of jurisdiction
4.	Apr. 14, 2016	Aug. 22, 2016	Opinion, <i>In re Certified Question of Law</i> , No. 16-01 (FISA Ct. Rev. Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%202016-01.pdf .	Authorizing collection of post-cut-through digits under a PR/TT order in the absence of reasonably available technology to distinguish between content and non-content DRAS, subject to a prohibition on the affirmative investigative use of content

5.	Dec. 31, 2015	Apr. 19, 2016	Memorandum Opinion, <i>In re Application of the Federal Bureau of Investigation for Orders Requiring the Production of Call Detail Records</i> , No. [REDACTED] (FISA Ct. Dec. 31, 2015), https://www.dni.gov/files/documents/12312015BR_Memo_Opinion_for_Public_Release.pdf .	Concluding that the Verified Application for Orders Requiring the Production of Call Detail Records meets the requirements of subsection (a) and (b) of §501 of FISA, and that minimization procedures submitted in accordance with §501(b)(2)(D) meet the definition of minimization procedures adopted pursuant to §501(g)
6.	Nov. 24, 2015	Dec. 2, 2015	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 15-99 (FISA Ct. Nov. 24, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR_15-99_Opinion_and_Order.pdf .	Authorizing (a) continued collection of bulk telephony metadata under §215 as amended by the USA Freedom Act until Nov. 28, 2015, and (b) retention of certain BR metadata for litigation
7.	Nov. 6, 2015	Apr. 19, 2016	Memorandum Opinion and Order, [REDACTED] (FISA Ct. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf .	Approving NSA §702 certifications, amended certifications, and accompanying targeting and minimization procedures, and rejecting amicus curiae Amy Jeffress's constitutional concerns regarding the querying of data using U.S. persons' information
8.	June 29, 2015	July 2, 2015	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things</i> , Nos. BR 15-75 / Misc. 15-01 (FISA Ct. June 29, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR_15-75_Misc_15-01_Opinion_and_Order_0.pdf .	Authorizing continued collection of bulk telephone metadata under §215 for 180 days until the USA Freedom Act takes effect
9.	June 18, 2015	Apr. 19, 2016	Memorandum Opinion, <i>In re [REDACTED] a U.S. Person</i> , No. PR/TT 15-52 (FISA Ct. June 18, 2015),	Finding "notwithstanding the novel question presented by the application," the appointment of amicus curiae was not

			https://www.dni.gov/files/documents/06182015_PR-TT_Opinion_for_Public_Release.pdf .	appropriate as (a) amici had not yet been designated; and (b) there was not enough time for meaningful participation
10.	June 17, 2015	June 19, 2015	Memorandum Opinion, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things</i> , Nos. BR 15-77, 15-78 (FISA Ct. June 17, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR15-77_15-78_Memorandum_Opinion.pdf .	Finding it unnecessary to appoint an amicus curiae, as the question before the court is a matter of statutory interpretation for which “only a single reasonable or rational outcome” exists; and determining that the USA FREEDOM Act reinstated the §215 BR provision of the PATRIOT Act that had lapsed on June 1, 2015
11.	Aug. 26, 2014	Sept. 29, 2015	Memorandum Opinion and Order, [REDACTED] (FISA Ct. Aug. 26, 2014), https://www.dni.gov/files/documents/0928/FISC_Memorandum_Opinion_and_Order_26_August_2014.pdf .	Approving §702 certifications
12.	Aug. 11, 2014	Apr. 11, 2017	Opinion and Order, <i>In Re Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act</i> , Nos. Multiple including [REDACTED] (FISA Ct. Aug. 11, 2014), https://www.dni.gov/files/documents/icotr/51117/Doc%2020%E2%80%9320Aug.%202014%20FISC%20Opinion%20&%20Order%20re%20FBI%E2%80%99s%20Minimization%20Procedures.pdf .	Granting government motion to amend the standard minimization procedures for the purpose of disseminating information to the National Center for Missing and Exploited Children (NCMEC) for a law enforcement purpose, and to amend the retention provisions to exempt information retained for litigation-related reasons
13.	Aug. 7, 2014	Aug. 8, 2014	Opinion and Order, <i>In re Orders of this Court Interpreting Section 215 of the Patriot Act</i> , No. Misc. 13-02 (FISA Ct. Aug. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-7.pdf .	Ordering declassification of a redacted version of the Feb. 19, 2013 FISC opinion in No. BR-25 and finding that the second redaction proposal passes muster

14.	June 19, 2014	June 27, 2014	Memorandum Opinion, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 14-96 (FISA Ct. June 19, 2014) (Zagel, J.), http://www.fisc.uscourts.gov/sites/default/files/BR%2014-96%20Opinion-1.pdf .	Approving new minimization procedures, “fully agree[ing] with and adopt[ing] the constitutional and statutory analyses contained in” previous court opinions, and authorizing collection of bulk telephone metadata under §215
15.	Mar. 21, 2014	Apr. 15, 2014	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things</i> , No. BR 14-01 (FISA Ct. Mar. 21, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR14-01 Opinion-3.pdf .	Granting the motion of the plaintiffs in <i>Jewel v. NSA</i> and <i>First Unitarian Church v. NSA</i> for leave to correct the record, and ordering the government to make a filing explaining its failure to notify FISC of the March 10, 2014 preservation orders in <i>Jewel</i> and <i>First Unitarian</i> and the plaintiffs’ understanding of the scope of the orders, upon learning that counsel considered them relevant to the §215 telephony metadata at issue in FISC’s Feb. 25 Opinion and Order (which had denied extended preservation of §215 records for litigation purposes)
16.	Mar. 20, 2014	Apr. 28, 2014	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things</i> , No. BR 14-01 (FISA Ct. Mar. 20, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR14-01 Opinion and Order-1.pdf .	Declining a petition filed by [REDACTED] “to vacate, modify, or reaffirm” a Jan. 3, 2014 production order
17.	Mar. 12, 2014	Apr. 15, 2014	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things</i> , No. BR 14-01 (FISA Ct. Mar. 12, 2014),	Granting Mar. 11, 2014 motion for temporary relief from five-year data destruction rule pending resolution of

			http://www.fisc.uscourts.gov/sites/default/files/BR14-01 Opinion-2.pdf .	preservation issues raised in <i>Jewel v. NSA</i> and <i>First Unitarian Church v. NSA</i>
18.	Mar. 7, 2014	Apr. 15, 2014	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things</i> , No. BR 14-01 (FISA Ct. Mar. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR14-01 Opinion-1.pdf .	Denying government motion for a second amendment to the Jan. 3, 2014 primary order approving §215 collection, seeking to retain telephony metadata beyond five years for purposes of pending civil litigation
19.	[REDACTED] (2014)	June 13, 2017	Opinion on Motion for Disclosure of Prior Decisions, [REDACTED] (FISA Ct. 2014), https://www.dni.gov/files/documents/icotr/702/EFF%202016--CV--02041(HSG)%20Doc%2012%2006.13.17%20--%20REDACTED.PDF .	Denying motion for disclosure of prior FISC decisions on the grounds that “neither FISA nor the ...[FISC] Rules of Procedure...require, or provide for discretionary, disclosure of the Requested Opinions in the circumstances of this case,” and determining that the Due Process Clause of the Fifth Amendment “does not compel the requested disclosure.”
20.	[REDACTED] (2014)	June 13, 2017	Memorandum Opinion and Order, [REDACTED] (FISA Ct. 2014), https://www.dni.gov/files/documents/icotr/702/Bates%20510-548.pdf .	Holding that the 2014 Directives meet the requirements of §702 and are otherwise lawful, including inter alia, that they are consistent with the Fourth Amendment as there is no “distinctive or heightened risk of the government acquiring any greater volume of communications of or concerning United States persons”; comparing context to <i>In re Directives</i>
21.	Dec. 18, 2013	Apr. 15, 2014	Memorandum Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things</i> , No. BR 13-158 (FISA Ct. Dec. 18, 2013),	Granting motion by the Center for National Security Studies to file an amicus brief on why §215 does not authorize bulk collection of telephony metadata records,

			http://www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Memorandum-2.pdf .	and denying motions for reconsideration or en banc review, access to the government’s application or the FISC docket, and declassification of relevant legal arguments on the grounds that “information already made available to the public, including opinions of his Court, provides sufficient context for the Center to brief the issue specified herein.”
22.	Dec. 13, 2013	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. Dec. 13, 2013), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2015%2006.13.17%20--%20REDACTED.PDF .	Holding that the Nov. 15, 2013 amended minimization procedures are consistent with the requirements of 50 U.S.C. §§1881a(d)-(e) and the Fourth Amendment
23.	Oct. 11, 2013	Apr. 15, 2014	Memorandum Opinion and Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 13-158 (FISA Ct. Oct. 11, 2013) (McLaughlin, J.), http://www.fisc.uscourts.gov/sites/default/files/BR13-158 Memorandum-1.pdf .	Authorizing bulk metadata collection and agreeing with Judge Eagan’s July 2013 Mem. Op. in BR 13-109 that collection of bulk telephone metadata meets the §215 relevance standard; holding, under <i>Smith v. Maryland</i> , that the Fourth Amendment is inapplicable
24.	Sept. 13, 2013	Apr. 16, 2014	Opinion and Order, <i>In re Orders of this Court Interpreting Section 215 of the Patriot Act</i> , No. Misc. 13-02 (FISA Ct. Sept. 13, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc13-02 Order-2.pdf .	Ruling on ACLU motion to release FISC opinions: motion denied with respect to records that are part of ongoing FOIA litigation; government ordered to conduct declassification review of other opinions
25.	Aug. 30, 2013	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. Aug. 30, 2013), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2003%2006.13.17%20--%20REDACTED.PDF .	Holding that the certifications included as part of the July 31, 2012 submission contain the required statutory elements and that the targeting and minimization procedures adopted for use in connection

				with those certifications are consistent with the applicable statutory requirements and the Fourth Amendment, but, because of a recently-disclosed compliance incident under investigation by the government, suspending its review of amendments to previously-approved certifications also part of the July 31 submission
26.	Aug. 29, 2013	Sept. 17, 2013	Amended Memorandum Opinion and Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 13-109 (FISA Ct. Aug. 29, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR13-109 Order-1.pdf .	Granting the application for bulk telephony metadata collection, holding that “ <i>Smith v. Maryland</i> ” compels the conclusion that there is no Fourth Amendment impediment to the collection,” comparing §215 to the Stored Communications Act, and determining that bulk collection meets the “relevance” standard under 50 U.S.C. §1842(c)(2) as relevant records would be contained in the bulk data
27.	June 12, 2013	Apr. 15, 2014	Opinion and Order, <i>In re Motion for Consent to Disclosure of Court Records or, in the Alternative, A Determination of the Effect of the Court’s Rules on Statutory Access Rights</i> , No. 13-01 (FISA Ct. June 12, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc13-01 Opinion-1.pdf .	Finding, contrary to the Government’s argument in District Court that FISC rules prevent the District Court from ordering disclosure of a FISC opinion if it is found to be subject to FOIA, that the District Court has the authority to do so
28.	Feb. 19, 2013; redacted version filed Aug. 27, 2014	Aug. 28, 2014	Opinion, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 13-25 (FISA Ct. Feb. 19, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR13-25 Opinion-1.pdf .	Finding that the application submitted by the government in support of an FBI investigation of a USP meets the statutory First Amendment requirement as well as the language requiring that the tangible things sought are relevant to an authorized

				investigation to protect against international terrorism
29.	Sept. 25, 2012	Aug. 21, 2013	Memorandum Opinion, [REDACTED] (FISA Ct. Sept. 25, 2012), http://www.dni.gov/files/documents/September2012BatesOpinionandOrder.pdf .	Noting that in 2011 “the government made a series of submissions to the Court disclosing that it had materially misrepresented the scope of NSA’s ‘upstream collection’ under §702 (and prior authorities including the Protect America Act),” and determining that new measures adopted by the NSA to purge data from past overcollection were sufficient to make the program legal
30.	[REDACTED] (2012)	June 13, 2017	Memorandum Order and Opinion, [REDACTED] (FISA Ct. 2012), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2007%2006.13.17%20--%20REDACTED%20w%20replacemnt%20page.pdf .	Holding that the NSA’s amended minimization procedures used in this case, permitting the sharing of certain unminimized communications, are consistent with the requirements of 50 U.S.C. §§1881a(d)-(e) and with the Fourth Amendment
31.	Nov. 30, 2011	Aug. 21, 2013	Memorandum Opinion, [REDACTED] (FISA Ct. Nov. 30, 2011), http://www.dni.gov/files/documents/November2011BatesOpinionandOrderPart1.pdf (Part 1) and http://www.dni.gov/files/documents/November2011BatesOpinionandOrderPart2.pdf (Part 2).	Approving amended minimization procedures adopted to correct the statutory and constitutional deficiencies identified by the Court in its Oct. 3, 2011 Mem. Op. and restarting §702 upstream collection
32.	Oct. 3, 2011	Aug. 21, 2013	Memorandum Opinion, [REDACTED], 2011 WL 10945618 (FISA Ct. Oct. 3, 2011), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and-Order-20140716.pdf .	Holding that the NSA misled the Court on the nature of §702 upstream collection, acquiring tens of thousands entirely domestic communications of USPs and that the minimization procedures failed on

				statutory and constitutional (Fourth Amendment) grounds (Bates, J.)
33.	May 13, 2011	Jan. 31, 2018	Opinion and Order, <i>[REDACTED]</i> , Nos. <i>[REDACTED]</i> (FISA Ct. May 13, 2011), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-10.pdf .	Directing the government to destroy information obtained by unauthorized electronic surveillance
34.	Dec. 10, 2010	Jan. 31, 2018	Opinion and Order, <i>[REDACTED]</i> , Nos. <i>[REDACTED]</i> (FISA Ct. Dec. 10, 2010), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-11.pdf .	Ordering the government to submit further information regarding its proposed retention and use of the results of unauthorized surveillance
35.	[REDACTED] (2010)	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. 2010), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2013%2006.13.17%20--%20REDACTED.PDF .	Holding that the targeting and minimization procedures used in this case are consistent with the requirements of 50 U.S.C. §§1881a(d)-(e) and with the Fourth Amendment; noting government noncompliance in relation to purging domestic U.S. communications and subsequent NSA dissemination of intelligence reports containing the data that should have been purged; and finding that the NSA's process for purging §702 communications is consistent with its targeting and minimization procedures
36.	[REDACTED] (2010)	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. 2010), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2004%2006.13.17%20--%20REDACTED_updatedf.pdf .	Holding that the targeting and minimization procedures used in this case are consistent with the requirements of 50 U.S.C. §§1881a(d)-(e) and the Fourth Amendment

37.	[REDACTED] (2010)	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. 2010), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2002%2006.13.17%20--%20REDACTED_updated.pdf .	Holding that the targeting and minimization procedures used in this case are consistent with the requirements of 50 U.S.C. §§1881a(d)-(e) and the Fourth Amendment
38.	[REDACTED]	Nov. 18, 2013	Memorandum Opinion, <i>[REDACTED]</i> , No. PR/TT [REDACTED] (FISA Ct.) (Bates, J.), https://www.dni.gov/files/documents/1118/CLEANEDPRTT_2.pdf .	Granting in part and denying in part an application to engage in bulk Internet metadata collection and to query and use information previously obtained by NSA and noting, “the government acknowledges that NSA exceeded the scope of authorized acquisition continuously during the more than [REDACTED] years of acquisition under these orders.” (Bates Mem. Op.)
39.	Nov. 5, 2009	Sept. 10, 2013	Supplemental Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 09-15 (FISA Ct. Nov. 5, 2009), http://www.dni.gov/files/documents/section/pub_No_v_5_2009_Supplemental_Opinion_and_Order.pdf .	Noting noncompliance of NSA sharing of information requirements (NSA had created an email distribution list with 189 analysts, only 53 of whom had the adequate training and guidance and to whom BR metadata query results were sent); reiterating the manner in which query results may be shared within NSA; and elaborating on the reporting requirement imposed by the Court’s Oct. 30, 2009 order (Walton, J.)
40.	Apr. 7, 2009	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. Apr. 7, 2009), https://www.dni.gov/files/documents/icotr/702/Bates%20549-579.pdf .	Holding §702 targeting and minimization procedures used in this case are consistent with the requirements of 50 U.S.C. §§1881a(d)-(e) and with the Fourth Amendment, noting that in 2008 the government reported overcollection, and determining that preventative and remedial

				measures to limit overcollection incidents adequately protects Fourth Amendment interests
41.	[REDACTED] (2009)	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. 2009), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2011%2006.13.17%20--%20REDACTED.PDF .	Holding that the targeting and minimization procedures used in this case are consistent with the requirements of 50 U.S.C. §§1881a(d)-(e) and with the Fourth Amendment, recognizing that continued NSA noncompliance problems “principally involve analysts improperly acquiring the communications of U.S. persons, suggesting that the CIA problem is “arguably more troubling because it reflects a profound misunderstanding of minimization procedures,” recognizing that the government’s practice (unbeknownst to the Court) had been to report only certain noncompliance incidents and not others (such as failure to de-task accounts even after NSA learned that the targets entered the U.S.); and noting that the government must report to the Court every compliance incident that relates to the operation of the targeting or minimization procedures [NB: similar to No. 42, below, with slightly different language and redactions]
42.	[REDACTED] (2009)	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. 2009), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2005%2006.13.17%20--%20REDACTED.PDF .	[Almost entirely consistent language and redactions to item 41, but with some slight differences]

43.	Dec. 12, 2008	Sept. 10, 2013	Supplemental Opinion, <i>In re Production of Tangible Things From [REDACTED]</i> , No. BR 08-13 (FISA Ct. Dec. 12, 2008), https://www.dni.gov/files/documents/section/pub_Dec_12_2008_Supplemental_Opinions_from_the_FISC.pdf .	Concluding that call detail records are subject to production under 50 U.S.C. §1861; addressing tension with 18 U.S.C. §§2702-2703 (relevant provisions of Electronic Communications Privacy Act)
44.	[REDACTED] (2008)	June 13, 2017	Memorandum Order and Opinion, <i>[REDACTED]</i> (FISA Ct. 2008), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2001%2006.13.17%20--%20REDACTED%20w%20replacemnt%20page.pdf .	Holding §702 targeting and minimization procedures used in this case are consistent with the requirements of 50 U.S.C. §§1881a(d)-(e) and with the Fourth Amendment; referencing a Sept. 4, 2008 Memorandum Opinion and accompanying Order [which has not been released]
45.	Aug. 27, 2008	Aug. 27, 2008	Order and Memorandum Opinion, <i>In re Proceedings Required by Section 702(i) of the FISA Amendments Act of 2008</i> , No. Misc 08-01 (FISA Ct. Aug. 27, 2008), http://www.fas.org/irp/agency/doj/fisa/fisc082708.pdf .	Denying ACLU's motion (a) to be notified of the caption and briefing schedule for any proceedings under §702(i) in which the Court would consider legal questions relating to the scope, meaning, and constitutionality of the FAA; (b) that the Government be required to file public versions of its legal briefs with selective redactions; (c) that the ACLU be granted leave to file a legal brief addressing the constitutionality of the FAA and to participate in oral argument before the Court; and (d) that any legal opinions issued by the Court be made available to the public, with only the redactions necessary to protect information properly classified; and citing the Aug. 9, 2007 determination that (1) the common law and (2) the First Amendment provide no public

				right of access because the records being sought, although different from the earlier case, are subject to the same comprehensive statutory scheme
46.	Aug. 22, 2008	Jan. 15, 2009	<i>In re Directives to Yahoo! Inc. Pursuant to Section 105B of Foreign Intelligence Surveillance Act</i> , 551 F.3d 1004 (FISA Ct. Rev. 2008), http://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf .	FISCR holding that petitioner easily exceeded the threshold for standing; determining that the directives issued to communications service providers under the PAA, requiring production of customers' data, were consistent with the statutory framing and the Fourth Amendment (as applied); and finding a Warrant Clause exception akin to the "special needs" exception for domestic foreign intelligence collection targeted at FPs/AFP outside the United States
47.	Apr. 25, 2008	Sept. 11, 2014	Memorandum Opinion, <i>In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act</i> , No. 105B(g): 07-01 (Walton, J.), https://cdt.org/files/2014/09/38-yahoo702-memorandum-opinion-unredacted.pdf	Holding that the court retained jurisdiction despite the lapse of the PAA; determining that the directives served on Yahoo! met the PAA statutory requirements and the Fourth Amendment; and finding that service providers can bring Fourth

				Amendment challenges on behalf of their customers
48.	Jan. 15, 2008	Sept. 11, 2014	Memorandum Opinion and Order, <i>[REDACTED]</i> , (FISA Ct. 2008), https://www.dni.gov/files/documents/0909/Memorandum%20Opinion%20and%20Order%2020080115.pdf	Considering DNI/AG certification related to Yahoo! PRISM case under a “clearly erroneous” standard of review; discussing PAA
49.	Dec. 11, 2007	Dec. 11, 2007	Memorandum Opinion, <i>In re Motion for Release of Court Records</i> , 526 F. Supp. 2d 484 (FISA Ct. 2007), https://www.aclu.org/sites/default/files/pdfs/safefree/fisc_order_2007_1211.pdf .	Finding ACLU motion within FISC’s jurisdiction; denying motion for release of Court orders and government pleadings regarding §702 on common law and First Amendment right of access grounds because FISC proceedings traditionally have been closed
50.	Aug. 2, 2007	Dec. 12, 2014	Order and Memorandum Opinion, <i>In re [REDACTED]</i> , No. <i>[REDACTED]</i> (FISA Ct. Aug. 2, 2007), https://www.documentcloud.org/documents/1379006-large-content-fisa-order-documents.html .	Responding to an application to establish an early warning system to alert the government to the presence of FPs/AFP’s in the United States; noting that the new procedures “would enable the Government to direct electronic surveillance with a much higher degree of speed and agility than would be possible through the filing of individual FISA applications,”; establishing probable cause that the targets are FPs/AFP’s and using/about to use the facilities; clarifying at what point the NSA is deemed to have obtained knowledge of a facility for the purposes of the May 31, 2007 order
51.	Apr. 3, 2007	Dec. 12, 2014	Order and Memorandum Opinion, <i>In re [REDACTED]</i> , No. <i>[REDACTED]</i> (FISA Ct. Apr.	Rejecting the definition of “facility” from the Jan. 10, 2007 foreign content order;

			3, 2007), https://www.dni.gov/files/documents/1212/CERTIFIED_COPY - Order and Memorandum Opinion 04 03 07 12-11 Redacted.pdf .	finding that probable cause findings for selectors must be made by FISC, not the NSA
52.	[REDACTED]	Nov. 18, 2013	Opinion and Order, <i>[REDACTED]</i> , No. PR/TT [REDACTED] (FISA Ct.) (Kollar-Cotelly, J.), https://www.odni.gov/files/documents/1118/CLEAN_EDPRTT 1.pdf .	Holding bulk Internet metadata collection is consistent with 50 U.S.C. §§1841-1846, that the restrictions on retention, accessing, use, and dissemination of the information satisfies the requirements of 50 U.S.C.§1842, and that the installation and use of the PR/TT devices for bulk email and Internet metadata collection is consistent with the First and Fourth Amendments, despite the acknowledgment that “The raw volume of the proposed collection is enormous,” and will result in the collection of USPs inside the country “who are not the subject of any FBI investigation” (internal quotations omitted) (Kollar-Kotelly Op.)
53.	Nov. 18, 2002	N/A	<i>In re Sealed Case</i> , 310 F.3d 717 (FISA Ct. Rev. 2002), https://scholar.google.com/scholar_case?case=14926646895729978023&q=310+F.3d+717+&hl=en&as_sdt=20006 .	Bringing down the wall; overturning the FISA Ct. ruling (below); allowing foreign intelligence searches to be used even when the primary purpose of the collection is a criminal investigation
54.	May 17, 2002	N/A	<i>In re All Matters Submitted to Foreign Intelligence Surveillance Court</i> , 218 F. Supp. 2d 611 (FISA Ct. 2002) (reversed by <i>In re Sealed Case</i>), https://scholar.google.com/scholar_case?case=16515626632671842776&q=218+F.+Supp.+2d+611+&hl=en&as_sdt=20006 .	Holding that minimization procedures must prevent prosecutors from directing foreign intelligence searches (re-building the wall)

55.	June 11, 1981	June 11, 1981	<i>In re Application of the United States for an Order Authorizing the Physical Search of Nonresidential Premises and Personal Property</i> (FISC Ct. June 11, 1981), reprinted in S. Rep. No. 97-280 at 16-19 (1981)	Holding that the electronic search provisions of the 1978 FISA do not authorize FISC to issue orders for search of real property
56.	[REDACTED]	Sept. 25, 2017	Supplemental Opinion and Amendment to Primary Order, [REDACTED] (FISA Ct.) (Bates, J.), https://www.dni.gov/files/documents/icotr/EFF%20FOIA%20Sep%2025%20Doc%209.pdf .	Responding to government request for clarification in previous Mem. Op., which limited collection authority for several categories of metadata collection under PR/TT
57.	[REDACTED]	Jan. 31, 2018	Memorandum Opinion, [REDACTED] (FISA Ct.) (Hogan, J.), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-13.pdf .	Holding that the particular type of surveillance requested constitutes “electronic surveillance” as defined in FISA
58.	[REDACTED]	Jan. 31, 2018	Opinion, [REDACTED] (FISA Ct.) (Broomfield, J.), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-8.pdf .	[Labeled as an opinion but almost entirely redacted]
59.	[REDACTED]	Jan. 31, 2018	Memorandum Opinion as to Electronic Surveillance Pursuant to [REDACTED] (FISA Ct.) (Kollar-Kotelly, J.), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-4.pdf .	Heavily redacted; appears to be reporting noncompliance (“For the first time, on the evening of [REDACTED] [DOJ] orally informed this Judge that for weeks [REDACTED].” *2; noting “The Court is without jurisdiction [REDACTED].” *3; authorizing some sort of electronic surveillance

60.	[REDACTED]	Jan.31, 2018	Opinion and Order, <i>[REDACTED]</i> (FISA Ct.) (Baker, J.) https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-2.pdf .	Denying in part and granting in part the government's Motion for Reconsideration; [procedural history almost entirely redacted]; holding that the practices at issue are not moot, thus presenting the court with a live issue; citing to classified <i>In Re Electronic and Data Communications Surveillance Definitions, Memorandum of Law and Fact Regarding Electronic and Data Communications Surveillance under the Foreign Intelligence Surveillance Act</i> (Nov. 5, 2003); evaluating Fourth Amendment implications; holding that the FBI marking procedures violated the statutory minimization requirements
-----	------------	--------------	--	--

Summary Chart: Declassified & Redacted FISC Orders

Index No.	Doc Date	Release Date	Document Name and Location
1.	Jan. 9, 2018	Jan. 9, 2018	Order, <i>In re Certification of Questions of Law to the Foreign Intelligence Surveillance Court of Review</i> , No. 18-01 (FISA Ct. Rev. Jan. 9, 2018), http://www.fisc.uscourts.gov/sites/default/files/FISCR%2018%2001%20WCB%20Order%20180109_0.pdf .
2.	Jan. 5, 2018	Jan. 7, 2018	Certified Question of Law, <i>In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act</i> , No. Misc. 13-08 (FISA Ct. Jan. 5, 2018), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013%2008%20Certification%20Order%20with%20Attached%20En%20Banc%20Decision.pdf .
3.	Apr. 26, 2017	May 11, 2017	Memorandum Opinion and Order, [REDACTED] (FISA Ct. Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf .
4.	Apr. 25, 2017	Apr. 26, 2017	Order, <i>In re Unknown Foreign Intelligence Surveillance Court Orders</i> , Not Docketed (FISA Ct. Apr. 25, 2017), http://www.fisc.uscourts.gov/sites/default/files/APR%2025%20Order.pdf .
5.	Mar. 22, 2017	Mar. 22, 2017	Order, <i>In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act</i> , No. Misc. 13-08 (FISA Ct. Mar. 22, 2017), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-08%20Order.pdf .
6.	Jan. 25, 2017	Jan. 25, 2017	Opinion and Order, <i>In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act</i> , No. Misc. 13-08 (FISA Ct. Jan. 25, 2017), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-08%20Opinion%20and%20Order_0.pdf .
7.	Oct. 26, 2016	May 10, 2017	Order, [REDACTED] (FISA Ct. Oct. 26, 2016), https://www.dni.gov/files/documents/icotr/51117/2016_Certification_FISC_Extension_Order_Oct_26_2016.pdf .
8.	Apr. 27, 2016	Apr. 27, 2016	Order, <i>In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act</i> , No. 105B(g) 07-01 (FISA Ct. Apr. 27, 2016), http://www.fisc.uscourts.gov/sites/default/files/105B%28g%29%2007-01.pdf .

9.	Feb. 12, 2016	Aug. 22, 2016	Certified Question of Law, <i>In [REDACTED] A U.S. Person</i> , No. PR/TT 2016-[REDACTED] (FISA Ct. Feb. 12, 2016), https://www.dni.gov/files/icotr/PCTD%20FISC-R%20Certification%2020160818%20pdf.pdf .
10.	Nov. 24, 2015	Dec. 2, 2015	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]</i> , No. BR 15-99 (FISA Ct. Nov. 24, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR_15-99_Opinion_and_Order.pdf .
11.	Nov. 6, 2015	Apr. 19, 2016	Memorandum Opinion and Order, <i>[Redacted]</i> , No. [Redacted] (FISA Ct. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf .
12.	Sept. 17, 2015	Sept. 24, 2015	Order Appointing an Amicus Curiae, <i>Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things</i> , No. BR 15-99 (FISA Ct. Nov. 24, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR_15-99_Order_Appointing_Amicus_Curiae.pdf .
13.	Aug. 27, 2015	Aug. 28, 2015	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]</i> , No. BR 15-99 (FISA Ct. Aug. 27, 2015), https://www.dni.gov/files/documents/BR_15-99_Primary_Order.pdf .
14.	Aug. 13, 2015	Apr. 11, 2017	Order Appointing an Amicus Curiae, <i>[REDACTED]</i> , No. [REDACTED] (FISA Ct. Aug. 13, 2015), https://www.dni.gov/files/documents/icotr/51117/Doc%204%20%E2%80%93%20Aug.%202015%20FISC%20Order%20Appointing%20an%20Amicus%20Curiae.pdf .
15.	June 29, 2015	July 2, 2015	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things</i> , Nos. BR 15-75 / Misc. 15-01 (FISA Ct. June 29, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR_15-75_Misc_15-01_Opinion_and_Order_0.pdf .
16.	June 29, 2015	July 2, 2015	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things</i> , No. BR 15-75 (FISA Ct. June 29, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR_15-75_Primary_Order%28redacted%29.pdf .
17.	Feb. 26, 2015	Approved for public release,	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things</i> , No. BR 15-24 (FISA Ct. Feb. 26, 2015), https://www.dni.gov/files/documents/0311/BR_15-24_Primary_Order_-_Redacted.pdf .

		Mar. 9, 2015; Posted, Mar. 11, 2015	
18.	Dec. 4, 2014	Declassified Dec. 24, 2014; posted Jan. 12, 2015	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 14-166 (FISA Ct. Dec. 4, 2014), https://www.dni.gov/files/documents/0112/BR_14-166 Primary Order FINAL.pdf .
19.	Sept. 11, 2014	Declassified Oct. 17, 2013; posted Nov. 6, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 14-125 (FISA Ct. Sept. 11, 2014), https://www.dni.gov/files/documents/1106/BR_14-125 Primary Order.pdf .
20.	Aug. 26, 2014	Sept. 29, 2015	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. Aug. 26, 2014), https://www.dni.gov/files/documents/0928/FISC Memorandum Opinion and Order 26 August 2014.pdf .
21.	Aug. 11, 2014	Apr. 11, 2017	Opinion and Order, <i>In Re Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act</i> , Nos. Multiple including [REDACTED] (FISA Ct. Aug. 11, 2014), https://www.dni.gov/files/documents/icotr/51117/Doc%202020E2%80%93%20Aug.%202014%20FISC%20Opinion%20&%20Order%20re%20FBI%E2%80%99s%20Minimization%20Procedures.pdf .
22.	Aug. 7, 2014	Aug. 8, 2014	Opinion and Order, <i>In re Orders of this Court Interpreting Section 215 of the Patriot Act</i> , No. Misc. 13-02 (FISA Ct. Aug. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-7.pdf .
23.	June 19, 2014	June 27, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 14-96 (FISA Ct. June 19, 2014), https://www.dni.gov/files/documents/0627/BR_14-96 Primary Order.pdf .
24.	Mar. 28, 2014	June 27, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 14-67 (FISA

			Ct. Mar. 28, 2014), https://www.dni.gov/files/documents/0627/BR_14-67_Primary_Order.pdf .
25.	Mar. 21, 2014	Apr. 15, 2014	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things</i> , No. BR 14-01 (FISA Ct. Mar. 21, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR_14-01_Opinion-3.pdf .
26.	Mar. 20, 2014	Apr. 28, 2014	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things</i> , No. BR 14-01 (FISA Ct. Mar. 20, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR_14-01_Opinion_and_Order-1.pdf .
27.	Mar. 12, 2014	Apr. 15, 2014	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things</i> , No. BR 14-01 (FISA Ct. Mar. 12, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR_14-01_Opinion-2.pdf .
28.	Mar. 7, 2014	Apr. 15, 2014	Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things</i> , No. BR 14-01 (FISA Ct. Mar. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR_14-01_Opinion-1.pdf .
29.	Feb. 5, 2014	Feb. 12, 2014	Order Granting the Government's Motion to Amend the Court's Primary Order Dated January 3, 2014, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things</i> , No. BR 14-01 (FISA Ct. Feb. 5, 2014), https://www.dni.gov/files/documents/BR_14-01_MTA_and_Order_with_redactions(Final).pdf .
30.	Jan. 3, 2014	Apr. 15, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 14-01 (FISA Ct. Jan. 3, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR_14-02_Order-2.pdf .
31.	[REDACTED] (2014)	June 13, 2017	Memorandum Opinion and Order, [REDACTED] (FISA Ct. 2014), https://www.dni.gov/files/documents/icotr/702/Bates%20510-548.pdf .
32.	Dec. 18, 2013	Apr. 15, 2014	Memorandum Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things</i> , No. BR 13-158 (FISA Ct. Dec. 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Memorandum-2.pdf .
33.	Dec. 13, 2013	June 13, 2017	Memorandum Opinion and Order, [REDACTED] (FISA Ct. Dec. 13, 2013), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2015%2006.13.17%20--%20REDACTED.PDF .

34.	Oct. 11, 2013	Apr. 15, 2014	Memorandum Opinion and Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 13-158 (FISA Ct. Oct. 11, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR_13-158_Memorandum-1.pdf .
35.	Sept. 13, 2013	Apr. 16, 2014	Opinion and Order, <i>In re Orders of this Court Interpreting Section 215 of the Patriot Act</i> , No. Misc. 13-02 (FISA Ct. Sept. 13, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc_13-02_Order-2.pdf .
36.	Aug. 30, 2013	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. Aug. 30, 2013), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2003%2006.13.17%20--%20REDACTED.PDF .
37.	Aug. 29, 2013	Sept. 17, 2013	Amended Memorandum Opinion and Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED]</i> , No. BR 13-109 (FISA Ct. Aug. 29, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR_13-109_Order-1.pdf .
38.	June 12, 2013	Apr. 15, 2014	Opinion and Order, <i>In re Motion for Consent to Disclosure of Court Records or, in the Alternative, A Determination of the Effect of the Court's Rules on Statutory Access Rights</i> , No. 13-01 (FISA Ct. June 12, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc_13-01_Opinion-1.pdf .
39.	Apr. 25, 2013	June 5, 2013	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 13-80 (FISA Ct. Apr. 25, 2013), https://www.aclu.org/files/natsec/nsa/20130816/Section_215_-_Primary_Order.pdf .
40.	[REDACTED] (2012)	June 13, 2017	Memorandum Order and Opinion, <i>[REDACTED]</i> (FISA Ct. 2012), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2007%2006.13.17%20--%20REDACTED%20w%20replacemnt%20page.pdf .
41.	June 22, 2011	Jan. 17, 2014	Supplemental Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 11-107 (FISA Ct. June 22, 2011), https://www.aclu.org/files/section215/20140123/FISC_Supplemental_Order_BR_11-107.pdf .
42.	June 22, 2011	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 11-107 (FISA Ct. June 22, 2011), http://www.dni.gov/files/documents/11714/FISC_Order%20BR_11-107.pdf .

43.	May 13, 2011	Jan. 31, 2018	Opinion and Order, [REDACTED], Nos. [REDACTED] (FISA Ct. May 13, 2011), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-10.pdf .
44.	Apr. 13, 2011	Jan. 17, 2014	Supplemental Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 11-57 (FISA Ct. April 13, 2011), https://www.aclu.org/files/section215/20140123/FISC Supplemental Order BR 11-57.pdf .
45.	Apr. 13, 2011	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 11-57 (FISA Ct. April 13, 2011), http://www.dni.gov/files/documents/11714/FISC Order%2C BR 11-57.pdf .
46.	Feb. 10, 2011	Jan. 17, 2014	Amendment to Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 11-07 (FISA Ct. Feb. 10, 2011), https://www.aclu.org/files/section215/20140123/FISC Amended Order BR 11-07.pdf .
47.	Jan. 20, 2011	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 11-07 (FISA Ct. Jan. 20, 2011), http://www.dni.gov/files/documents/11714/FISC Order%2C BR 11-07.pdf .
48.	Dec. 10, 2010	Jan. 31, 2018	Opinion and Order, [REDACTED], Nos. [REDACTED] (FISA Ct. Dec. 10, 2010), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-11.pdf .
49.	[REDACTED]	Aug. 11, 2014	Primary Order, [REDACTED], No. PR/TT [REDACTED] (FISA Ct.)(Bates, J.), https://www.dni.gov/files/0808/Final 009.FISC Primary Order.pdf .
50.	Nov. 23, 2010	Mar. 28, 2014	Supplemental Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 10-82 (FISA Ct. Nov. 23, 2010), https://www.dni.gov/files/documents/0328/104. BR 10-82 supplemental opinion - Redacted 20140328.pdf .
51.	Aug. 19, 2010	June 30, 2014	Order, <i>In re DNI / AG Certification 2010-A</i> , No. 702(i)-10-02 (FISA Ct. Aug. 19, 2010), https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0194/5073f0cb.dir/doc.pdf .
52.	Oct. 29, 2010	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 10-70

			(FISA Ct. Oct. 29, 2010), http://www.dni.gov/files/documents/11714/FISC_Order%2C BR_10-70.pdf .
53.	Aug. 4, 2010	Ja. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 10-49 (FISA Ct. Aug. 4, 2010), http://www.dni.gov/files/documents/11714/FISC_Order%2C BR_10-49.pdf .
54.	May 14, 2010	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 10-17 (FISA Ct. May 14, 2010), http://www.dni.gov/files/documents/11714/FISC_Order%2C BR_10-17.pdf .
55.	Feb. 26, 2010	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 10-10 (FISA Ct. Feb. 26, 2010), http://www.dni.gov/files/documents/11714/FISC_Order%2C BR_10-10.pdf .
56.	[REDACTED] (2010)	June 13, 2017	Memorandum Opinion and Order, [REDACTED] (FISA Ct. 2010), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV- 02041(HSG)%20Doc%2013%2006.13.17%20--%20REDACTED.PDF .
57.	[REDACTED] (2010)	June 13, 2017	Memorandum Opinion and Order, [REDACTED] (FISA Ct. 2010), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV- 02041(HSG)%20Doc%2004%2006.13.17%20--%20REDACTED_updatedf.pdf .
58.	[REDACTED] (2010)	June 13, 2017	Memorandum Opinion and Order, [REDACTED] (FISA Ct. 2010), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV- 02041(HSG)%20Doc%2002%2006.13.17%20--%20REDACTED_updated.pdf .
59.	Dec. 16, 2009	July 8, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 09-19 (FISA Ct. Dec. 16, 2009), https://www.dni.gov/files/documents/0708/BR_09-19 Primary_Order.pdf .
60.	Nov. 5, 2009	Sept. 10, 2013	Supplemental Opinion and Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 09-15 (FISA Ct. Nov. 5, 2009), http://www.dni.gov/files/documents/section/pub_Nov_5_2009_Supplemental_Opinion and_Order.pdf .

61.	[REDACTED]	Aug. 11, 2014	Supplemental Order, [REDACTED], No. PR/TT [REDACTED] (FISA Ct.), https://www.dni.gov/files/0808/Final_006.FISC Supplemental Order.pdf .
62.	Oct. 30, 2009	July 8, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 09-15 (FISA Ct. Oct. 30, 2009), http://www.dni.gov/files/documents/0708/BR 09-15 Primary Order.pdf .
63.	Sept. 25, 2009	Sept. 10, 2013	Order Regarding Further Compliance Incidents, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 09-13 (FISA Ct. Sept. 25, 2009), http://www.documentcloud.org/documents/785211-pub-sept-25-2009-order-regarding-further.html .
64.	Sept. 3, 2009	Sept. 10, 2013	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 09-13, (FISA Ct. Sept. 3, 2009), http://www.dni.gov/files/documents/section/pub_Sep 3 2009 Primary Order from FISC.pdf .
65.	July 22, 2009	Nov. 18, 2013	Order, [REDACTED], No. BR 06-05 (FISA Ct. July 20, 2009), https://www.odni.gov/files/documents/1118/CLEANED089.T.BR 06-05 Motions and Or...Unseal 16AUGU-1-17-Sealed.pdf .
66.	July 9, 2009	July 8, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 09-09 (FISA Ct. July 9, 2009), http://www.dni.gov/files/documents/0708/BR 09-09 Primary Order.pdf .
67.	June 22, 2009	Sept. 10, 2013; also Nov. 18, 2013 with different redactions	Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 09-06, PR/TT [REDACTED] (FISA Ct. June 22, 2009), http://www.dni.gov/files/documents/section/pub_Jun 22 2009 Order.pdf and https://www.odni.gov/files/documents/1118/CLEANED101_Order and Supplemental Order (6-22-09)-sealed.pdf .
68.	[REDACTED]	Aug. 11, 2014 (provided to Congress)	Supplemental Order, [REDACTED], No. PR/TT [REDACTED] (FISA Ct.), https://www.dni.gov/files/0808/Final_004.FISC Primary Order.pdf .

		Aug. 31, 2009)	
69.	May 29, 2009	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 09-06 (FISA Ct. May 29, 2009), http://www.dni.gov/files/documents/11714/FISC Order%2C BR 09-06.pdf .
70.	Mar. 5, 2009	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 09-01 (FISA Ct. Mar. 5, 2009), http://www.dni.gov/files/documents/11714/FISC Order%2C BR 09-01.pdf .
71.	Apr. 7, 2009	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. Apr. 7, 2009), https://www.dni.gov/files/documents/icotr/702/Bates%20549-579.pdf .
72.	Mar. 2, 2009	Sept. 10, 2013	Order, <i>In re Production of Tangible Things from [REDACTED]</i> , No. BR 08-13 (FISA Ct. Mar. 2, 2009), https://www.dni.gov/files/documents/section/pub_March 2 2009 Order from FISC.pdf .
73.	Jan. 28, 2009	Sept. 10, 2013	Order Regarding Preliminary Notice of Compliance Incident Dated January 15, 2009, <i>In re Production of Tangible Things from [REDACTED]</i> , No. BR 08-13 (FISA Ct. Jan. 28, 2009), http://www.dni.gov/files/documents/section/pub_Jan 28 2009 Order Regarding Prelim Notice of Compliance.pdf .
74.	[REDACTED] (2009)	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. 2009), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2011%2006.13.17%20--%20REDACTED.PDF .
75.	[REDACTED] (2009)	June 13, 2017	Memorandum Opinion and Order, <i>[REDACTED]</i> (FISA Ct. 2009), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2005%2006.13.17%20--%20REDACTED.PDF .
76.	[REDACTED]	Aug. 11, 2014 (provided to Congress Mar. 13, 2009)	Primary Order, <i>[REDACTED]</i> , No. PR/TT [REDACTED] (FISA Ct.) (Walton, J.), https://www.dni.gov/files/0808/Final 003.FISC Primary Order.pdf .
77.	Dec. 12, 2008	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 08-13

			(FISA Ct. Dec. 12, 2008), http://www.dni.gov/files/documents/11714/FISC Order%20BR 08-13.pdf .
78.	[REDACTED] (2008)	June 13, 2017	Memorandum Order and Opinion, [REDACTED] (FISA Ct. 2008), https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2001%2006.13.17%20--%20REDACTED%20w%20replacemnt%20page.pdf .
79.	Aug. 19, 2008	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 08-08 (FISA Ct. Aug. 19, 2008), http://www.dni.gov/files/documents/11714/FISC Order%20BR 08-08.pdf .
80.	Aug. 27, 2008	Aug. 27, 2008	Order and Memorandum Opinion, <i>In re Proceedings Required by Section 702(i) of the FISA Amendments Act of 2008</i> , No. Misc 08-01 (FISA Ct. Aug. 27, 2008), http://www.fas.org/irp/agency/doj/fisa/fisc082708.pdf .
81.	June 26, 2008	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 08-07 (FISA Ct. June 26, 2008), http://www.dni.gov/files/documents/11714/FISC Order%20BR 08-07.pdf .
82.	Apr. 3, 2008	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 08-04 (FISA Ct. Apr. 3, 2008), http://www.dni.gov/files/documents/11714/FISC Order%20BR 08-04.pdf .
83.	Illegible (possibly Jan. 2008)	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 08-01 (FISA Ct. [Illegible]), http://www.dni.gov/files/documents/11714/FISC Order%20BR 08-01.pdf .
84.	Oct. 18, 2007	Jan. 17, 2014	Primary Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 07-016 (FISA Ct. Oct. 18, 2007), http://www.dni.gov/files/documents/11714/FISC Order%20BR 07-16.pdf .
85.	Oct. 11, 2007		Order, [REDACTED], (FISA Ct. Oct. 11, 2007), https://cdt.org/files/2014/09/49-yahoo702-memorandum-opinion-and-order-dni-ag-certification.pdf
86.	Aug. 2, 2007	Dec. 12, 2014	Order and Memorandum Opinion, <i>In re [REDACTED]</i> , No. [REDACTED] (FISA Ct. Aug. 2, 2007), https://www.documentcloud.org/documents/1379006-large-content-fisa-order-documents.html .

87.	July 25, 2007	Jan. 17, 2014	Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 07-14 (FISA Ct. July 25, 2007), http://www.dni.gov/files/documents/11714/FISC_Order%2C_BR_07-14.pdf .
88.	May 31, 2007	Dec. 12, 2014	Order, <i>In re [REDACTED]</i> , No. [REDACTED] (FISA Ct. May 31, 2007), https://www.documentcloud.org/documents/1379006-large-content-fisa-order-documents.html .
89.	May 31, 2007	Jan. 17, 2014	Amendment to Order for Purposes of Querying the Metadata Archive [REDACTED], <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 07-10 (FISA Ct. May 31, 2007), https://www.aclu.org/files/section215/20140123/FISC_Amended_Order_BR_07-10.pdf .
90.	May 3, 2007	Jan. 17, 2014	Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 07-10 (FISA Ct. May 3, 2007), http://www.dni.gov/files/documents/11714/FISC_Order%2C_BR_07-10.pdf .
91.	Apr. 5, 2007	Dec. 12, 2014	Order, <i>In re [REDACTED]</i> , No. [REDACTED] (FISA Ct. Apr. 5, 2007), https://www.dni.gov/files/documents/1212/Signed_Primary_Order_-_04_05_07_-_12-11_-_Redacted.pdf .
92.	Apr. 3, 2007	Dec. 12, 2014	Order and Memorandum Opinion, <i>In re [REDACTED]</i> , No. [REDACTED] (FISA Ct. Apr. 3, 2007), https://www.dni.gov/files/documents/1212/CERTIFIED_COPY_-_Order_and_Memorandum_Opinion_04_03_07_12-11_Redacted.pdf .
93.	Feb. 7, 2007	Jan. 17, 2014	Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 07-04 (FISA Ct. Feb. 7, 2007), http://www.dni.gov/files/documents/11714/FISC_Order%2C_BR_07-04.pdf .
94.	Jan. 10, 2007	Dec. 12, 2014	Order, <i>In re Various Known and Unknown Agents of [REDACTED] Presumed United States Persons</i> , No. [REDACTED] (FISA Ct. Jan. 10, 2007), https://www.dni.gov/files/documents/1212/FISC_Order_01_10_07_-_12-11_-_Redacted.pdf .
95.	Jan. 10, 2007	Dec. 12, 2014	Order, <i>In re [REDACTED]</i> , No. [REDACTED] (FISA Ct. Jan. 10, 2007), https://www.dni.gov/files/documents/1212/FISC_Order_01_10_07_12-11_-_Redacted.pdf .
96.	Nov. 15, 2006	Jan. 17, 2014	Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 06-12 (FISA Ct. Nov. 15, 2006), https://www.aclu.org/files/section215/20140123/FISC%20Order%20BR%2006-12.pdf .

97.	Aug. 18, 2006	Jan. 17, 2014	Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 06-08, (FISA Ct. Aug. 18, 2006), https://www.aclu.org/files/section215/20140123/FISC%20Order%20BR%2006-08.pdf .
98.	May 24, 2006	Sept. 10, 2013	Order, <i>In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED]</i> , No. BR 06-05 (FISA Ct. May 24, 2006), http://www.dni.gov/files/documents/section/pub_May_24_2006_Order_from_FISC.pdf .
99.	[REDACTED]	Nov. 18, 2013	Opinion and Order, <i>[REDACTED]</i> , No. PR/TT [REDACTED] (FISA Ct.), https://www.odni.gov/files/documents/1118/CLEANEDPRTT_1.pdf .
100.	[REDACTED]	Jan. 31, 2018	Supplemental Order, <i>[REDACTED]</i> (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-1.pdf .
101.	[REDACTED]	Jan. 31, 2018	Opinion and Order, <i>[REDACTED]</i> (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-2.pdf .
102.	[REDACTED]	Jan. 31, 2018	Supplemental Order, <i>[REDACTED]</i> (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-5.pdf .
103.	[REDACTED]	Jan. 31, 2018	Order, <i>[REDACTED]</i> (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-6.pdf .
104.	[REDACTED]	Jan. 31, 2018	Supplemental Order, <i>[REDACTED]</i> (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-9.pdf .
105.	[REDACTED]	Jan. 31, 2018	Supplemental Order, <i>[REDACTED]</i> (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-12.pdf .
106.	[REDACTED]	Sept. 25, 2017	Order, <i>[REDACTED]</i> (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF%20FOIA%20Sep%2025%20Doc%201.pdf .
107.	[REDACTED]	Sept. 25, 2017	Supplemental Order, <i>[REDACTED]</i> (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF%20FOIA%20Sep%2025%20Doc%203.pdf .
108.	[REDACTED]	Sept. 25, 2017	Order, <i>[REDACTED]</i> (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF%20FOIA%20Sep%2025%20Doc%206.pdf .
109.	[REDACTED]	Sept. 25, 2017	Primary Order for Pen Register and Trap and Trace Device(s), <i>[REDACTED]</i> (FISA Ct.),

			https://www.dni.gov/files/documents/icotr/EFF%20FOIA%20Sep%2025%20Doc%207.pdf .
110.	[REDACTED]	Sept. 25, 2017	Primary Order for Pen Register and Trap and Trace Device(s), [REDACTED] (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF%20FOIA%20Sep%2025%20Doc%208.pdf .
111.	[REDACTED]	Sept. 25, 2017	Supplemental Opinion and Amendment to Primary Order, [REDACTED] (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF%20FOIA%20Sep%2025%20Doc%209.pdf .
112.	[REDACTED]	Sept. 25, 2017	Order, [REDACTED] (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF%20FOIA%20Sep%2025%20%20Doc%202010.pdf .
113.	[REDACTED]	Sept. 25, 2017	Order, [REDACTED] (FISA Ct.), https://www.dni.gov/files/documents/icotr/EFF%20FOIA%20Sep%2025%20Doc%2011.pdf .

JAN 09 2018

LeeAnn Flynn Hall, Clerk of Court

United States Foreign Intelligence Surveillance Court of Review

IN RE: CERTIFICATION OF QUESTIONS OF LAW TO
THE FOREIGN INTELLIGENCE SURVEILLANCE
COURT OF REVIEW

Docket No. FISCR 18-01

Upon Certification for Review by the United States
Foreign Intelligence Surveillance Court.

Before BRYSON, CABRANES, AND TALLMAN, *Judges*.

In Docket No. Misc. 13-08, the Foreign Intelligence Surveillance Court ("FISC") has certified a question of law to this court pursuant to 50 U.S.C. § 1803(j). The certified question is whether the American Civil Liberties Union, the American Civil Liberties Union of the Nation's Capital, and the Media Freedom and Information Access Clinic have adequately established Article III standing to assert their claim of a qualified First Amendment right of public access to FISC judicial opinions.

This court accepts the certification and directs as follows:

(1) The parties to the proceeding before the FISC are invited to file supplemental briefs in this matter. The

briefs should be no more than 30 pages in length and should be filed by February 23, 2018.

(2) Pursuant to 50 U.S.C. § 1803(i), this court appoints Professor Laura Donohue, one of the courts' designated statutory amici, to serve as amicus curiae in this matter. The amicus curiae is invited to file a brief of no more than 30 pages within 45 days of the date of this order.

(3) Within 10 days of the date that the last opening brief is filed by the parties and the amicus curiae, the parties and the amicus curiae may each file a reply brief of no more than 10 pages.

(4) The Clerk is directed to provide each member of this court with copies of all of the briefs filed with the FISC in this matter.

IT IS SO ORDERED.

SIGNED this 9th day of January, 2018.



WILLIAM C. BRYSON
Presiding Judge
United States Foreign Intelligence
Surveillance Court of Review

NOV 09 2017

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

Jessie Ann Flynn Hall, Clerk of Court

IN RE OPINIONS & ORDERS OF THIS COURT
ADDRESSING BULK COLLECTION OF DATA
UNDER THE FOREIGN INTELLIGENCE
SURVEILLANCE ACT.

Docket No. Misc. 13-08

BOASBERG, J., writing for the Court and joined by JJ. SAYLOR, DEARIE, RUSSELL, JONES, and CONTRERAS:

Figuring out whether a plaintiff has standing to bring a novel legal claim can feel a bit like trying to distinguish a black cat in a coal cellar. “Although the two concepts unfortunately are blurred at times, standing and entitlement to relief are not the same thing. Standing is a prerequisite to filing suit, while the underlying merits of a claim . . . determine whether the plaintiff is entitled to relief.” *Arreola v. Godinez*, 546 F.3d 788, 794-95 (7th Cir. 2008). The Initial Opinion in this action decided that Movants – the American Civil Liberties Union and Yale Law School’s Media Freedom and Information Access Clinic – had suffered no injury-in-fact and thus lacked standing to bring their First Amendment claim for access to redacted portions of certain of this Court’s opinions. Sitting *en banc* for the first time in our history, we now vacate that decision. Whatever the merits of Movants’ suit, we conclude that they have asserted a sufficient injury-in-fact to pursue it.

I. Background

By necessity, this Court conducts much of its work in secrecy. But it does so within a judicial system wedded to transparency and deeply rooted in the ideal that “justice must satisfy the appearance of justice.” Levine v. United States, 362 U.S. 610, 616 (1960).

It comes as no surprise, then, that members of the public may at times seek to challenge whether certain controversies merit our continued secrecy or, instead, require some degree of transparency. The matter before us was born from two such challenges. On June 6, 2013, two newspapers released certain classified information about a surveillance program run by the Government since 2006. Within a day, the Director of National Intelligence declassified further details about this bulk-data-collection program, acknowledging for the first time that this Court had approved much of it under Section 215 – the “business records” provision – of the Patriot Act, 50 U.S.C. § 1861.

Very shortly thereafter, Movants filed a motion in this Court asking that we unseal our “opinions evaluating the meaning, scope, and constitutionality of Section 215.” FISC No. Misc. 13-02, Motion of June 2, 2013. They argued that, because officials had now “revealed the essential details of the program,” there was no legitimate interest in continuing to withhold its legal justification. Id. at 18. Movants thus contended that their First Amendment right of access to court proceedings and documents, as recognized by the Supreme Court in Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980), now compelled the release of these rulings. Id. at 6-15. They alternatively asked that we invoke FISC Rule of Procedure 62(a) to request that the Government review the opinions’ classification and publish any declassified portions. Id. at 15-18.

Judge Saylor opted for the latter discretionary route in this first action. In re Orders of this Court Interpreting Sec. 215 of the Patriot Act, No. Misc. 13-02, 2013 WL 5460064 (Foreign Intel. Surv. Ct. Sept. 13, 2013). Before doing so, however, he concluded that Movant ACLU had established Article III standing to pursue its First Amendment challenge, as its asserted injury satisfied the familiar tripartite standing requirement – *i.e.*, it was “concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.” Id. at *2 (quoting Clapper v. Amnesty Int’l USA, 568 U.S. 398, 409 (2013)). More specifically, he reasoned that, because the ACLU had alleged that the continued withholding of our opinions violated its First Amendment right of access to them, its claimed injury was 1) “actual,” as the opinions were not available, 2) “traceable” to the Government’s decision not to make them public, and 3) redressable by “this Court’s directing that those opinions be published.” Id. Judge Saylor also determined that the injury was sufficiently particularized because Movants were “active particip[ants] in the legislative and public debates about the proper scope of Section 215,” and the withheld information would assist them in these conversations. Id. at *4. Ultimately, however, he did not reach the merits of their First Amendment claim, choosing instead to order the Executive Branch under Rule 62(a) to conduct a declassification review of certain of our prior opinions. Id. at *8.

Around the same time, the Government released more details about the bulk-data-collection program, including a white paper that explained how FISC Judges had periodically approved the directives to telecommunications providers to produce bulk telephonic metadata for use in the Government’s counterterrorism efforts. See Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act (Aug. 9, 2013). This Court, too, took steps to make more information available to the public. In particular, we

asked the Executive Branch to review several of our opinions, and we released redacted versions of two about the collection of bulk telephony metadata under Section 215. In re Opinions & Orders of this Court Addressing Bulk Collection of Data under the Foreign Intelligence Surveillance Act, No. Misc. 13-08, 2017 WL 427591, at *2-3 (FISC Jan. 25, 2017).

While these revelations may have slaked some of Movants' thirst for information, they also opened up new lines of inquiry. Movants thus filed another motion – which kicked off the current action – on November 7, 2013, asking us to unseal classified sections of our opinions laying out the legal basis for the data collection. See Movants' Motion of Nov. 7, 2013, available at <http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-08%20Motion-2.pdf>. Here, again, they claimed that these passages were “subject to the public’s First Amendment right of access” and should be released because “no proper basis exists to keep the legal discussions in [them] secret.” Id. at 1. They further contended that we should once more exercise our discretion under Rule 62(a) to ask for a second classification review by the Government and then verify that its response complied with the dictates of the First Amendment. Id. at 24-27.

On November 18, 2013, however, while briefing was ongoing on this issue, the Government published two more redacted opinions by this Court. In re Opinions & Orders of this Court Addressing Bulk Collection of Data under FISA, 2017 WL 427591, at *3. Including the previous pair we had already released, these four opinions constituted all of our rulings that were responsive to Movants' second Motion. In other words, before the Government had even filed an Opposition, the relevant opinions had been “subjected to classification review and the unclassified portions released” with – according to the Government – “as much information . . . as possible consistent with national security.” Opp. of Dec. 6, 2013, at 2.

Given such release, the Government's subsequent Opposition argued that the Court should now dismiss Movants' second action. Any further review, it maintained, would merely "duplicate the[se] result[s]," and there was "no basis for th[is] Court to order [it]." Id. The Government also contended that Movants lacked standing to seek such relief because Rule 62(a) allowed only a party to the proceeding that generated the opinion to move for publication, and Movants had not been involved in the underlying actions. Id. at 2-3. Finally, the Government urged this Court not to order yet another review since Movants could challenge the classification decisions through a Freedom of Information Act case in federal district court. Id. at 3-4.

On January 25, 2017, in a lengthy and thoughtful Opinion, Presiding Judge Collyer determined that Movants had no standing to press their case, and she thus dismissed it. See In re Opinions & Orders of this Court Addressing Bulk Collection of Data under FISA, 2017 WL 427591, at *1. Her Opinion focused in particular on a potential standing problem that the parties had not previously identified – namely, whether Movants had alleged the invasion of a "legally and judicially cognizable" interest sufficient to establish the injury-in-fact prong of the standing analysis. Id. at *7. The Court first took the position that an interest was not legally protected "when its asserted legal source – whether constitutional, statutory, common law or otherwise – does not apply or does not exist." Id. at *8.

On this basis, the Court then engaged in a lengthy merits analysis of Movants' claim under the Richmond Newspapers "experience and logic" test to determine whether such a First Amendment right existed in the unique context of FISC judicial proceedings. Id. at *16-21. Although the Constitution does not expressly provide for access to judicial records, in Richmond Newspapers, the Supreme Court "firmly established for the first time that the press and general public have a constitutional right of access to criminal trials." Globe Newspaper Co. v. Superior

Court, 457 U.S. 596, 603 (1982). Since then, it has extended this right to other judicial processes, but has also recognized that such a First Amendment right of access is not absolute. Id. at 607. Rather, to determine whether the public has a right of access to particular judicial proceedings, courts must ask two questions: “whether the place and process have historically been open to the press and general public” (the experience inquiry) and “whether public access plays a significant positive role in the functioning of the particular process in question” (the logic inquiry). Press-Enterprise Co. v. Superior Court (Press Enterprise II), 478 U.S. 1, 8 (1986). Applying this test, Judge Collyer in this case ultimately answered both prongs in the negative, and she therefore concluded that the right of access did not extend to FISC judicial proceedings. In re Opinions & Orders of this Court Addressing Bulk Collection of Data under FISA, 2017 WL 427591, at *16-21. For this reason alone, the Court then held that Movants had not alleged a sufficient injury-in-fact and thus lacked standing to bring their claim. Id. at *21.

Movants quickly moved for reconsideration. As the resolution of the first and second actions had created an intra-court split on the standing issue, we *sua sponte* granted *en banc* review to reconsider the narrow question of whether Movants have asserted a sufficient injury-in-fact for standing purposes. See 50 U.S.C. § 1803(a)(2)(A); FISC R. P. 45 (allowing the Court to order a hearing or rehearing *en banc* if “necessary to secure and maintain uniformity of the Court’s decisions”). After substantial and reasoned debate and discussion among all eleven judges of this Court, we now answer that inquiry in the affirmative.

II. Analysis

Article III of the Constitution limits the jurisdiction of federal courts to actual “Cases” and “Controversies.” U.S. Const., art. III, § 2. But not just any dispute will do. See Lujan v. Defs. of Wildlife, 504 U.S. 555, 559-61 (1992). The Constitution instead confines the judiciary to deciding

contests that are “appropriately resolved through the judicial process,” as distinguished from those better left to the legislative or executive branches in a democratic government. Id. at 560 (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)). Standing doctrine helps police this boundary by requiring, as an “irreducible constitutional minimum,” that a plaintiff establish three elements to proceed with a claim: 1) an injury-in-fact that is 2) caused by the conduct complained of and 3) “likely” to be “redressed by a favorable decision.” Id. at 560-61 (quotations omitted).

The focus here is on the first prong. A term of art, an injury-in-fact is the “invasion of a legally protected interest which is both (a) concrete and particularized; and (b) actual or imminent, not conjectural, or hypothetical.” Id. at 560 (footnote, internal citations, and quotation omitted). For the purposes of evaluating whether a plaintiff has made this showing, though, “we must assume [Movants’] claim has legal validity.” Cooksey v. Futrell, 721 F.3d 226, 239 (4th Cir. 2013) (quotation omitted). Put another way, in deciding whether Movants have alleged a sufficient injury-in-fact for standing purposes, we “must be careful not to decide the question on the merits for or against [Movants], and must therefore assume that on the merits the [Movants] would be successful in their claims.” City of Waukesha v. EPA, 320 F.3d 228, 235 (D.C. Cir. 2003); see also Citizen Ctr. v. Gessler, 770 F.3d 900, 910 (10th Cir. 2014) (same); Parker v. District of Columbia, 478 F.3d 370, 377 (D.C. Cir. 2007) (“The Supreme Court has made clear that when considering whether a plaintiff has Article III standing, a federal court must assume *arguendo* the merits of his or her legal claim.”), aff’d sub nom. District of Columbia v. Heller, 554 U.S. 570 (2008); see also Warth v. Seldin, 422 U.S. 490, 501-02 (1975) (assuming validity of legal theory for purposes of standing analysis).

Starting from the premise that Movants’ claim is meritorious means that we must assume that withholding our classified opinions violates their First Amendment right of access to judicial

proceedings under the Richmond Newspapers test. From this base, we can readily conclude that this injury is “concrete,” as well as “actual,” because the opinions are currently not available to them. For at least the reasons articulated by Judge Saylor, moreover, it is sufficiently “particularized” from that of the public because of Movants’ active participation in ongoing debates about the legal validity of the bulk-data-collection program.

The Initial Opinion, of course, did not quibble with these conclusions, but instead homed in on the prefatory language of the definition of what constitutes an injury-in-fact. While not every Supreme Court decision even specifies that an alleged injury-in-fact must be to a “legally protected interest,” *see, e.g., Clapper*, 568 U.S. at 409, the Opinion correctly pointed out that some cases have treated this as an independent requirement to establish standing in appropriate circumstances. But from this starting point, the Initial Opinion faltered in concluding that Movants had alleged no legally protected interest because the First Amendment’s right of access to court proceedings “did not apply” to FISC Opinions. In re Opinions & Orders of this Court Addressing Bulk Collection of Data under FISA, 2017 WL 427591, at *21.

As courts have repeatedly affirmed, “For purposes of standing, the question [simply] cannot be whether the Constitution, properly interpreted, extends protection to the plaintiff’s asserted right or interest.” Initiative & Referendum Inst. v. Walker, 450 F.3d 1082, 1092 (10th Cir. 2006) (*en banc*) (emphasis added). “If that were the test, every losing claim would be dismissed for want of standing.” *Id.*; *see also Ass’n of Data Processing Serv. Orgs., Inc. v. Camp*, 397 U.S. 150, 153 & n.1 (2003) (admonishing against use of “legal interest” test as part of standing analysis when it goes to merits of claim). We must instead assume that Movants are correct that they have a constitutional right of access, Waukesha, 320 F.3d at 235 – so long as that right is cognizable. That is, we ask only whether courts are capable of knowing or recognizing such an

interest. See Black's Law Dictionary (10th ed. 2014) (defining "cognizable" as "[c]apable of being known or recognized"); see also Judicial Watch, Inc. v. U.S. Senate, 432 F.3d 359, 364 (D.C. Cir. 2005) (Williams, J., concurring) (explaining Supreme Court uses terms "legally protected" and "judicially cognizable" interchangeably "(1) to encompass the other conventionally stated requirements (that the injury be concrete and particularized, and actual or imminent) and (2) possibly to serve as a screen (perhaps open-ended) against interests that it would make little sense to treat as adequate").

A plaintiff, for instance, might lack standing "to complain about his inability to commit crimes because no one has a right to a commit a crime," and no Court could recognize such an interest. Citizen Ctr. v. Gessler, 770 F.3d 900, 910 (10th Cir. 2014). On the other hand, he would have standing to bring colorable First Amendment claims, even if he would ultimately lose on the merits. Take the seminal example of Buckley v. Valeo, 424 U.S. 1 (1976). There, the Supreme Court allowed plaintiffs to attack campaign-finance laws as unconstitutional, even though, as it turned out, there is no specific "First Amendment right to make unlimited campaign contributions." Initiative & Referendum Inst., 450 F.3d at 1092-93 (citing Buckley, 424 U.S. at 96). As the Tenth Circuit noted, "We could use any unsuccessful constitutional claim to illustrate the point." Id. at 1092. Indeed, were we to define rights with any greater level of specificity, no plaintiff would have standing to challenge established First Amendment precedent. This is certainly not the case. See, e.g., Citizens United v. FEC, 558 U.S. 310, 365-66 (2010) (overturning precedent that upheld restrictions on corporate independent expenditures).

At bottom, the legally-protected-interest test is not concerned with determining the proper scope of the First Amendment right or whether a plaintiff is correct that such right has in fact been invaded; that is a merits inquiry. Waukesha, 320 F.3d at 235. The test instead seeks only to assess

whether the interest asserted by the plaintiff is of the type that “deserve[s] protection against injury.” 13 Charles Alan Wright, Arthur R. Miller, *et al.*, Federal Practice & Procedure § 3531.4 (3d ed. 2008).

Against this backdrop, the sufficiency of Movants’ allegation of such a legally protected interest appears clear. They identify the invasion of an interest – the First Amendment right to access judicial proceedings – that courts have repeatedly held is capable of “being known or recognized.” The Supreme Court first acknowledged that this interest is one the Constitution protects against wrongful invasion in Richmond Newspapers, 448 U.S. 555, when a plurality held that the public’s “right to attend criminal trials is implicit in the guarantees of the First Amendment.” Id. at 580 (footnote omitted). Since then, that Court has also held that this right safeguards the public’s qualified access to other criminal proceedings, including witness testimony, Globe Newspaper, 457 U.S. at 603-11, *voir dire*, Press-Enterprise Co. v. Superior Court (Press Enterprise I), 464 U.S. 501, 505-10 (1984), and preliminary hearings. Press Enterprise II, 478 U.S. at 10-15.

Many federal Courts of Appeals have likewise held this legally protected interest invaded when the public is walled off from other aspects of criminal trials, such as bail, plea, or sentencing hearings. *See, e.g.*, N.Y. Civil Liberties Union v. N.Y.C. Transit Auth., 684 F.3d 286, 297-98 (2d Cir. 2012) (collecting cases); In re Wash. Post Co., 807 F.2d 383, 388-89 (4th Cir. 1986) (plea and sentencing hearings); In re Hearst Newspapers, LLC, 641 F.3d 168, 175-86 (5th Cir. 2011) (sentencing). Finally, at least six Circuits have concluded that the First Amendment qualified right of access also extends to “civil trials and to their related proceedings and records.” N.Y. Civil Liberties Union, 684 F.3d at 298 (emphasis added) (so holding and collecting cases from the Third, Fourth, Seventh, Eighth, and Eleventh Circuits).

These cases all demonstrate that Movants, in asserting a First Amendment right of access to judicial processes, are seeking to vindicate “the sort of interest that the law protects when it is wrongfully invaded.” Aurora Loan Servs., Inc. v. Craddieth, 442 F.3d 1018, 1024 (7th Cir. 2006) (emphases modified). No more than this is necessary for standing purposes, even if Movants ultimately fail to prove that the precise scope of the First Amendment right extends to redacted portions of our judicial opinions under the Richmond Newspapers test. The dissent, by contrast, would require Plaintiffs to make that more specific showing at the standing stage – an inquiry that would swallow any merits determination on the First Amendment’s contours. It is erroneous to understand the cognizable-interest requirement as “beg[ging] the question of the legal validity of the[ir] claim.” Initiative & Referendum Inst., 450 F.3d at 1093 n.3. Rather, as the Tenth Circuit sitting *en banc* has instructed, courts must avoid any such “mischief” inherent in “us[ing] standing concepts to address the question whether the plaintiff has stated a claim.” Id. (quoting 13 Wright & Miller, § 3531.4 (2d ed. Supp. 2005)).

Our conclusion that Movants have met this cognizable-interest requirement is also consistent with the approach adopted by every Circuit to consider a similar claim. As far as we can tell, courts have uniformly found standing to bring a First Amendment right-of-access suit so long as plaintiffs allege an invasion related to judicial proceedings. That is so no matter how novel or meritless the claim may be. Some courts have stretched the right-of-access even farther for standing purposes. In Flynt v. Rumsfeld, 355 F.3d 697 (D.C. Cir. 2004), for example, journalists creatively contended that they had a First Amendment right of access to travel with military-combat units to cover the war in Afghanistan. Id. at 698. Although the D.C. Circuit ultimately held that “no such constitutional right exists” – in fact, having deemed Richmond Newspapers entirely inapplicable – it nevertheless easily concluded that plaintiffs had standing to bring their

suit. Id. at 698, 702-04. This was the case even though the journalists' desire to embed with troops was much farther afield from the core Richmond Newspapers right than the one Movants hope to establish today. Here, they ask only to extend the public's right of access to another Article III context – *i.e.*, FISC judicial proceedings.

The dissent criticizes the Court of Appeals' analysis in Flynt, *see post* at 20, but its dislike of the decision does not diminish its import. In any event, the D.C. Circuit does not stand alone in its approach. The Seventh Circuit, for example, has considered a historian's standing to bring a common-law right-of-access claim to sealed grand-jury materials. *See Carlson v. United States*, 837 F.3d 753, 757-61 (7th Cir. 2016). The plaintiff, it reasoned, "need[ed] only a 'colorable claim' to a right to access these documents, because '[w]ere we to require more than a colorable claim, we would decide the merits of the case before satisfying ourselves of standing.'" Id. at 758 (internal citation omitted); *see also Okla. Observer v. Patton*, 73 F. Supp. 3d 1318, 1321-22, 1325 (W.D. Okla. 2014) (holding plaintiffs had standing to bring First Amendment right-of-access claim to view executions, but dismissing suit as right did "not extend to the circumstances existing here"); United States v. Ring, 47 F. Supp. 3d 38, 41-42 (D.D.C. 2014) (holding criminal defendant had standing to sue for public access to PowerPoint presentation used during proffer session despite holding on merits that "neither a common law nor First Amendment right of access" attached to the record).

Many courts – including the Supreme Court – have not even felt it necessary to address standing in dealing with tenuous right-of-access claims, despite judges' obligation to raise *sua sponte* any jurisdictional defects. Indeed, courts have routinely ignored what the dissent would believe is a serious question, even while expressly addressing their jurisdiction in other respects. For example, the Fourth and Sixth Circuits rejected mootness challenges to suits asserting a First

Amendment right of access to search-warrant proceedings, despite ultimately deciding that the plaintiffs had no such right to these sealed records under the Richmond Newspapers test. See In re Search of Fair Finance, 692 F.3d 424, 428-29, 433 (6th Cir. 2012) (finding claim not moot); Balt. Sun Co. v. Goetz, 886 F.2d 60, 63-65 (4th Cir. 1989) (same). Mootness, of course, shares a common undergirding with standing: “[T]he requisite personal interest that must exist at the commencement of the litigation (standing) must continue throughout its existence (mootness).” Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 528 U.S. 167, 189 (2000) (quoting Arizonans for Official English v. Arizona, 520 U.S. 43, 68 n.22 (1997)). To survive a mootness challenge, then, the plaintiffs must have necessarily demonstrated that the requisite personal injury existed at least in the first instance. Even more recently, in Phillips v. DeWine, 841 F.3d 405 (6th Cir. 2016), the Sixth Circuit rejected a much more farfetched challenge by inmates to the constitutionality of Ohio’s “statutory scheme concerning the confidentiality of information related to lethal injection.” Id. at 410, 419-20. At the outset, the court concluded that the plaintiffs lacked standing to bring their free-speech and prior-restraint causes of action, as their asserted injuries were too hypothetical. But it apparently had no similar concern as to their First Amendment right-of-access claim, holding instead on the merits that no such right existed. Id. at 417-20.

A long list of courts have acted in this fashion. See, e.g., Houchins v. KOED, Inc., 438 U.S. 1, 7-15 (1978) (holding First Amendment provides the media no right of access to county jail, but never questioning standing); Dhiab v. Trump, 852 F.3d 1087, 1096 (D.C. Cir. 2017) (holding plaintiffs have no “right under the First Amendment to receive properly classified national security information filed” in habeas action, but not questioning standing); Wood v. Ryan, 759 F.3d 1076, 1088 (9th Cir. 2014) (Bybee, J., dissenting) (criticizing “majority’s newfound right of access” for

death row inmate seeking information on method of his execution as “dramatic extension of anything” previously recognized, but never questioning standing), vacated, 135 S. Ct. 21 (mem.) (summarily vacated on merits, not standing); In re U.S. for an Order Pursuant to 18 U.S.C. Section 2703(D), 707 F.3d 283, 291-92 (4th Cir. 2013) (holding no First Amendment right under Richmond Newspapers to court orders and proceedings pursuant to Stored Communications Act, but never questioning standing); In re N.Y. Times Co. to Unseal Wiretap, 577 F.3d 401, 409-11 (2d Cir. 2009) (rejecting, under Richmond Newspapers, newspaper’s request to unseal wiretap applications and related materials, but not questioning standing to bring novel claim); Calder v. IRS, 890 F.2d 781, 783-84 (5th Cir. 1989) (applying Richmond Newspapers and holding plaintiff had no First Amendment or statutory right of access to IRS records, but never questioning standing). Although we do not directly rely on any of these cases, we find the uniformity is telling.

Similarly, two former judges of this Court also found it unnecessary to call standing into doubt when rejecting claims premised on the public’s right of access to FISC records, see In re Proceedings Required by § 702(i) of FISA Amendments Act of 2008, No. 08-01, 2008 WL 9487946 (FISC Aug. 27, 2008) (McLaughlin, J.); In re Motion for Release of Court Records, 526 F. Supp. 2d 484 (FISC 2007) (Bates, J.), and, as explained above, Judge Saylor expressly held that plaintiffs did have standing to bring such claims under the First Amendment in Movants’ first action. See In re Orders of this Court Interpreting Section 215 of the Patriot Act, No. 13-02, 2013 WL 5460064, at *2-4 (FISC Sept. 13, 2013).

The Initial Opinion, by contrast, relies on no case that concludes that a plaintiff lacks a legally cognizable interest, and thus standing, simply because that party cannot show a First Amendment right of access applies or exists in the context of the judicial proceeding at issue. The best it could muster is a single case where the plaintiff sought a common-law right of access to

discovery materials. Bond v. Utreras, 585 F.3d 1061, 1074 (7th Cir. 2009). The Seventh Circuit held that these discovery files – exchanged between parties – “had never been filed with the court and [had] never influenced the outcome of a judicial proceeding.” Id. Whatever the merits of that decision, it provides no guidance here, where Plaintiffs seek material far more rooted in judicial proceedings: our opinions. Perhaps recognizing Bond as thin support, the dissent relegates that case to a footnote. Otherwise, no case appears throughout its 25 pages in which any court declined to find standing in like circumstances. This lack of precedential support speaks volumes.

At times, the dissent suggests a variant justification for dismissing the suit: it sees “no legal basis to find that Movants present a colorable claim.” *Post* at 13 (emphasis added); see also id. at 17 n.16 (“In the instant matter, the question is whether Movants have a colorable right under the First Amendment to access information in FISC opinions that the Executive Branch determined was classified.”). This alternative argument seems decidedly weaker to us. Courts have repeatedly set an exceedingly low bar to establish colorability. See Kennedy v. Conn. Gen. Life Ins. Co., 924 F.2d 698, 700 (7th Cir. 1991) (holding only if claim is “frivolous is jurisdiction lacking”); Panaras v. Liquid Carbonic Indus. Corp., 74 F.3d 786, 790 (7th Cir. 1996) (describing the requirement as “not . . . stringent”). Under this colorability standard, only “a plaintiff whose claimed legal right is so preposterous as to be legally frivolous may lack standing on the ground that the right is not ‘legally protected.’” Initiative & Referendum Inst., 450 F.3d at 1093. Whatever the merits of Movants’ First Amendment right-of-access claim, it finds its basis in well-established law. The right to access, even in its more narrow formulation, at least covers “a right of access to certain criminal [and civil] proceedings and the documents filed in those proceedings.” Phillips, 841 F.3d at 418. Movants merely allege that those “certain” documents include our FISC opinions – *i.e.*, opinions filed in an Article III judicial proceeding. This asserted right is certainly more analogous

to the historical right than – for example – a claim that the First Amendment also grants access to travel with troop battalions on a foreign battlefield. Yet, in Flynt, 355 F.3d 697, the D.C. Circuit never mentioned that it might be frivolous to consider such an extension. In fact, the dissent points to no federal court that has ever dismissed as frivolous a novel claim seeking to extend the First Amendment right of access to a new judicial process. We decline to be the first.

The dissent also suggests our analysis should differ because Plaintiffs seek “classified information.” *Post* at 24 (internal quotation marks omitted). It is true that courts rarely presume to review the Executive Branch’s decisionmaking, at least without a statutory hook. See Dep’t of Navy v. Egan, 484 U.S. 518, 538 (1988). Yet the classified information here is not housed in the Executive Branch; instead, it arises within an Article III proceeding, and Plaintiffs seek access to portions of judicial opinions. As explained above, the right to access judicial proceedings is well established. Courts have thus not hesitated to review claims involving secret court proceedings, even when they ultimately find good reason to deny them. See In re Search of Fair Finance, 692 F.3d at 428-29, 433 (sealed search warrants); Goetz, 886 F.2d at 63-65 (same); In re N.Y. Times Co. to Unseal Wiretap, 577 F.3d at 409-11 (sealed wiretap applications).

Nor do we agree with the dissent that we should change our conclusion simply because we consider a constitutional challenge involving the Executive Branch. See *post* at 23-25. Even if the Supreme Court applies an “especially rigorous” standing analysis in this context, Raines v. Byrd, 521 U.S. 811, 819-20 (1997), it has never suggested such an analysis would involve jumping to the merits of the dispute. More to the point, the dissent cites Clapper v. Amnesty International, 568 U.S. 398 (2013), which noted that courts have declined to find standing when reviewing “actions of the political branches in the fields of intelligence gathering and foreign affairs.” *Post*

at 23-24 (quoting Clapper, 568 U.S. at 469). Although that decision admittedly contains some broad language, none offers much insight into the standing question posed here.

In Clapper, the Supreme Court considered a separate facet of the injury-in-fact test – namely, whether the plaintiffs’ theory of future injury was too speculative to be “certainly impending.” Id. at 409. In fact, Clapper’s definition of what constitutes an injury-in-fact did not even include the requirement of a “legally protected” interest upon which the Initial Opinion relies here. Id. at 409 (“To establish Article III standing, an injury must be ‘concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.’”) (citation omitted). Clapper, then, does not impose any special standing requirement on this score; in fact, it might be better read to impose no such showing at all. Schuchardt v. President of the United States, 839 F.3d 336, 348 n.8 (3d Cir. 2016) (“Despite Clapper’s observation that the standing inquiry is especially rigorous in matters touching on intelligence gathering and foreign affairs,” no court has held that “Article III imposes [a] heightened standing requirement for the often difficult cases that involve constitutional claims against the executive involving surveillance.”) (quoting Jewel v. NSA, 673 F.3d 902, 913 (9th Cir. 2011)) (internal quotations from Clapper omitted)). In any event, the claim presented here survives because the injury is a lack of access to the proceedings of a court, rather than one directly traceable to the activities of the political branches in intelligence gathering or foreign affairs.

* * *

At the end of the day, the question that the Initial Opinion asked and answered is not one of standing. It instead goes to the merits of Movants’ legal claim – *i.e.*, whether they have a qualified right of access under the First Amendment to portions of our opinions redacted by the Executive Branch under its classification authority. See Arreola, 546 F.3d at 794-95 (“Although

the two concepts unfortunately are blurred at times, standing and entitlement to relief are not the same thing.”). As that is not what concerns us today, we hold that Movants have sufficiently alleged the invasion of a legally cognizable interest as necessary to establish an injury-in-fact. Whether or not they will ultimately succeed in establishing that the Richmond Newspapers experience-and-logic test entitles them to relief, we believe that they should not be barred at this threshold procedural stage. We further offer no opinion on whether other jurisdictional impediments exist to this challenge, but hold only that Movants have established a sufficient injury-in-fact.

III. Conclusion

Because we hold that Movants have the requisite cognizable interest to pursue their constitutional claim, we vacate the Initial Opinion in this action and remand the matter to Judge Collyer for further consideration of Movants’ Motion.

COLLYER, Presiding Judge, joined by EAGAN, MOSMAN, CONWAY and KUGLER, Judges, dissenting:

In law as in life, the answer depends upon the question. Only by framing the question before us in its most general terms can the Majority answer with the unremarkable proposition that some courts – but not the Supreme Court – have found a First Amendment right of access to some federal court proceedings in civil cases when the place and process historically have been public. But the question the Majority poses is not the one presented by the motion in this case. I respectfully dissent and would affirm the decision in In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the FISA [hereinafter In re Opinions of This Court], No. Misc. 13-08, 2017 WL 427591 (FISA Ct. 2017).

The Foreign Intelligence Surveillance Court (“FISC”) is a special court with a special and discreet mission: to protect the rights of U.S. persons while reviewing surveillance measures to protect national security. FISC proceedings are classified and the Court operates under specific congressional direction that everything it does must respect and protect the secrecy of those classifications. No member of the public would have any “right” under the First Amendment to ask to observe a hearing in the FISC courtroom. Still less should we be inventing such a “right” in the present circumstances.

To be precise, what Movants seek is not “access to judicial proceedings,” as the Majority would have it. Rather, their current request is more limited and specific: having already received this Court’s opinions and orders addressing bulk collection of data with classified material redacted, Movants want us to rule that they have a “right” of access to the information classified by the Executive Branch and that Executive Branch agencies must defend each redaction in the face of Movants’ challenges.

The effect of the Court’s decision today is to displace Congress’s judgment that access to classified and ex parte FISC judicial opinions shall be resolved through the procedures set forth in Section 402 of the USA FREEDOM Act, which, as relevantly titled, governs the “[d]eclassification of significant decisions, orders, and opinions” of the FISC. Just as in the days of John Marshall, it is imperative that the Judiciary avoid the appearance of eroding the very principles intended to maintain the careful balance of powers set forth in the Constitution.¹ The Court’s decision today unfortunately fails in that effort.

One last introductory comment is due. FISC judges come from district courts around the country. Few of us knew each other before our appointments to the FISC. In our work on the FISC, as with our work in our home courts, we decide alone. The occasion of this en banc review of the In re Opinions of This Court decision has given us a rare and wonderful opportunity to wrestle together over some weighty legal principles and issues. This dissent is written in the same spirit.

I.

The question pending before the en banc Court is whether Movants have shown an injury in fact sufficient to establish constitutional standing and this Court’s jurisdiction. There is no dispute between the parties or the members of the Court that Article III of the Constitution limits the judicial power to the adjudication of cases or controversies in which a party seeking relief demonstrates standing for each asserted claim. There likewise is no dispute that the prevailing

¹ “Much more than legal niceties are at stake here. The statutory and (especially) constitutional elements of jurisdiction are an essential ingredient of separation and equilibration of powers, restraining the courts from acting at certain times, and even restraining them from acting permanently regarding certain subjects.” Steel Co. v. Citizens for a Better Env’t, 523 U.S. 83, 101 (1998).

legal standard is set forth in Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992), and requires that Movants “must have suffered an injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical.” Id. at 560 (internal quotation marks and citations omitted).

The Supreme Court has never abandoned the requirement of a “legally protected interest” for the purpose of establishing Article III standing.² See Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (confirming that “a plaintiff must show that he or she suffered an ‘invasion of a legally protected interest’” (quoting Lujan, 504 U.S. at 560)); Ariz. State Legislature v. Ariz. Indep. Redistricting Comm’n, 135 S. Ct. 2652, 2663 (2015) (same); United States v. Windsor, 133 S. Ct. 2675, 2685 (2013) (same). Furthermore, the Supreme Court has signaled that the phrase “legally protected interest” has meaning independent of the requirement that the alleged invasion be concrete and particularized as well as actual or imminent. Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 211 (1995) (stating “Adarand’s claim that the Government’s use of subcontractor compensation clauses denies it equal protection of the laws of course alleges an invasion of a legally protected interest, *and* it does so in a manner that is ‘particularized’ as to Adarand” (emphasis added)).

To determine whether Movants asserted a legally protected interest, “we do not consider the merits in connection with standing, [but] we do consider whether the plaintiffs have a legal right to do what is allegedly being impeded.” Citizen Ctr. v. Gessler, 770 F.3d 900, 910 (10th

² Even when the Supreme Court used the phrase “cognizable interests” for the purpose of evaluating standing it “stressed” that the injury must be both “*legally* and judicially cognizable.” Raines v. Byrd, 521 U.S. 811, 819 (1997) (emphasis added). Movants agree that “[t]he injury alleged must also be one that is ‘legally and judicially cognizable.’” Movants’ En Banc Opening Br. 6, available at <http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-08%20Movants%27%20En%20Banc%20Opening%20Brief.pdf>.

Cir. 2014). In other words, we consider whether there is some law that at least arguably could be deemed to protect Movants' legal interest such that they can be said to have advanced a colorable claim *to the asserted right*. Aurora Loan Servs., Inc. v. Craddieth, 442 F.3d 1018, 1024 (7th Cir. 2006). As the Seventh Circuit has explained:

The point is not that to establish standing a plaintiff must establish that a right of his has been infringed; that would conflate the issue of standing with the merits of the suit. It is that he must have a colorable claim to such a right. It is not enough that he claims to have been injured by the defendant's conduct. "The alleged injury must be legally and judicially cognizable. This requires, among other things, that the plaintiff have suffered 'an invasion of a legally protected interest.'"

Id. (quoting Raines, supra note 2, at 819 (quoting Lujan, 504 U.S. at 560)). To be clear, "[w]hile standing does not depend on the merits of the party's contention that certain conduct is illegal, standing does require an injury to the party arising out of a violation of a constitutional or statutory provision or other legal right." Fed. Deposit Ins. Corp. v. Grella, 553 F.2d 258, 261 (2d Cir. 1977). Accord Cox Cable Commc'ns, Inc. v. United States, 992 F.2d 1178, 1182 (11th Cir. 1993) ("No legally cognizable injury arises unless an interest is protected by statute or otherwise."). "The interest must consist of obtaining compensation for, or preventing, the violation of a legally protected right." Vermont Agency of Natural Res. v. U.S. ex rel. Stevens, 529 U.S. 765, 772 (2000).

II.

A.

Applying these legal standards, the Supreme Court has directed that "[a]lthough standing in no way depends on the merits of the plaintiff's contention that particular conduct is illegal, it often turns on the nature and source of the claim asserted." Warth v. Seldin, 422 U.S. 490, 500 (1975). Indeed, the Supreme Court has agreed unanimously that "standing is gauged by the specific common-law, statutory or constitutional claims that a party presents." Int'l Primate Prot.

League v. Adm'rs of Tulane Educ. Fund, 500 U.S. 72, 77 (1991). “Typically . . . the standing inquiry requires careful judicial examination of a complaint’s allegations to ascertain whether the particular plaintiff is entitled to adjudication *of the particular claims asserted*.” Id. (internal quotation marks omitted, emphasis in original).

Accordingly, to determine whether Movants have a legally protected interest the first step is to examine the specific constitutional claims Movants present. Id. Movants assert a First Amendment-protected interest to access information in certain FISC judicial opinions that the Executive Branch determined is classified national security information. Movants further assert a First Amendment-protected interest to require the Executive Branch to explain its rationale for classification and respond to Movants’ challenges to their constitutionality, and for the FISC to decide between them.³ Movants’ Mot. 1, 24. They invoke no other source of right for their claims.

The Majority Opinion strays from Movants’ “particular claims” and recasts their legal interest as broadly as possible into “access to judicial proceedings,” Majority Op. 10. By doing so, the Majority scrambles the scope of an interest recognized under the qualified First Amendment right of public access and the scope of an interest recognized under the common law

³ Specifically, Movants seek access to classified information that was redacted from four FISC judicial opinions that were declassified, in part, and made public in 2013. Now that the opinions are public, Movants ask the Court to compel the Executive Branch to conduct a second declassification review and “require the government to justify its proposed redactions, permit Movants an opportunity to respond, and then make findings on the record about whether the proposed redactions are narrowly tailored to avert a substantial risk of harm to a compelling governmental interest.” Movants’ Reply Br. 2, available at <http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-08%20Reply-1.pdf>. Movants claim the qualified First Amendment right of public access mandates these procedures as a matter of right, although they concede that “much of this Court’s work may not be subject to a constitutional right of access” Movants’ Reply Br. 1.

right of access. The result is a legal analysis that ignores the Supreme Court's direction to examine the nature and source of Movants' claims and gauge their standing by the specific constitutional claims they present. This confusion has consequences because the First Amendment and the common law are analyzed differently.

The First Amendment provides no general right of access to government proceedings. Houchins v. KOED, Inc., 438 U.S. 1, 15 (1978) (plurality) (“The Constitution itself is neither a Freedom of Information Act nor an Official Secrets Act” and “[n]either the First Amendment nor the Fourteenth Amendment mandates a right of access to government information or sources of information within the government’s control.”). Accord Phillips v. DeWine, 841 F.3d 405, 419 (6th Cir. 2016) (rejecting a broad assertion of a First Amendment right to government information that pertains to a government proceeding and noting that “[n]either this court nor the Supreme Court has ever recognized a right so broad”). Nor does the First Amendment provide a presumptive⁴ or general right of access to “judicial proceedings” as a subset of government proceedings. See, e.g., id. (noting that Houchins “sets the baseline principle for First Amendment claims seeking access to information held by the government”). Richmond Newspapers and its progeny offer an “exception” to the Houchins rule that there is no First Amendment right to access government proceedings, id. at 418, but that exception is limited to judicial proceedings that satisfy what has come to be known as the “experience” and “logic” tests

⁴ When courts refer to a “presumptive First Amendment right of access,” see, e.g., N.Y. Civil Liberties Union v. New York City Transit Auth., 684 F.3d 286, 296 (2d Cir. 2012), that “presumption” only comes into play after the First Amendment actually applies or attaches. There is, however, no “presumption” that the First Amendment applies or attaches to any particular judicial proceeding or document; instead, the Supreme Court established the non-presumptive test set forth in Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980) (plurality opinion), and its progeny.

set forth by the Supreme Court to determine when the First Amendment applies to a particular judicial proceeding to which access is sought, see Press-Enter. Co. v. Superior Court, 478 U.S. 1, 9 (1986) (“Press-Enterprise II”) (“If the particular proceeding in question passes these tests of experience and logic, a qualified First Amendment right of public access attaches.”).

The D.C. Circuit observed in Flynt v. Rumsfeld, 355 F.3d 697 (D.C. Cir. 2004), that the Supreme Court has found that a qualified First Amendment right of public access applies to *criminal* judicial proceedings only when the place and process historically have been open to the public and public access plays a significant positive role in the functioning of the particular process in question. 355 F.3d at 704. Lower courts have extended the Richmond Newspapers exception to certain trial-like civil proceedings found to satisfy the same experience and logic tests, but the Supreme Court has never ratified that approach. Id.

Again, standing must be “gauged by the specific . . . constitutional claims that a party presents.” Int’l Primate Prot. League, 500 U.S. at 77. The “specific” constitutional claims Movants present are claims under the First Amendment to access information in FISC judicial opinions that the Executive Branch has determined is classified national security information. The FISC issued those opinions in ex parte proceedings that are unique to its jurisdiction under 50 U.S.C. §§ 1842(b) and 1861(b)(1). Movants also assert a concomitant right to challenge the constitutionality of each of those classification decisions, to require the Executive Branch to defend them, and to obtain FISC rulings on it all. Because the unclassified portions of the FISC opinions at issue have already been made public, Movants’ alleged interest can only be described as accessing “classified information in FISC judicial opinions”⁵ and not the broader universe of

⁵ This framing of the interest is consistent with the Court’s prior precedent addressing whether the qualified First Amendment right of public access applies to classified FISC judicial proceedings. See In re Motion for Release of Court Records, 526 F. Supp. 2d 484, 491-97 (FISA

“access to judicial proceedings” generally, as perceived by the Majority Opinion.⁶ See, e.g., Doe, 749 at 266 (limiting the First Amendment to “secur[ing] a right of access only to *particular* judicial records and documents” and not to “all judicial documents and records”).

To be sure, one can find broad statements about a right of the public to access judicial proceedings more generally. But those statements concern the common law right of access, which is a right that was not invoked by Movants and is analytically distinct from the First Amendment right they claimed. As the Fourth Circuit cogently explained, “[t]he common-law presumptive right of access extends to all judicial documents and records” whereas “[b]y *contrast*, the First Amendment secures a right of access only to *particular* judicial records and documents” when it applies. See Doe v. Pub. Citizen, 749 F.3d 246, 265-66 (4th Cir. 2014) (internal quotation marks and citation omitted, emphases added).⁷ The Sixth Circuit echoed this

Ct. 2007) (concluding that the First Amendment provides no public right of access to FISC judicial records).

⁶ Movants contend their interest is in “opinions containing significant legal interpretation of the Constitution and statutory law” and they argue that “[f]or those sorts of opinions, at least, the First Amendment has always required courts to operate openly” Movants’ Reply Br. 1. This argument is clearly erroneous. For example, the Supreme Court has implied, and federal circuit courts of appeal have expressly held, that the qualified First Amendment right of public access does not apply to grand jury proceedings where significant opinions are frequently made. See, e.g., Douglas Oil Co. of Cal. v. Petrol Stops Nw., 441 U.S. 211, 218-21 (1979) (making clear that grand jury proceedings historically have been closed to the public and public access would hinder the efficient functioning of those proceedings so such proceedings impliedly would not satisfy the test of experience and logic set forth in Richmond Newspapers); In re Motions of Dow Jones & Co., 142 F.3d 496, 499 (D.C. Cir. 1998) (“A settled proposition, one the press does not contest, is this: there is no First Amendment right of access to grand jury proceedings.”); United States v. Smith, 123 F.3d 140, 148 (3d Cir. 1997) (“Not only are grand jury proceedings not subject to any First Amendment right of access, but third parties can gain access to grand jury matters only under limited circumstances.”).

⁷ Accord In re U.S. for an Order Pursuant to 18 U.S.C. § 2703(D), 707 F.3d 283, 291 n.8 (4th Cir. 2013) (rejecting plaintiffs’ contention that the First Amendment protects a general right to access judicial orders and proceedings because “[t]his interpretation of the First Amendment

sentiment when it stated that the First Amendment covers only “*certain* proceedings and documents filed therein and nothing more.” Phillips, 841 F.3d at 419 (internal quotation marks omitted, emphasis added).

In describing the right of access to judicial records under the common law, the Supreme Court has stated that “[i]t is clear that the courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents.” Nixon v. Warner Commc’ns, Inc., 435 U.S. 589, 597 (1978). That right, however, is not sacrosanct and yields when, for example, “Congress has created an administrative procedure for processing and releasing to the public” the material sought by a litigant, id. at 603, which arguably is the case here. Section 402 of the USA FREEDOM Act of 2015⁸—fittingly titled “Declassification of significant decisions, orders, and opinions”—now provides procedures for making FISC judicial opinions publicly available. In addition, the Freedom of Information Act (“FOIA”) dictates what “[e]ach agency shall make available to the public” 5 U.S.C. § 552(a). Moreover, this Court previously held that, with respect to FISC proceedings, the common law right of access is preempted by the Foreign Intelligence Surveillance Act of 1978, codified as amended at 50 U.S.C. §§ 1801-1885c (West 2015) (“FISA”). In re Motion for Release of Court Records, 526 F. Supp. 2d at 490-91 (rejecting the ACLU’s claim of a common law right of access because, among other reasons, “[t]he requested records are being maintained under a comprehensive statutory scheme designed to protect FISC records from routine public

right of access is too broad, and directly contrary to our holding that this right extends only to particular judicial records and documents”).

⁸ Pub. L. No. 114-23, 129 Stat. 268 (2015), as codified at 50 U.S.C. § 1872.

disclosure”). The essential point, however, is that Movants have not claimed a violation of the common law right of access.

B.

After properly framing Movants’ interest as an interest in accessing classified information in FISC judicial opinions rather than the expansion adopted by the Majority, it is necessary to decide whether that interest is protected by law. Movants cite the qualified First Amendment right of public access as their only legally protected interest.⁹ The only interest protected by the qualified First Amendment right of public access, however, is an interest in access to trial-like judicial proceedings¹⁰ and related documents when the place and process historically have been open to the public and public access plays a significant positive role in the functioning of the particular process in question. See, e.g., Press-Enterprise II, 478 U.S. at 9 (stating that the “particular proceeding” in question must pass the tests of experience and logic for the qualified First Amendment right of access to attach); Cincinnati Gas & Electric Co. v.

⁹ In re Opinions of This Court, No. Misc. 13-08, 2017 WL 427591, at *21.

¹⁰ As discussed supra page 7, the Supreme Court has never extended the qualified First Amendment right of public access to non-criminal proceedings and the D.C. Circuit continues to adhere to the Supreme Court’s application. See, e.g., Flynt, 355 F.3d 697 at 704 (“To summarize, neither this Court nor the Supreme Court has ever applied Richmond Newspapers outside the context of criminal proceedings, and we will not do so today.”). Other courts, though, have extended the right to certain trial-like civil and administrative proceedings. See, e.g., N.Y. Civil Liberties Union v. N.Y.C. Transit Auth., 684 F.3d 286, 298 (2d Cir. 2012). While we all recognize this contrary authority, it remains true that, “[b]olstered by the Sixth Amendment’s express right for a ‘public trial’ in ‘all criminal prosecutions,’ public access to criminal trials forms the core of this First Amendment constitutional right.” In re Application of WP Co. LLC, 201 F. Supp. 3d 109, 117 (D.D.C. 2016) (internal citations omitted). See also United States v. Doe, 63 F.3d 121, 127 (2d Cir. 1995) (reciting history of open criminal trials and noting “[i]n Gannett [Co., Inc. v. DePasquale], 443 U.S. 368] 379-81, the Supreme Court, striking the balance in favor of the criminal defendant, determined that the Sixth Amendment guarantee of a public trial was personal to the accused and did not grant the press and general public an independent right of access, at least to pretrial suppression hearings”).

Gen. Electric Co., 854 F.2d 900, 903 (6th Cir. 1988) (applying the same tests to a civil proceeding). To distill this point to its essence for our purposes, it is fair to say that the qualified First Amendment right of public access protects only an interest in judicial proceedings and related documents involving places and processes that have been historically public.¹¹ That rubric patently does not apply to the FISC, FISC proceedings or FISC judicial opinions, or to information classified by the Executive Branch and redacted in declassified versions of FISC judicial opinions.

Working in secrecy at the FISC is not simply a matter of “necessity.” Majority Op. 2. It is a legislative imperative under FISA. See, e.g., 50 U.S.C. §§ 1803(c) (stating that “[t]he record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security procedures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence”), 1805(a) (mandating that, “[u]pon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified” if certain specified findings are made), 1842(d)(1) (same), 1861(c)(1) (same). The FISC has twice emphasized this congressional mandate. See In re Opinions & Orders of This Court, No. Misc. 13-08, 2017 WL 427591, at *15; In re Motion for Release of Court Records, 526 F. Supp. 2d at 488-90. And at least twice the FISC has emphasized that its proceedings have never been public, it has never held a public hearing, and the number of opinions released to the public is statistically minor relative to the thousands of classified decisions it has issued. See In re Opinions & Orders of This Court, 2017 WL 427591,

¹¹ The Majority agrees. Majority Op. 6 (admitting that “to determine whether the public has a right of access to particular judicial proceedings, courts must ask . . . whether the place and process historically have been open to the press and general public” (internal quotation marks omitted)).

at *17-20; In re Motion for Release of Court Records, 526 F. Supp. 2d at 487-88, 492-93.

Notably, too, in this matter no sealing order or other discretionary action has been taken by the Court to impede public access to its classified opinions or the classified information redacted from its declassified and public opinions.¹² The point is not just that FISC proceedings and judicial documents have never been historically public, but, importantly, the FISC does not exercise discretionary decision making about whether to conduct its proceedings in a non-public fashion—it is required to do so by statute.

This history of non-public proceedings weighs heavily against Movant’s asserted First Amendment right of access to information classified by the Executive Branch. Even “[m]ore significant is that from the beginning of the republic to the present day, there is no tradition of publicizing secret national security information” Dhiab v. Trump, 852 F.3d 1087, 1094 (D.C. Cir. 2017). “The tradition is exactly the opposite.” Id.

Movants argue that this Court should not defer to the Executive Branch’s classification decisions but should review and potentially reject those decisions. Movants’ Reply Br. 2. This argument is considered only to determine whether Movants have identified a right that the First Amendment protects, not to rule on its merits. They have not identified such a First Amendment right to FISC review of Executive Branch classification decisions. Furthermore, this Court has

¹² In Bond v. Utreras, 585 F.3d 1061, 1073 (7th Cir. 2009), the Seventh Circuit noted that the common law offers a presumptive right of access to most documents filed in court based on the principle that courts “are public institutions that operate openly” and “judicially imposed limitations on this right are subject to the First Amendment.” Because the FISC issued no sealing order or protective order preventing Movants’ access to the classified information they seek, there has been no “judicially imposed limitation” that would be subject to the First Amendment. Furthermore, contrary to the Majority Opinion’s assertion that Bond is “thin support,” Majority Op. 15, it stands for the very proposition asserted in the January 25, 2017 Opinion, 2017 WL 427591, at *10, which is that when there is no law that applies to protect a plaintiff’s asserted interest, there is no legally protected interest sufficient to establish Article III standing.

previously said that “[u]nder FISA and the applicable Security Procedures, there is no role for this Court independently to review, and potentially override, Executive Branch classification decisions” and, even “if the FISC were to assume the role of independently making declassification and release decisions in the probing manner requested by the ACLU, there would be a real risk of harm to national security interests and ultimately to the FISA process itself.” In re Motion for Release of Court Records, 526 F. Supp. 2d at 491.

The Majority Opinion fails to accord these principles the governing weight to which they are entitled. Richmond Newspapers specifically established a two-part test for determining when the qualified First Amendment right of access applies – and that standard requires both the place and the process to have been historically public.¹³ The Majority Opinion appears to accept this principle,¹⁴ even as it fails to apply it. There is no legal basis to find that Movants present a colorable claim the First Amendment protects their asserted interest in accessing a place and process that is distinctly not public and required by law to *not* be public.

III.

The Majority Opinion most strenuously decries the January 25, 2017 decision in In re Opinions of This Court because the Majority believes that deciding Movants have no legally protected interest necessarily, and improperly, involved deciding the merits of Movants’ cause of action. The Majority Opinion chastises the decision for having “engaged in a lengthy merits analysis of Movants’ claim under the Richmond Newspapers ‘experience and logic’ test,”

¹³ “The First Amendment guarantees the press and the public access to aspects of court proceedings, including documents, ‘if such access has historically been available, and serves an important function of monitoring prosecutorial or judicial misconduct.’” United States v. El-Sayegh, 131 F.3d 158, 161 (D.C. Cir. 1997). Accord Press-Enterprise II, 478 U.S. at 9.

¹⁴ See note 11, supra.

Majority Op. 5. But the Majority fails to explain why it believes that addressing Richmond Newspapers constituted deciding the merits of the motion. Plainly an examination of the law invoked by Movants may be part of—even essential to—a proper analysis of standing. See Warth, 422 U.S. at 500 (“[S]tanding . . . often turns on the nature and source of the claim asserted.”); Int’l Primate Prot. League, 500 U.S. at 77 (“[S]tanding is gauged by the specific common-law, statutory or constitutional claims that a party presents.”). Because application of the experience and logic tests revealed that Movants have no right of public access to classified FISC judicial documents or proceedings, they failed to identify an interest that is legally protected and, thus, have no standing.

The Majority takes the mistaken and circular view that, because the Court must assume that on the merits Movants would be successful in their claims when it evaluates standing, it therefore follows that, “[f]rom this base,” the Court can conclude that Movants satisfy the requirements of Article III standing. Majority Op. 8. The Majority misinterprets the Supreme Court’s edict that consideration of Article III standing does not involve consideration of the merits. “Because a review of standing does not review the merits of a claim, but the parties and forum involved, our assumption during the standing inquiry that the plaintiff will eventually win the relief he seeks does not, on its own, assure that the litigant has satisfied *any element of standing.*” Fla. Audubon Soc’y v. Bentsen, 94 F.3d 658, 664 n.1 (D.C. Cir. 1996) (internal citations omitted, emphasis added). “Any assumption as to the outcome of the litigation simply does not resolve the issues critical to a standing inquiry.” Id. That is because, as the Second Circuit has noted, “[t]he standing question is distinct from whether [a litigant] *has a cause of action!*” Carver v. New York, 621 F.3d 221, 226 (2d Cir. 2010) (citing Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)) (emphasis added). Cf. Libertad v. Welch, 53 F.3d 428, 439 (1st Cir.

1995) (“Appellants need not establish the elements of their cause of action in order to sue, only to succeed on the merits.”).

“[W]hat has been traditionally referred to as the question of standing . . . involves analysis of ‘whether a party has a sufficient stake in an otherwise justiciable controversy to obtain judicial resolution of that controversy’”¹⁵ DaCosta v. Laird, 471 F.2d 1146, 1152 (2d Cir. 1973) (quoting Sierra Club v. Morton, 405 U.S. 727, 731-732 (1972)) (emphasis omitted). The “merits analysis . . . determines whether a claim is one for which relief can be granted if factually true.” Catholic League for Religious & Civil Rights v. City and Cnty. of San Francisco, 624 F.3d 1043, 1049 (9th Cir. 2010) (en banc). “A party’s injury in fact is distinct from its potential causes of action.” Am. Farm Bureau Fed’n v. U.S. Env’tl. Prot. Agency, 836 F.3d 963, 968 (8th Cir. 2016). As demonstrated below, whether Movants can establish the elements of their cause of action alleging that the Court improperly withheld information that the Executive Branch improperly determined was classified national security information requires consideration of factual and legal issues separate from the question of whether the First Amendment applies at all to certain FISC judicial opinions and proceedings. The Majority overlooks this important nuance in the Supreme Court’s legal standard that otherwise prohibits consideration of standing from reaching the merits of the cause of action.

The Majority’s error also represents a misreading of Richmond Newspapers and its progeny, as well as cases that find no standing when a plaintiff fails to identify a legally protected interest. The Majority Opinion notes the Tenth Circuit’s statement in Initiative &

¹⁵ “Although the standing question is often dressed in the dazzling robe of legal jargon, its essence is simple—what kind of injuries are courts empowered to remedy and what kind are they powerless to address?” Schaffer v. Clinton, 240 F.3d 878, 883 (10th Cir. 2001).

Referendum Inst. v. Walker, 450 F.3d 1082, 1092 (10th Cir. 2006) that, “[f]or purposes of standing, the question cannot be whether the Constitution, properly interpreted, extends protection to the plaintiff’s asserted right or interest.” Majority Op. 8 (quoting Walker, 450 F.3d at 1092). But the Majority misunderstands the import of the statement: its principle applies when, unlike this matter, there is an *applicable* constitutional provision and both standing and the merits involve the same question about the *scope* of that applicable constitutional provision. See Day v. Bond, 500 F.3d 1127, 1136-1138 (10th Cir. 2007) (“Critically, however, in Walker, the plaintiffs’ asserted injury and their claimed constitutional violation were one and the same.”). When standing and the merits require different legal analyses, standing can be, and must be, decided first and independently. Id. The Tenth Circuit explained:

[W]e did note [in Walker] that “the term ‘legally protected interest’ must do some work in the standing analysis . . . [and] has independent force and meaning without any need to open the door to merits considerations at the jurisdictional stage.” Id. at 1093. . . .

Practically speaking, Walker mandates that we assume, during the evaluation of the plaintiff’s standing, that the plaintiff will prevail on his merits argument—that is, that the defendant has violated the law. See id. (“For purposes of standing, we must assume the [p]laintiffs’ claim has legal validity.”). But there is still work to be done by the standing requirement, and Supreme Court precedent bars us from assuming jurisdiction based upon a hypothetical legal injury. See Lujan, 504 U.S. at 560, 112 S. Ct. 2130. While Walker addressed an instance in which the merits of the plaintiffs’ claims mirrored the alleged standing injury, that is not always the case. *There are cases, such as the one before us here, where the alleged injury upon which the plaintiffs rely to establish standing is distinct from the merits of claims they assert. E.g., In re Special Grand Jury 89–2*, 450 F.3d 1159, 1172–73 (10th Cir.2006) (“[A] plaintiff can have standing despite losing on the merits—that is, even though the [asserted legally protected] interest would not be protected by the law in that case.”); see also Duke Power Co. v. Carolina Evt’l Study Grp., Inc., 438 U.S. 59, 78–79, 98 S.Ct. 2620, 57 L.Ed.2d 595 (1978).

Here, the issue of standing is not necessarily determined by the merits determination. The merits issue is whether K.S.A. § 76–731a is preempted by 8 U.S.C. § 1623. The standing question is whether § 1623 creates a private cause of action. Each of these issues is separate and independent,

and we may determine whether the Plaintiffs here have standing to assert a private cause of action under § 1623 without reaching the merits of whether § 1623 preempts § 76–731a. See DH2, Inc. v. U.S. Sec. & Exchange Comm’n, 422 F.3d 591, 592 (7th Cir. 2005) (determining that the plaintiff lacked standing because its injury was speculative, without addressing the merits of the underlying claim).

Under these conditions, Walker simply does not apply. Accordingly, we now turn to the pure standing question whether § 1623 confers a private cause of action upon the Plaintiffs.

Id. (emphases added).¹⁶ Day makes a useful distinction that is helpful to the immediate discussion.

According to the Tenth Circuit, decisions on standing and the merits remain independent legal inquiries whenever a decision on the merits would *not* necessarily decide standing. Only when both merits and standing require a decision on the same legal question does that Circuit find them conjoined so that standing cannot be separately decided first.¹⁷ That is not the case here.

In Press-Enterprise II the Supreme Court made clear that, when the qualified First Amendment right of public access applies (which is an antecedent inquiry Movants failed to

¹⁶ To be clear, Walker itself involved a recognized First Amendment right because plaintiffs were asserting a free-speech interest expressly protected by the First Amendment. 450 F.3d at 1088. In the instant matter, the immediate question is whether Movants have a colorable right under the First Amendment to access information in FISC opinions that the Executive Branch determined was classified.

¹⁷ The Tenth Circuit has also recounted “instances in which courts have examined the merits of the underlying claim and concluded that the plaintiffs lacked a legally protected interest and therefore lacked standing.” Skull Valley Band of Goshute Indians v. Nielson, 376 F.3d 1223, 1236 (10th Cir. 2004). The D.C. Circuit has clearly held that when “plaintiff’s claim has no foundation in law, he has no legally protected interest and thus no standing to sue.” Claybrook v. Slater, 111 F.3d 904, 907 (D.C. Cir. 1979) (citations omitted). Deciding standing can often come close to the merits without violating legal principles. See Arjay Assocs., Inc. v. Bush, 891 F.2d 894, 898 (Fed. Cir. 1989) (stating that “[b]ecause appellants have no right to conduct foreign commerce in products excluded by Congress, they have in this case no right capable of judicial enforcement and have thus suffered no injury capable of judicial redress”).

surmount in this case), a cause of action arises if (1) access was denied (2) without specific, on-the-record findings (3) demonstrating that “closure [was] essential to preserve higher values” and (4) closure was “narrowly tailored to serve that interest.” 478 U.S. at 13-14 (quoting Press-Enter. Co. v. Superior Ct., 464 U.S. 501, 510 (1984) (“Press-Enterprise I”). Movants contend that their cause of action also includes as an element a right to challenge the government’s classification decisions. Movants’ Reply In Support of Their Mot. for the Release of Court Records 4, available at <http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-08%20Reply-1.pdf>. These elements form Movants’ cause of action, the merits of which were never discussed in In re Opinions of This Court.

As to standing, however, the question focuses on whether classified FISC judicial opinions and proceedings have been historically open to the public and arise from a trial-like setting, see Richmond Newspapers, so that Movants have a colorable legally protected interest. This latter question does not run to the merits of their cause of action but, instead, to “whether the plaintiffs have a legal right to do what is allegedly being impeded.” Citizen Ctr., 770 F.3d at 910; see also Grella, 553 F.2d at 261 (“standing does require an injury to the party arising out of a legal right”); Cox Cable Commc’ns, Inc., 992 F.2d at 1182 (there is no injury “unless an interest is protected”).

The Majority ignores this directly-applicable precedent in opining that the January 25, 2017 decision ruled improperly on the merits in deciding that Movants had not asserted a legally

protected interest under the First Amendment.¹⁸ The Majority confuses proper application of the Article III requirement that a litigant present a cognizable legal interest with a merits decision on whether that legal interest was unlawfully impaired.

IV.

The Majority Opinion raises other considerations that, in my estimation, are not persuasive and do not detract from the foregoing analysis. From the outset, the Majority Opinion not only confuses the scope of the qualified First Amendment right of public access with the common law presumptive right of access, but the Majority also characterizes as “novel” Movants’ theory that a qualified First Amendment right of public access applies to classified and ex parte FISC judicial proceedings that historically never have been public. However, it is not novel. Movants initially presented their First Amendment theory to the FISC more than a decade ago, at which time it was considered and decisively rejected. See In re Motion for Release of Court Records, 526 F. Supp. 2d 484. This same theory has been re-litigated without success multiple times since.¹⁹

¹⁸ See In re Opinions of This Court, 2017 WL 427591, at *9-13 (listing cases). The Majority Opinion fails to distinguish these cases and cites no applicable precedent to the contrary. Each of the cases cited in In re Opinions of This Court involved dismissal for lack of subject matter jurisdiction, which is not a decision on the merits. See, e.g., Havens v. Mabus, 759 F.3d 91, 98 (D.C. Cir. 2014) (stating that “[w]e have previously held that dismissals for lack of jurisdiction are not decisions on the merits”).

¹⁹ See In re Orders of This Court Interpreting S. 215 of the Patriot Act, No. Misc. 13-02, 2013 WL 5460064, at *1 (FISA Ct. 2013) (stating that the ACLU “assert[ed] a qualified First Amendment right of access to the opinions in question”); In re Proceedings Required by 702(i) of FISA Amendments Act of 2008, Misc. No. 08-01, 2008 WL 9487946, at *3 (FISA Ct. 2008) (observing that the ACLU’s request for release under the First Amendment “is similar to a request it made on August 9, 2007”); In re Motion for Release of Court Records, Misc. No. 07-01 (FISA Ct. Feb. 8, 2008) (rejecting on reconsideration the ACLU’s First Amendment theory).

More importantly, the Majority suggests that novelty might have legal significance to the real issue, i.e., whether Movants' claims involve injury to a legally protected interest. For example, the Majority Opinion states, "[a]s far as we can tell, courts have uniformly found standing to bring a First Amendment right-of-access suit so long as plaintiffs allege an invasion related to judicial proceedings" and "[t]hat is so no matter how novel or meritless the claims may be." Majority Op. 11. The Majority Opinion cites no case to support this claim of "uniform" judicial "findings." At best, the Majority Opinion goes on to assert that "[s]ome courts have stretched the right-of-access even farther for standing purposes," Majority Op. 11, then cites a single D.C. Circuit decision, namely Flynt v. Rumsfeld, 355 F.3d 697 (D.C. Cir. 2004).

The Flynt decision does not do the work the Majority asks of it. Contrary to the Majority's characterization, the Flynt court found that appellants "asserted no *cognizable* First Amendment claim." 355 F.3d at 703 (emphasis added). Nonetheless, the Flynt court found that they had standing to bring (at best some of) their claims alleging a press right to embed with combat troops, which was advanced based on the First Amendment's express guarantees of free press and speech, not the qualified First Amendment right of public access. Id. The Flynt court discussed standing in a single paragraph that omits without explanation Lujan's definition of "injury in fact" as "an invasion of a *legally protected interest* which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical."²⁰ 504 U.S. at 560 (internal quotation marks and citations omitted, emphasis added). Since Flynt, the Supreme Court has repeatedly reiterated that required element of an injury-in-fact, see supra page 3, calling into question the perfunctory discussion of standing in Flynt. Finally, the Flynt court's

²⁰ Flynt also makes no mention of the alternative formulation that an "injury in fact" must be legally and judicially cognizable. See Raines, 521 U.S. at 819.

standing analysis did not give any consideration to the novelty of the appellants' claim of a right to embed with troops and did not involve a request for access to judicial proceedings.

The Majority Opinion adds that “many courts—including the Supreme Court—have not even felt it necessary to address standing in dealing with tenuous right-of-access claims,” Majority Op. 12, and “[a] long list of courts have acted in this fashion,” Majority Op. 13. The Majority Opinion then cites eight decisions from six courts: (1) Houchins v. KQED, Inc., 438 U.S. 1 (1978); (2) Dhiab, 852 F.3d 1087; (3) Phillips, 841 F.3d 405; (4) In re United States for an Order Pursuant to 18 U.S.C. Section 2703(D), 707 F.3d 283; (5) In re Search of Fair Finance, 692 F.3d 424 (6th Cir. 2012); (6) In re New York Times Company to Unseal Wiretap and Search Warrant Materials, 577 F.3d 401 (2d Cir. 2009); (7) Baltimore Sun Company v. Goetz, 886 F.2d 60 (4th Cir. 1989); (8) Calder v. Internal Revenue Service, 890 F.2d 781, 783-84 (5th Cir. 1989)). All of these cases collapse upon examination.

Three of the cases cited by the Majority—Dhiab, In re New York Times Company and Baltimore Sun—did not address standing because they involved permissive intervenors.²¹ The federal circuits are split about whether third-parties moving to intervene permissively under Rule 24(b) of the Federal Rules of Civil Procedure in ongoing litigation in which a case or controversy already exists must themselves demonstrate Article III standing. See Mangual v. Rotger-Sabat, 317 F.3d 45, 61 (1st Cir. 2003) (stating that “the circuits are split on the question of whether standing is required to intervene if the original parties are still pursuing the case and thus maintaining a case or controversy”). Cf. In re Endangered Species Act § 4 Deadline Litig., 704

²¹ See Dhiab, 852 F.3d at 1090 (stating that the district court “granted the [press] organizations’ motion to intervene”); In re N.Y. Times Co. to Unseal Wiretap & Search Warrant Materials, 577 F.3d at 401 (stating in background section that newspaper moved to intervene and citing the district court case confirming that fact); Baltimore Sun, 886 F.2d at 62 (stating that the Baltimore Sun had petitioned the district court to intervene).

F.3d 972, 980 (D.C. Cir. 2013) (“It remains, however, an open question in this circuit whether Article III standing is required for permissive intervention.”).

Houchins involved news media organizations that sought to expand the *scope* of the First Amendment’s express protections for a free press into an “implied special right of access to government-controlled sources of information.” 438 U.S. at 7-8. It is not surprising that the Supreme Court did not discuss standing given that the question was not whether the First Amendment’s right of a free press applied but, rather, whether, properly interpreted, the scope of that right mandated the access sought by the news media organizations. Id.

Because the remaining cases, Phillips, In re United States for an Order Pursuant to 18 U.S.C. Section 2703(D), In re Search of Fair Finance and Calder were silent about the question of standing²² it is inappropriate to draw any conclusion about what they “felt” about standing. Ariz. Christian Sch. Tuition Org. v. Winn, 563 U.S. 125, 144 (2011) (“The Court would risk error if it relied on assumptions that have gone unstated and unexamined.”). At best, it might be argued that the absence of any relevant discussion of standing by these courts *implies* that they thought there was standing, except that “[w]hen a potential jurisdictional defect is neither noted nor discussed in a federal decision, the decision does not stand for the proposition that no defect existed.” Id.²³ “There is no such thing as a precedential *sub silentio* jurisdictional holding[.]” Cuba v. Pylant, 814 F.3d 701, 709 (5th Cir. 2016).

²² Although the Sixth Circuit in Phillips addressed standing with respect to other constitutional claims asserted by the plaintiffs, it failed to do so for the so-called “right-of-access-to-government-proceedings” claim. 841 F.3d at 414-20.

²³ See also United States v. L. A. Tucker Truck Lines, Inc., 344 U.S. 33, 38 (1952) (“Even as to our own judicial power or jurisdiction, this Court has followed the lead of Chief Justice Marshall who held that this Court is not bound by a prior exercise of jurisdiction in a case where it was not questioned and it was passed *sub silentio*.”).

V.

The Majority Opinion fails to persuade. It confuses the scope of a legally protected interest under the qualified First Amendment right of public access with the scope of such an interest under the common law. It further confuses the standing requirement under Article III that a litigant present an injury to a protected legal interest with the merits decision on whether the litigant can actually prove that the asserted legal interest was impaired. Under Richmond Newspapers, the qualified First Amendment right of public access patently does not apply to non-trial-like judicial proceedings that are not public and never have been. The errors in the Majority Opinion effectively relax the requirements for Article III standing when members of the public ask to review and comment on redacted classified information in FISC judicial opinions. As a result, anyone in the United States apparently has a legally protected First Amendment interest in accessing information in FISC judicial opinions that the Executive Branch determined is classified and may invoke this Court's statutorily-limited and specialized jurisdiction to challenge those classification decisions as unconstitutional. I cannot agree. For these reasons I would conclude that Movants lack standing to assert their claims as Article III standing requirements are understood and applied in any case. But the Court should apply those requirements with particular rigor in *this* case.

The Supreme Court has instructed the lower courts to apply a more rigorous analysis of standing when a party seeks to challenge actions by the Executive or Legislative Branches on constitutional grounds. See, e.g., Raines, 521 U.S. at 819-20. To be precise, the Supreme Court has stated that "our standing inquiry has been *especially rigorous* when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." Id. (emphasis added). Accord Crawford v. United States Dep't of the Treasury, 868 F.3d 438, 457 (6th Cir. 2017). Layered onto this

“especially rigorous” analysis is the Supreme Court’s observation that “we have often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs,” as also is the case here. Clapper v. Amnesty Int’l USA, 568 U.S. 398, 409 (2013).²⁴

Intelligence gathering is one of the “vital aspects of national security.” Gen. Dynamics Corp. v. United States, 563 U.S. 478, 486 (2011). “Matters intimately related to . . . national security are rarely proper subjects for judicial intervention.” Haig v. Agee, 453 U.S. 280, 292 (1981). Accordingly, “unless Congress specifically has provided otherwise, courts traditionally

²⁴ The Majority disagrees that “we should change our conclusion simply because we consider a constitutional challenge involving the Executive Branch.” Majority Op. 16. The Majority’s position is difficult to follow; one cannot avoid a Raines analysis here. An especially rigorous standing analysis is required—without reference to the merits—whenever the merits of the dispute would force a court to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional. Raines, 521 U.S. at 819-20. Movants are asking the FISC to do exactly that. Critically, there has been no sealing, closure, or protective order issued by the FISC to impede Movants’ access to the classified information they seek, so there is no discretionary judicial action being challenged by Movants, unlike cases in which the qualified First Amendment right of access was found to apply. See, e.g., Press-Enter. II, 478 U.S. at 4 (judicial closure order); Press-Enter. I, 464 U.S. at 503-504 (same); Globe Newspaper Co. v. Superior Court for Norfolk Cnty., 457 U.S. 596, 598 (1982) (same); Richmond Newspapers, 448 U.S. at 559-60 (same).

The Majority Opinion also seizes on the dissent’s quotation from Clapper to insist that there is no “special standing requirement” for plaintiffs seeking review of acts by the political branches in the fields of intelligence gathering and foreign affairs. Majority Op. 17 (claiming that the dissent is reading Clapper to impose such a requirement and citing Schuchardt v. President of the United States, 839 F.3d 336 (3d Cir. 2016)). But Schuchardt addressed a heightened standing requirement in line with the analysis in Jewel v. Nat’l Sec. Agency, 673 F.3d 902, 913 (9th Cir. 2011), in which the Ninth Circuit rejected a district court’s requirement that plaintiffs demonstrate a “strong” and “persuasive” claim to Article III standing when suing NSA. This dissent quotes Clapper to caution against *relaxing* standing requirements and expanding judicial power, 568 U.S. at 408-409, not to advocate for special standing requirements. Like this dissent, Clapper made no mention of a “special” or “heightened” requirement to establish standing in the national security realm or otherwise. Rather, in combination, Raines and Clapper require courts to ensure the vigor of the principles of separation of powers by giving close attention and exacting consideration to the elements of standing when asked to review actions of the political branches involving intelligence gathering.

have been reluctant to intrude upon the authority of the Executive in . . . national security affairs,” Dep’t of Navy v. Egan, 484 U.S. 518, 530 (1988), including “the protection of classified information,” which the Supreme Court has directed “must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it,” id. at 529.

“Relaxation of standing requirements is directly related to the expansion of judicial power[.]” Clapper, 568 U.S. at 408-409 (quoting United States v. Richardson, 418 U.S. 166 (1974) (Powell, J., concurring)). “The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches.” Id. Importantly, “decision-making in the field[] of . . . national security is textually committed to the political branches of government.” Schneider v. Kissinger, 412 F.3d 190, 194 (D.C. Cir. 2005). In the exercise of that textually-committed decision-making, Congress has already provided two avenues for any member of the public to obtain access to FISC judicial opinions (Section 402 of the USA FREEDOM Act and FOIA), subject to Executive Branch classification decisions which, under FOIA, are subject to examination in federal district courts insofar as specifically provided by statute.

The Majority Opinion provides no basis in law for the FISC to expand its jurisdiction contrary to Supreme Court guidance, statutory provisions that limit its jurisdiction to a specialized area of national concern, and the evident congressional mandate that the Court conduct its proceedings ex parte and in accord with prescribed security procedures. Applying

well-established principles of Article III standing with the rigor appropriate to a constitutional challenge to Executive Branch determinations in the national security sphere, I continue to conclude that Movants lack standing to assert the constitutional claim in question.

For all these reasons, I respectfully dissent.

JAN 25 2017

UNITED STATES LeeAnn Flynn Hall, Clerk of Court
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE OPINIONS & ORDERS OF THIS COURT
ADDRESSING BULK COLLECTION OF DATA
UNDER THE FOREIGN INTELLIGENCE
SURVEILLANCE ACT.

Docket No. Misc. 13-08

OPINION

Pending before the Court is the MOTION OF THE AMERICAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF THE NATION'S CAPITAL, AND THE MEDIA FREEDOM AND INFORMATION ACCESS CLINIC FOR THE RELEASE OF COURT RECORDS,¹ which, as is evident from the motion's title, was filed jointly by the American Civil Liberties Union ("ACLU"), the American Civil Liberties Union of the Nation's Capital ("ACLU-NC"), and the Media Freedom and Information Access Clinic ("MFIAC") (collectively "the Movants"). The Movants ask the Court to "unseal its opinions addressing the legal basis for the 'bulk collection' of data" on the asserted ground that "these opinions are subject to the public's First Amendment right of access, and no proper basis exists to keep the legal discussion in these opinions secret." Mot. for Release of Ct. Records 1. As will be explained, however, the four opinions the Movants seek were never under seal and were declassified by the Executive Branch and made public with redactions in 2014. Consequently, although characterized as a request for the release of certain

¹ Hereinafter, this motion will be referred to as the "Motion for the Release of Court Records" and cited as "Mot. for Release of Ct. Records." Documents submitted by the parties are available on the Court's public website at <http://www.fisc.uscourts.gov/public-filings>.

of this Court's judicial opinions, what the Movants actually seek is access to the redacted material that remains classified pursuant to the Executive Branch's independent classification authority.

As explained in Parts I and II of the following Discussion, this Court has jurisdiction over the Motion for Release of Court Records only if it presents a case or controversy under Article III of the Constitution, which in turn requires among other things that the Movants assert an injury to a legally protected interest. The Movants claim that withholding the opinions in question contravenes a qualified right of access to those opinions under the First Amendment. If, contrary to the Movants' interpretation of the law, the First Amendment does not afford a qualified right of access to those opinions, they have failed to claim an injury to a legally protected interest. For reasons explained in Part III of the Discussion, the First Amendment does not apply pursuant to controlling Supreme Court precedent so there is no qualified right of access to those opinions. Accordingly, the Court holds that the Movants lack standing under Article III and the Court therefore must dismiss the Motion for Release of Court Records for lack of jurisdiction.

By no means does this result mean that the opinions at issue, or others like them, will never see the light of day. First, the opinions at issue have already been publicly released, subject to Executive Branch declassification review and redactions that withhold portions of those opinions found to contain information that remains classified. Members of the public seeking release of other opinions (or further release of redacted text in the opinions at issue in this matter) may submit requests under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and seek review of the Executive Branch's responses to those requests in a federal district court. Finally, as noted *infra* Part V, Congress has charged Executive Branch officials—not this

Court—with releasing certain significant Court opinions to the public, subject to declassification review. Those statutory mechanisms for public release are unaffected by the determination that the Court lacks jurisdiction over the instant motion.

BACKGROUND AND PROCEDURAL POSTURE

The Movants filed the pending motion in the wake of unauthorized but widely-publicized disclosures about National Security Agency (“NSA”) programs involving the bulk collection of data under the Foreign Intelligence Surveillance Act of 1978, codified as amended at 50 U.S.C. §§ 1801-1885c (West 2015) (“FISA”). The motion urges the Court to unseal its judicial opinions addressing the legality of bulk data collection on the ground that the First Amendment to the United States Constitution guarantees that the public shall have a qualified right of access to judicial opinions. Mot. for Release of Ct. Records 1, 2, 12-21. The Movants contend that this right of access applies even when national security interests are at stake. *Id.* at 17. According to the Movants, the right of access can be overcome only if the United States of America (the “Government”) satisfies a “strict” test requiring evidence of a substantial probability of harm to a compelling interest and no alternative means to protect that interest. *Id.* at 3, 21-24, 25, 28. Even if the Government demonstrates a substantial probability of harm to a compelling interest, the Movants maintain that “[a]ny limits on the public’s right of access must . . . be narrowly tailored and demonstrably effective in avoiding that harm.” *Id.* at 3. The Movants therefore insist that the First Amendment obligates the Court to review independently any portions of the Court’s judicial opinions that are being withheld from public disclosure via redaction and assess whether the redaction is sufficiently narrowly tailored to protect only a compelling interest and nothing more. *Id.* at 23.

To conduct this independent review, the Movants suggest that the Court should first invoke Rule 62 of the United States Foreign Intelligence Surveillance Court (“FISC”) Rules of Procedure and order the Government to perform a classification review of all judicial opinions addressing the legality of bulk data collection.² *Id.* at 24. If the ordered classification review results in the Government withholding any contents of the Court’s opinions by redaction, the Movants assert that the Court should schedule the filing of legal briefs to allow the Government to set forth the rationale for “its sealing request” and to accommodate the Movants’ presentation of countervailing arguments regarding “any sealing they believe to be unjustified,” *id.*, after which the Court should “test any sealing proposed by the government against the standard required by the First Amendment,” *id.* at 27. *See also* Movants’ Reply in Supp. of Their Mot. for Release of Ct. Records 2, 4. The Movants further request that the Court exercise its discretion to order a classification review pursuant to FISC Rule 62 even if the Court ultimately concludes that a First Amendment right of access does not apply in this matter. *Id.* at 27.

The Government opposes the Movants’ motion principally because the four opinions that address the legal bases for bulk collection were made public in 2014 after classification reviews conducted by the Executive Branch. Gov’t’s Opp’n Br. 1-2. Two opinions were published by the Court:

- Memorandum, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, Docket No. BR 13-158 (Oct. 11, 2013) (McLaughlin, J.), available at <http://www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Memorandum-1.pdf>; and

² Rule 62 provides in relevant part that, after consultation with other judges of the court, the Presiding Judge of the FISC may direct that an opinion be published and may order the Executive Branch to review such opinion and “redact it as necessary to ensure that properly classified information is appropriately protected pursuant to Executive Order 13526 (or its successor).” FISC Rule 62(a).

- Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, Docket No. BR 13-109 (Aug. 29, 2013) (Eagan, J.), available at <http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf>.

Gov't's Opp'n Br. 2. The other two opinions were released by the Executive Branch:

- Opinion and Order, [Redacted], Docket No. PR/TT [Redacted] (Kollar-Kotelly, J.), available at <https://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf>; and
- Memorandum Opinion, [Redacted], Docket No. PR/TT [Redacted] (Bates, J.), available at <https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf>.

Id. The Government submits that, because the Executive Branch already conducted thorough classification reviews of all four opinions before their publication and release, there is no reason for the Court to order the Government to repeat that process.³ *Id.* The Government further argues that the motion should be dismissed for lack of the Movants' standing to advance FISC Rule 62 as a vehicle for publication because that rule permits only a "party" to move for publication of the Court's opinions. *Id.* at 3. In support, the Government cites the Court's decision in *In re Orders of This Court Interpreting Section 215 of the PATRIOT Act*, No. Misc. 13-02, 2013 WL 5460064 (FISA Ct. Sept. 13, 2013), for the proposition that the term "party" in Rule 62 refers to a "party" to the proceeding that resulted in the opinion. Gov't's Opp'n Br. 3. The Government points out that the Movants were not such "parties" to any of the proceedings that begot the four opinions discussing the legality of bulk collection. *Id.* Finally, the Government contends that the Court should decline to exercise its own discretion to require the Executive Branch to conduct another classification review of the relevant opinions under Rule 62—or to permit the Movants to challenge the redaction of classified material—because FOIA

³ The Movants argue that the Executive Branch's classification reviews were insufficient and resulted in the four declassified opinions being "redacted to shreds." Movants' Reply In Supp. of Their Mot. for Release of Ct. Records 8.

supplies the proper legal mechanism to seek access to classified material withheld by the Executive Branch. *Id.* at 3-4. According to the Government, the FISC is not empowered to review independently and/or override Executive Branch classification decisions, *id.* at 4-6, nor should the FISC serve as an alternate forum to duplicate the judicial review afforded by FOIA, *id.* at 3-4.

DISCUSSION

Before proceeding to consider the merits of the pending motion the Court must first establish with certainty that it has jurisdiction. Because the FISC is an Article III court,⁴ it cannot exercise the judicial power to resolve the Movants' motion unless there is an actual "case or controversy" in which the Movants have standing. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (May 16, 2016) (discussing the constitutional limits on the exercise of judicial power). "No principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies" as set forth in Article III of the Constitution. *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 37 (1976). By framing the exercise of judicial power in terms of "cases or controversies," Article III recognizes:

[T]wo complementary but somewhat different limitations. In part those words limit the business of federal courts to questions presented in an adversary context and in a form historically viewed as capable of resolution through the judicial process. And in part those words define the role assigned to the judiciary in a tripartite allocation of power to assure that the federal courts will not intrude into areas committed to the other branches of government.

⁴ *See In re Sealed Case*, 310 F.3d 717, 731 (FISA Ct. Rev. 2002) (per curiam) (indicating that "the constitutional bounds that restrict an Article III court" apply to the FISC); *In re Kevork*, 634 F. Supp. 1002, 1014 (C.D. Cal. 1985) (rejecting the assertion that the FISC "is not a proper Article III court"), *aff'd*, 788 F.2d 566 (9th Cir. 1986).

Flast v. Cohen, 392 U.S. 83, 95 (1968). As will be discussed, the separation-of-powers concern poses particular unease in this case.

“From Article III’s limitation of the judicial power to resolving ‘Cases’ and ‘Controversies,’ and the separation-of-powers principles underlying that limitation, [the Supreme Court has] deduced a set of requirements that together make up the ‘irreducible constitutional minimum of standing.’” *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377, 1386 (2014) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). This doctrine of standing is an “essential and unchanging part of the case-or-controversy requirement of Article III” *Lujan*, 504 U.S. at 560. “In fact, standing is perhaps the most important jurisdictional doctrine, and, as with any jurisdictional requisite, we are powerless to hear a case when it is lacking.” *Bochese v. Town of Ponce Inlet*, 405 F.3d 964, 974 (11th Cir. 2005) (internal citations and quotation marks omitted). As the Supreme Court has observed:

In essence the question of standing is whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues. This inquiry involves both constitutional limitations on federal-court jurisdiction and prudential limitations on its exercise. In both dimensions it is founded in concern about the proper—and properly limited—role of the courts in a democratic society.

In its constitutional dimension, standing imports justiciability: whether the plaintiff has made out a “case or controversy” between himself and the defendant within the meaning of Art. III. This is the threshold question in every federal case, determining the power of the court to entertain the suit.

Warth v. Seldin, 422 U.S. 490, 498 (1975) (internal quotation marks and citations omitted).

I.

Accordingly, at the outset, the Court is obligated to ensure that it can properly entertain the Movants' motion because they have met their burden of establishing standing sufficient to satisfy the Article III requirement of a case or controversy. *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 342 (2006). To do so, the Movants "must clearly and specifically set forth facts sufficient to satisfy . . . Art. III standing requirements. A federal court is powerless to create its own jurisdiction by embellishing otherwise deficient allegations of standing." *Whitmore v. Arkansas*, 495 U.S. 149, 155-56 (1990). Moreover, because "standing is not dispensed in gross," *Lewis v. Casey*, 518 U.S. 343, 358 n.6 (1996), the Movants "must demonstrate standing for each claim [they] seek[] to press" as well as "for each form of relief sought," *DaimlerChrysler*, 547 U.S. at 352 (quoting *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 185 (2000)). Ultimately, "[i]f a dispute is not a proper case or controversy, the courts have no business deciding it, or expounding the law in the course of doing so." *DaimlerChrysler*, 547 U.S. at 341. Absent standing, the Court's exercise of judicial power "would be gratuitous and thus inconsistent with the Art. III limitation." *Simon*, 426 U.S. at 38.

Anticipating that standing might be an issue, the Movants commenced their legal arguments by first claiming that they established standing by virtue of the fact that they were denied access to judicial opinions. Mot. for Release of Ct. Records 10. The Movants assert that "[d]enial of access to court opinions alone constitutes an injury sufficient to satisfy Article III." *Id.* By footnote, the Movants also question in part the decision in *In re Orders of This Court Interpreting Section 215 of the PATRIOT Act*, 2013 WL 5460064, to the extent that it held that a party claiming the denial of public access to judicial opinions must further show either (1) that the lack of public access impeded the party's own activities in a concrete and particular way or

(2) that access would afford concrete and particular assistance to the party in the conduct of its own activities, although the Movants alternatively argue that “even if those showings are necessary to establish standing, [they] satisfy the additional requirements.” *Id.* at 11 n.27.

It appears that *In re Orders of This Court Interpreting Section 215 of the PATRIOT Act* was the first and only occasion on which a FISC Judge expressly addressed the question of a third party’s standing for the purpose of asserting a First Amendment right to access this Court’s judicial opinions.⁵ That was a case championed by these same Movants on the same ground that the First Amendment guarantees a qualified right of public access to judicial opinions, although in that case the Movants sought access to opinions analyzing Section 215 of the USA PATRIOT Act (as codified at 50 U.S.C. § 1861). *In re Orders of This Court Interpreting Section 215 of the PATRIOT Act*, 2013 WL 5460064, at *1. There, the parties neglected to address standing so the Court was obliged to consider it sua sponte based on the existing record, *id.*, after impliedly taking judicial notice of public matters, *id.* at *4 (stating that “[t]he Court ordinarily would not look beyond information presented by the parties to find that a claimant has Article III standing” but “[i]n this case . . . the ACLU’s active participation in the legislative and public debates about the proper scope of Section 215 and the advisability of amending that provision is obvious from the public record and not reasonably in dispute”). The Court found that the ACLU and the ACLU-NC had standing but MFIAC did not, *id.* at *4, albeit the Court later reinstated MFIAC as a party upon granting MFIAC’s motion seeking reconsideration of its standing on the strength of

⁵ *In re Motion for Release of Court Records*, 526 F. Supp. 2d 484 (FISA Ct. 2007), also involved a motion filed by the ACLU seeking the release of court documents. In that case, part of which is discussed at length *infra* Part IV, the ACLU’s standing was not addressed and the cited basis for the exercise of jurisdiction was the Court’s inherent supervisory power over its own records and files. *Id.* at 486-87 (citing *Nixon v. Warner Commc’ns, Inc.*, 435 U.S. 589, 598 (1978)).

additional information regarding MFIAC's activities, Opinion & Order Granting Mot. for Recons., *In re Orders of This Court Interpreting Section 215 of the PATRIOT Act*, No. Misc. 13-02 (Aug. 7, 2014), available at http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-6_0.pdf. The Court never reached the question of whether the First Amendment applied, however, and, instead, dismissed for comity the Movants' motion to the extent it sought opinions that were the subject of ongoing FOIA litigation in another federal jurisdiction. *In re Orders of This Court Interpreting Section 215 of the PATRIOT Act*, 2013 WL 5460064, at *6-7. The Court then exercised its own discretion to initiate declassification review proceedings for a single opinion pursuant to Rule 62. *Id.* at *8.

Recognizing that the decision in *In re Orders of This Court Interpreting Section 215 of the PATRIOT Act* involved the same Movants asserting, in essence, the same type of legal claim, the question of standing nevertheless must be independently examined in this case because "[t]his court, as a matter of constitutional duty, must assure itself of its jurisdiction to act in every case." *CTS Corp. v. EPA*, 759 F.3d 52, 57 (D.C. Cir. 2014). Significantly, the decision in *In re Orders of This Court Interpreting Section 215 of the PATRIOT Act* is distinguishable because it did not reach the question of whether the First Amendment applied and, if not, whether the Movants could establish standing in the absence of an interest protected by the First Amendment. This case also is in a unique posture because the Movants seek access to judicial documents that already have been made public and declassified by the Executive Branch, unlike the documents sought in *In re Orders of This Court Interpreting Section 215 of the PATRIOT Act*. An independent assessment of standing also is warranted in light of Article III's necessary function to circumscribe the Federal Judiciary's exercise of power, *Spokeo*, 136 S. Ct. at 1547, and given

the “highly case-specific” nature of jurisdictional standing inquiries, *Baur v. Veneman*, 352 F.3d 625, 637 (2d Cir. 2003).

Embarking on an analysis of standing in this matter, the Court is mindful that, because “[s]tanding is an aspect of justiciability,” “the problem of standing is surrounded by the same complexities and vagaries that inhere in justiciability.” *Flast*, 392 U.S. at 98. Indeed, “[s]tanding has been called one of ‘the most amorphous (concepts) in the entire domain of public law.’” *Id.* at 99 (quoting *Hearings on S. 2097 Before the Subcomm. on Constitutional Rights of the S. Judiciary Comm.*, 89th Cong. 498 (2d Sess. 1966) (statement of Prof. Paul A. Freund)). The United States Court of Appeals for the Second Circuit has referred to standing as a “labyrinthine doctrine,” *Fin. Insts. Ret. Fund v. Office of Thrift Supervision*, 964 F.2d 142, 146 (2d Cir. 1992), and even the Supreme Court has admitted that “‘the concept of Art. III standing’ has not been defined with complete consistency in all of the various cases decided by this Court which have discussed it,” *Whitmore*, 495 U.S. at 155 (quoting *Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc.*, 454 U.S. 464, 475 (1982)).

Despite its nebulousness, there are several fundamental guideposts that offer direction and a general framework to evaluate standing in any given case. To begin with, while it has long been the rule that standing “in no way depends on the merits of the plaintiff’s contention that particular conduct is illegal,” it nonetheless “often turns on the nature and source of the claim asserted.” *Warth*, 422 U.S. at 500. Supreme Court precedent “makes clear that Art. III standing requires an injury with a nexus to the substantive character of the statute or regulation at issue[.]” *Diamond v. Charles*, 476 U.S. 54, 70 (1986) (citing *Valley Forge Christian Coll.*, 454 U.S. at 472). Thus, “standing is gauged by the specific common-law, statutory or constitutional claims that a party presents.” *Int’l Primate Prot. League v. Adm’rs of Tulane Educ. Fund*, 500 U.S. 72,

77 (1991). “In essence, the standing question is determined by ‘whether the constitutional or statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff’s position a right to judicial relief.’” *E.M. v. New York City Dep’t of Educ.*, 758 F.3d 442, 450 (2d Cir. 2014) (quoting *Warth*, 422 U.S. at 500). “[A]lthough standing is an anterior question of jurisdiction, the grist and elements of [the Court’s] jurisdictional analysis require a peek at the substance of [the Movants’] arguments.” *Transp. Workers Union of Am., AFL-CIO v. Transp. Sec. Admin.*, 492 F.3d 471, 474-75 (D.C. Cir. 2007).

It also is well established that the doctrine of standing consists of three elements, the first of which requires the Movants to show that they suffered an “injury in fact.” *Lujan*, 504 U.S. at 560. The second element requires that the injury in fact be “fairly traceable” to the defending party’s challenged conduct and the third element requires that there be a likelihood (versus mere speculation) that the injury will be redressed by a favorable judicial decision. *Id.*

II.

Recently, the Supreme Court emphasized that “injury in fact” is the “[f]irst and foremost’ of standing’s three elements.” *Spokeo*, 136 S. Ct. at 1547 (quoting *Steel Co. v. Citizens for Better Env’t*, 523 U.S. 83, 103 (1998)). Importantly for the purpose of resolving the pending motion, the Supreme Court has “stressed that the alleged injury must be legally and judicially cognizable.” *Raines v. Byrd*, 521 U.S. 811, 819 (1997). “This requires, among other things, that the plaintiff have suffered an invasion of a *legally protected interest* which is . . . concrete and particularized, and that the dispute is traditionally thought to be capable of resolution through the judicial process[.]” *Id.* (internal quotation marks and citations omitted, emphasis added). “[A]n injury refers to the invasion of some ‘legally protected interest’ arising

from constitutional, statutory, or common law.” *Pender v. Bank of Am. Corp.*, 788 F.3d 354, 366 (4th Cir. 2015) (quoting *Lujan*, 504 U.S. at 578).

The meaning of the phrase “legally protected interest” has been a source of perplexity in the case law as a result, at least in part, of the Supreme Court’s pronouncement that a party can have standing even if he loses on the merits. See *Warth*, 422 U.S. at 500 (stating that “standing in no way depends on the merits of the plaintiff’s contention that particular conduct is illegal”); *In re Special Grand Jury 89-2*, 450 F.3d 1159, 1172 (10th Cir. 2006) (“The term *legally protected interest* has generated some confusion because the Court has made clear that a plaintiff can have standing despite losing on the merits” (emphasis in original)); *Judicial Watch, Inc. v. U.S. Senate*, 432 F.3d 359, 363 (D.C. Cir. 2005) (Williams, J., concurring) (expressing “puzzlement” over the Supreme Court’s use of the phrase “legally protected” as a “modifier” and examining the discordant state of the case law’s treatment of the phrase); *United States v. Richardson*, 418 U.S. 166, 180-81 (1974) (Powell, J., concurring) (questioning the Supreme Court’s approach in *Flast*, 392 U.S. at 99-101, on the ground that “[t]he opinion purports to separate the question of standing from the merits . . . yet it abruptly returns to the substantive issues raised by a plaintiff for the purpose of determining whether there is a logical nexus between the status asserted and the claim sought to be adjudicated” (internal quotation marks omitted)); *Ass’n of Pub. Agency Customers v. Bonneville Power Admin.*, 733 F.3d 939, 951 n.23 (9th Cir. 2013) (“The exact requirements for a ‘legally protected interest’ are far from clear.”). The confusion is compounded by the fact that the Supreme Court has occasionally resorted to using the phrase “judicially cognizable interest” rather than, or interchangeably with, the phrase “legally protected interest.” *Judicial Watch*, 432 F.3d at 364 (Williams, J., concurring) (“[T]he [Supreme] Court appears to use the ‘legally protected’ and ‘judicially cognizable’ language

interchangeably.”); *ABF Freight Sys., Inc. v. Int’l Bhd. of Teamsters*, 645 F.3d 954, 959 (8th Cir. 2011) (citing *Lujan* for the proposition that “[a] ‘legally protected interest’ requires only a ‘judicially cognizable interest’”); *Lujan*, 504 U.S. at 561-63, 575, 578 (initially stating that a plaintiff must have suffered “an invasion of a legally protected interest” to satisfy Article III but then reverting to use of the term “cognizable” to characterize the viability of that interest to establish standing); *Bennett v. Spear*, 520 U.S. 154, 167 (1997) (stating that “standing requires: (1) that the plaintiff have suffered an ‘injury in fact’—an invasion of a judicially cognizable interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical”); *Warth*, 422 U.S. at 514 (referring to a “judicially cognizable injury” in the context of discussing the legality of Congress expanding by statute the interests that may establish standing). Adding to the uncertainty, in some cases the Supreme Court makes no mention whatsoever of the requirement that an injury entail the invasion of either a “legally protected” or “judicially cognizable” interest. *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1147 (2013) (“To establish Article III standing, an injury must be ‘concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.’” (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010))); *Massachusetts v. EPA*, 549 U.S. 497, 517 (2007) (“To ensure the proper adversarial presentation, *Lujan* holds that a litigant must demonstrate that it has suffered a concrete and particularized injury that is either actual or imminent, that the injury is fairly traceable to the defendant, and that it is likely that a favorable decision will redress that injury.”).

Deciphering the meaning of the phrase “legally protected interest” also is muddled by the varying approaches courts use to identify the relevant “interest” at stake. In at least one case the United States Court of Appeals for the Fourth Circuit suggested that the interest at issue could be

considered subjectively from the perspective of the party asserting standing. *Doe v. Pub. Citizen*, 749 F.3d 246, 262 (4th Cir. 2014) (intimating that litigants need only assert an interest that “in their view” was protected by the common law or the Constitution). Other courts focus objectively on whether the Constitution, a statute or the common law actually recognizes the asserted interest. *See, e.g., Sargeant v. Dixon*, 130 F.3d 1067, 1069 (D.C. Cir. 1997) (stating that “[a] legally cognizable interest means an interest recognized at common law or specifically recognized as such by the Congress”).

Still other courts have examined whether the type or form of the injury is traditionally deemed to be a legal harm, such as an economic injury or an invasion of property rights, although such an inquiry can blend into the question of whether the injury is concrete and particularized. *See, e.g., Danvers Motor Co., Inc. v. Ford Motor Co.*, 432 F.3d 286, 293 (3d Cir. 2005) (stating that “[m]onetary harm is a classic form of injury-in-fact” that “is often assumed without discussion” and an invasion of property rights, “whether it sounds in tort . . . or contract . . . undoubtedly ‘affect[s] the plaintiff in a personal and individual way’” (quoting *Lujan*, 504 U.S. at 560 n.1)). At least one court has found standing by analogizing to interests that were never advanced by the party asserting standing.⁶ *See In re Special Grand Jury 89-2*, 450 F.3d at

⁶ It is unclear how this approach can be reconciled with the Supreme Court’s admonitions that standing “is gauged by the specific common-law, statutory or constitutional claims *that a party presents*,” *Int’l Primate Prot. League*, 500 U.S. at 77 (emphasis added), and a “federal court is powerless to create its own jurisdiction by embellishing otherwise deficient allegations of standing,” *Whitmore*, 495 U.S. at 155-56. The Tenth Circuit opined that the Supreme Court’s decision in *Bennett*, 520 U.S. at 167, presented a “new locution” according to which the substitution of the phrase “judicially cognizable interest” for “legally protected interest” signaled that the Supreme Court had abandoned *Lujan*’s requirement of a “legally protected interest” in favor of a formulation that provides that “an interest can support standing even if it is not protected by law (at least, not protected in the particular case at issue) so long as it is the sort of interest that courts think to be of sufficient moment to justify judicial intervention.” *In re Special Grand Jury 89-2*, 450 F.3d at 1172. The question of whether the Supreme Court intended to abandon the requirement for a “legally protected interest” seems to have been

1172-1173 (characterizing former grand jurors' requests to lift the secrecy obligation imposed by Rule 6(e) of the Federal Rules of Criminal Procedure as an interest in "stating what they know" that mirrors the First Amendment claims of litigants challenging speech restrictions and commenting that "there is no requirement that the legal basis for the interest of a plaintiff that is 'injured in fact' be the same as, or even related to, the legal basis for the plaintiff's claim, at least outside the taxpayer-standing context").

Although no universal definition of the phrase "legally protected interest" has been developed by the case law,⁷ the Supreme Court and a majority of federal jurisdictions have concluded that an interest is not "legally protected" or cognizable for the purpose of establishing standing when its asserted legal source—whether constitutional, statutory, common law or

resolved in the negative by the Supreme Court's decision in *Raines*, which was decided shortly after *Bennett* and was joined by Justice Antonin Scalia, the author of the Court's unanimous decision in *Bennett*. In *Raines*, as stated *supra*, the Supreme Court "stressed that the alleged injury must be legally and judicially cognizable" and went on to state that "[t]his requires, among other things, that the plaintiff have suffered 'an invasion of a legally protected interest which is . . . concrete and particularized.'" 521 U.S. at 819 (quoting *Lujan*, 504 U.S. at 560). The Supreme Court's recent decision in *Spokeo* also employs the locution requiring that, "[t]o establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" 136 S. Ct. at 1548 (quoting *Lujan*, 504 U.S. at 560) (emphasis added).

⁷ The bewildering state of the law might explain in part why one commentator has referred to the "injury in fact" requirement as "a singularly unhelpful, even incoherent, addition to the law of standing," William A. Fletcher, *The Structure of Standing*, 98 Yale L.J. 221, 231 (1988), and another has taken what the United States Court of Appeals for the Tenth Circuit described as the "somewhat cynical view" that "[t]he only conclusion [regarding what injuries are sufficient for standing] is that in addition to injuries to common law, constitutional, and statutory rights, a plaintiff has standing if he or she asserts an injury that the Court deems sufficient for standing purposes." *In re Special Grand Jury 89-2*, 450 F.3d at 1172 (second alteration in original) (quoting Erwin Chemerinsky, *Federal Jurisdiction* § 2.3.2 at 74 (4th ed.2003)).

otherwise—does not apply or does not exist. The United States Court of Appeals for the District of Columbia Circuit (the “D.C. Circuit”)⁸ has offered the following explanation:

Whether a plaintiff has a legally protected interest (and thus standing) does not depend on whether he can demonstrate that he will succeed on the merits. Otherwise, every unsuccessful plaintiff will have lacked standing in the first place. Thus, for example, one can have a legal interest in receiving government benefits and consequently standing to sue because of a refusal to grant them even though the court eventually rejects the claim. *See generally Public Citizen v. United States Dep’t of Justice*, 491 U.S. 440, 109 S. Ct. 2558, 105 L.Ed.2d 377 (1989) (plaintiffs had standing to bring suit under [Federal Advisory Committee Act (“FACA”), 5 U.S.C. App. §§ 1-15] although claim failed). Indeed, in *Lujan* the Court characterized the “legally protected interest” element of an injury in fact simply as a “cognizable interest” and, without addressing whether the claimants had a statutory right to use or observe an animal species, concluded that the desire to do so “undeniably” was a cognizable interest. *Lujan*, 504 U.S. at 562–63, 112 S. Ct. at 2137–38.

On the other hand, if the plaintiff’s claim has no foundation in law, he has no legally protected interest and thus no standing to sue. *See, e.g., Arjay Assocs. v. Bush*, 891 F.2d 894, 898 (Fed. Cir. 1989) (“We hold that appellants lack standing because the injury they assert is to a nonexistent right”); *ACLU v. FCC*, 523 F.2d 1344, 1348 (9th Cir. 1975) (“If ACLU’s claim is meritorious, standing exists; if not, standing not only fails but also ceases to be relevant.”); *United Jewish Org. of Williamsburgh v. Wilson*, 510 F.2d 512, 521 (2d Cir. 1975) (“Whether our decision on this point is cast on the merits or as a matter of standing is probably immaterial.”), *aff’d*, 430 U.S. 144, 97 S. Ct. 996, 51 L.Ed.2d 229 (1977).

Claybrook v. Slater, 111 F.3d 904, 907 (D.C. Cir. 1997). Furthermore, although the question of whether a litigant’s interest is “legally protected” does not depend on the merits of the claim, it nevertheless is the case that “there are instances in which courts have examined the merits of the underlying claim and concluded that the plaintiffs lacked a legally protected interest and therefore lacked standing.” *Skull Valley Band of Goshute Indians v. Nielson*, 376 F.3d 1223, 1236 (10th Cir. 2004) (citing *Skull Valley Band of Goshute Indians v. Leavitt*, 215 F. Supp. 2d 1232, 1240–41 (D. Utah 2002) (discussing cases), *Claybrook*, 111 F.3d at 907, and *Arjay Assocs.*

⁸ For brevity and convenience, this opinion hereinafter will omit the phrase “United States Court of Appeals for the” from the identification of federal circuit courts of appeal.

Inc. v. Bush, 891 F.2d 894, 898 (Fed. Cir. 1989)). *Accord Martin v. S.E.C.*, 734 F.3d 169, 173 (2d Cir. 2013) (per curiam) (declining to reach the merits of a litigant's claims when standing was lacking "except to the extent that the merits overlap with the jurisdictional question").

In *McConnell v. FEC*, 540 U.S. 93 (2003), *overruled in part on other grounds*, *Citizens United v. FEC*, 558 U.S. 310 (2010), the Supreme Court concluded that a group of litigants lacked Article III standing because their claims could not be deemed "legally cognizable" when the Court had never previously recognized the broadly-asserted interest and that interest was premised on a mistaken interpretation of inapplicable legal precedent. The litigants in *McConnell* consisted in part of a group of voters, organizations representing voters, and candidates who collectively challenged, among other things, the constitutionality of a particular section of the Bipartisan Campaign Reform Act of 2002 ("BCRA") that amended the Federal Election Campaign Act of 1971 ("FECA") by "increas[ing] and index[ing] for inflation certain FECA contribution limits." 540 U.S. at 226. As relevant here, the litigant group argued that, as a result of the amendments, they suffered an injury they identified as the deprivation of an "equal ability to participate in the election process based on their economic status." *Id.* at 227. The group asserted that this injury was legally cognizable according to voting-rights case law that they viewed as prohibiting "electoral discrimination based on economic status . . . and upholding the right to an equally meaningful vote." *Id.* (internal quotation marks omitted). The Supreme Court, however, disclaimed the notion that it had ever "recognized a legal right comparable to the broad and diffuse injury asserted by the . . . plaintiffs." *Id.* In addition, the group's "reliance on this Court's voting rights cases [was] misplaced" because those cases required only "nondiscriminatory access to the ballot and a single, equal vote for each voter" whereas the group had not claimed that they were denied such equal access or the right to vote. *Id.* The

Court further stated that it had previously “noted that ‘[p]olitical ‘free trade’ does not necessarily require that all who participate in the political marketplace do so with exactly equal resources,’” so the group’s “claim of injury . . . is, therefore, not to a legally cognizable right.” *Id.* (quoting *FEC v. Massachusetts Citizens for Life, Inc.*, 479 U.S. 238, 257 (1986)).

In *Bond v. Utreras*, 585 F.3d 1061, 1065-66 (7th Cir. 2009), the Seventh Circuit reviewed a district court order lifting a protective order and permitting a journalist to intervene in a civil rights case involving allegations that Chicago police officers mentally and physically abused a plaintiff while performing their official duties. The journalist sought to “unseal” police department records relating to citizen complaints against Chicago police officers that the city had produced during pretrial discovery but never filed with the court. *Id.* at 1066. The journalist claimed that no good cause existed to continue the protective order under Rule 26(c) of the Federal Rules of Civil Procedure. *Id.* at 1065. Several months after dismissing the underlying lawsuit, which had settled, *id.*, the district court “reevaluated whether ‘good cause’ existed to keep the documents confidential, and in so doing applied a ‘presumption’ of public access to discovery materials,” *id.* at 1067. On balance, the district court concluded that the city’s interest in keeping the records confidential was outweighed by the public’s interest in information about police misconduct; as a result, the court granted the journalist’s request to intervene and lifted the protective order. *Id.* On appeal by the city, the Seventh Circuit characterized as a “mistake” the district court’s failure to consider whether the journalist had standing in view of the fact that the underlying lawsuit had been dismissed. *Id.* at 1068. The Seventh Circuit held that a third party seeking permissive intervention to challenge a protective order after a case has been dismissed “must meet the standing requirements of Article III in addition to Rule 24(b)’s requirements for permissive intervention.” *Id.* at 1072. Discussing Article III’s standing requirements, *id.* at

1072-73, the Seventh Circuit noted that, “while a litigant need not definitely ‘establish that a right of his has been infringed,’ he ‘must have a colorable *claim* to such a right’ to satisfy Article III,” *id.* at 1073 (emphasis in original) (quoting *Aurora Loan Servs., Inc. v. Craddieth*, 442 F.3d 1018, 1024 (7th Cir. 2006)). Because the district court’s decision to lift the protective order was premised on a presumptive right of access to discovery materials, *id.* at 1067, the Seventh Circuit analyzed the legal basis of such a presumptive right and concluded that, while “most documents filed in court are presumptively open to the public,” *id.* at 1073, it nevertheless is the case that “[g]enerally speaking, the public has no constitutional, statutory (rule-based), or common-law right of access to *unfiled* discovery,” *id.* at 1073 (emphasis in original). The Seventh Circuit also found no support for the notion that Rule 26(c) “creates a freestanding public right of access to unfiled discovery.” *Id.* at 1076. It then proceeded to consider and reject whether, alternatively, the First Amendment supplied such a right. *Id.* at 1077-78. Lacking any legal basis to assert a right to unfiled discovery, the Seventh Circuit held that the journalist “has no injury to a legally protected interest and therefore no standing to support intervention.” *Id.* at 1078.

Griswold v. Driscoll, 616 F.3d 53 (1st Cir. 2010), is another instructive case. The First Circuit held that litigants lacked a legally protected interest because the source of the interest, the First Amendment, did not apply. In *Griswold*, students, parents, teachers, and the Assembly of Turkish American Associations (“ATAA”) collectively challenged a decision by the Commissioner of Elementary and Secondary Education of Massachusetts to revise a statutorily-mandated advisory curriculum guide. 616 F.3d at 54-56. The Commissioner’s initial revisions were motivated by political pressure to assuage a Turkish cultural organization that objected to the curriculum guide’s references to the Armenian genocide as biased for failing to acknowledge an opposing contra-genocide perspective. *Id.* at 54-55. After the revised curriculum guide was

submitted to legislative officials, the Commissioner again modified it – at the request of Armenian descendants – by removing references to all pro-Turkish websites (including websites that presented the contra-genocide perspective) except the Turkish Embassy’s website. *Id.* at 55. The plaintiffs sued claiming that the revisions to the curriculum guide were made in violation of their rights under the First Amendment to “inquire, teach and learn free from viewpoint discrimination . . . and to speak.” *Id.* at 56. In an opinion notable for its authorship by U.S. Supreme Court Associate Justice David Souter (Ret.), sitting by designation, the First Circuit affirmed the dismissal of the ATAA’s First Amendment claim as time barred and then considered whether the remaining plaintiffs had standing to assert a First Amendment right. *Id.* Remarking that “we see this as a case in which the dispositive questions of standing and statement of cognizable claim are difficult to disentangle,” the First Circuit found it “prudent to dispose of both standing and merits issues together.” *Id.* The First Circuit then evaluated whether the challenged advisory curriculum guide was analogous to a virtual school library—in which case the revisions to the guide would be subject to First Amendment review pursuant to the plurality decision in *Board of Education, Island Trees Union Free School District No. 26 v. Pico*, 457 U.S. 853 (1982)—or whether the guide was more properly characterized as an element of curriculum over which the State Board of Education may exercise discretion. *Id.* at 56-60. The First Circuit ultimately regarded the complaint as pleading “a curriculum guide claim that should be treated like one about a library, in which case pleading cognizable injury and stating a cognizable claim resist distinction.” *Id.* at 56. Declining to extend “the *Pico* plurality’s notion of non-interference with school libraries as a constitutional basis for limiting the discretion of state authorities to set curriculum,” the First Circuit found that the guide was an element of curriculum, *id.* at 59, so that “revisions to the Guide after its submission to legislative officials,

even if made in response to political pressure, did not implicate the First Amendment,” *id.* at 60. The First Circuit therefore affirmed the lower court’s judgment that the First Amendment did not apply to the challenged curriculum guide and, as a result, the plaintiffs had failed to establish either a cognizable injury or a cognizable claim. *Id.* at 56, 60.

The D.C. Circuit’s decision in *Claybrook*, cited *supra*, also lends authority to the proposition that a party lacks standing when the statutory, constitutional, common law or other source of the asserted legal interest does not apply or does not exist. *Claybrook* involved a lawsuit filed by Joan Claybrook, a co-chair of Citizens for Reliable and Safe Highways (“CRASH”), who sued the Administrator of the Federal Highway Administration (“FHWA”) for failing to prevent an agency advisory committee from passing a resolution that criticized CRASH’s fund-raising literature. 111 F.3d at 905, 906. Claybrook claimed that the Administrator violated the Federal Advisory Committee Act (“FACA”), 5 U.S.C. App. §§ 1-15, by permitting the advisory committee to vote on and pass the challenged resolution, which Claybrook claimed was not on the committee’s agenda and not within the committee’s authority. *Id.* at 906. The Administrator countered by arguing that Claybrook lacked standing “because the legal duty she claims he violated does not exist.” *Id.* at 907. Upon analysis of the relevant provisions of FACA, 5 U.S.C. App. §§ 9(c)(B), 10(a)(1), 10(a)(2), 10(e), 10(f), the D.C. Circuit agreed that the Act did not impose the asserted legal duty that served as a basis for Claybrook’s claimed injury, the agency otherwise complied with the Act, and the decision to adjourn the advisory committee meeting was committed to the agency’s discretion pursuant to 5 U.S.C. § 701(a)(2). *Id.* at 907-909. Because FACA offered no recourse to Claybrook, the D.C. Circuit held that “[i]n sum, we are left with no law to apply to Claybrook’s claim and consequently Claybrook lacks standing.” *Id.* at 909.

The Ninth Circuit reached a similar result in *Fleck & Assocs., Inc. v. Phoenix, an Arizona Mun. Corp.*, 471 F.3d 1100 (9th Cir. 2006). The appellant in *Fleck & Assocs.* was a “for-profit corporation that operate[d] . . . a gay men’s social club in Phoenix, Arizona” where “[s]exual activities [took] place in the dressing rooms and in other areas of the club.” 471 F.3d at 1102. Pursuant to a Phoenix ordinance banning the operation of live sex act businesses, a social club operated by the appellant was subjected to a police search during which two employees were questioned and detained. *Id.* at 1102-1103. The appellant was also “threatened with similar actions.” *Id.* at 1103. The appellant sued the city seeking both injunctive and declaratory relief on the ground that the ordinance violated its constitutional privacy rights. *Id.* at 1102. The district court interpreted the appellant’s complaint to raise one claim based on the invasion of its customers’ privacy rights and a second claim based on the invasion of the appellant’s rights as a corporation. *Id.* at 1103. With respect to the claim based on the customers’ privacy rights, the district court found that the appellant lacked standing to pursue that claim and, alternatively, the appellants’ customers had no privacy rights in the social club so dismissal was further warranted for failure to state a claim for relief. *Id.* The district court held, however, that the appellant had standing to assert its own privacy rights as a corporation, albeit “[t]he court did not . . . identify what those corporate rights might have been” and “immediately proceeded to hold that [the appellant] lacked any cognizable privacy rights and dismissed for failure to state a claim.” *Id.* On appeal, the Ninth Circuit agreed with the district court that the appellant lacked associational standing⁹ to assert its customers’ rights but held that the district court erred by addressing the merits of the customers’ privacy rights in the social club when the court lacked subject matter

⁹ “Under the doctrine of ‘associational’ or ‘representational’ standing an organization may bring suit on behalf of its members whether or not the organization itself has suffered an injury from the challenged action.” *Id.* at 1105.

jurisdiction. *Id.* at 1103, 1105, 1106. Discussing the appellant's claim of "traditional" Article III standing based on its asserted privacy rights as a corporation, the Ninth Circuit noted that the appellant "squarely identifie[d] the source of its supposed right as the liberty guarantee described in *Lawrence v. Texas*, 539 U.S. 558, 123 S. Ct. 2472, 156 L. Ed. 2d 508 (2003)." *Id.* at 1104. The Ninth Circuit determined, however, that no corporate right to privacy emanated from that case, *id.* at 1105, 1106, and, as a result, "[b]ecause the right to privacy described in *Lawrence* is purely personal and unavailable to a corporation, [the appellant corporation] failed to allege an injury in fact sufficient to make out a case or controversy under Article III," *id.* at 1105.

In *Muntaqim v. Coombe*, 449 F.3d 371 (2d Cir. 2006) (en banc) (per curiam), the Second Circuit considered a prisoner's complaint challenging New York Election Law section 5-106 on the ground that it denied felons the right to vote in violation of section 2 of the Voting Rights Act "because it 'result[ed] in a denial or abridgement of the right . . . to vote on account of race.'" 449 F.3d at 374 (quoting 42 U.S.C. § 1973(a), transferred to 52 U.S.C. § 10301). Because the prisoner was a resident of California before he was incarcerated, *id.* at 374, and the Second Circuit concluded that "under New York law, [his] involuntary presence in a New York prison [did] not confer residency for purposes of registration and voting," *id.* at 376, the court found that "his inability to vote in New York arises from the fact that he was a resident of California, not because he was a convicted felon subject to the application of New York Election Law section 5-106," *id.* As a result, the Second Circuit held that that the prisoner "suffered no 'invasion of a legally protected interest.'" *Id.* (quoting *Lujan*, 504 U.S. at 560).

Other federal circuits similarly have concluded that, when the source of the legal interest asserted by a litigant does not apply or does not exist, the litigant has not established a colorable claim to a right that is "legally protected" or "cognizable" for the purpose of establishing an

injury in fact that satisfies Article III's standing requirement. *See, e.g., 24th Senatorial Dist. Republican Comm. v. Alcorn*, 820 F.3d 624, 633 (4th Cir. 2016) (finding that "[b]ecause neither Virginia law nor the Plan [of Organization that governs the Republican Party of Virginia] gives [the litigant] 'a legally protected interest' in determining the nomination method in the first place, he fails to make out 'an invasion of a legally protected interest,' i.e. actual injury, in this case" (quoting *Lujan*, 504 U.S. at 560) (emphasis in original)); *Spirit Lake Tribe of Indians ex rel. Comm. of Understanding and Respect v. Nat'l Collegiate Athletic Ass'n*, 715 F.3d 1089, 1092 (8th Cir. 2013) (noting that injury resulting from a college ceasing to use a Native American name, "even if . . . sufficiently concrete and particularized . . . does not result from the invasion of a legally protected interest"); *White v. United States*, 601 F.3d 545, 555 (6th Cir. 2010) (stating that the plaintiffs "must demonstrate an injury-in-fact to a legally protected interest" but failed to do so because "none of the purported 'constitutional' injuries actually implicates the Constitution"); *Pichler v. UNITE*, 542 F.3d 380, 390-92 (3d Cir. 2008) (affirming dismissal on the ground that litigants failed to establish an injury to a "legally protected interest" because the Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725, was interpreted to apply only to an individual whose personal information was contained in a motor vehicle record and not to spouses who might share that same personal information but were not the subject of the motor vehicle record); *Bochese*, 405 F.3d at 984 (litigant was not an intended beneficiary of a contract amendment so he "had no 'legally cognizable interest' in that agreement and therefore lack[ed] standing to challenge its rescission"); *Aiken v. Hackett*, 281 F.3d 516, 519-20 (6th Cir. 2002) (appellants who claimed they were denied a benefit in violation of the Equal Protection Clause but did not allege that they would have received the benefit under a race-neutral policy lacked standing because they "failed to allege the invasion of a right that the law

protects”); *Arjay Assocs.*, 891 F.2d at 898 (stating that “[b]ecause appellants have no right to conduct foreign commerce in products excluded by Congress, they have in this case no right capable of judicial enforcement and have thus suffered no injury capable of judicial redress”).

III.

Several considerations favor the above-described understanding of the injury in fact requirement, the first of which is its inherent logic. For an interest to be deemed “legally” protected or cognizable it must have some foundation in the law. *Claybrook*, 111 F.3d at 907 (stating, as quoted above, that “if the plaintiff’s claim has no foundation in the law, he has no legally protected interest”). Thus, if the interest underlying a litigant’s claimed injury is premised on a law that does not apply or does not exist, it directly follows that the litigant does not possess an interest that is “legally protected.” *Cf. Pender*, 788 F.3d at 366 (indicating that a legally protected interest “aris[es] from constitutional, statutory, or common law” (citing *Lujan*, 504 U.S. at 578)).

Another consideration is the degree to which the approach taken by the majority of jurisdictions remains faithful to the proper role of standing as an element of Article III’s constitutional limit on the exercise of judicial power. As the Supreme Court has said, “the Constitution extends the ‘judicial Power’ of the United States only to ‘Cases’ and ‘Controversies’” and the Court “ha[s] always taken this to mean cases and controversies of the sort traditionally amenable to, and resolved by, the judicial process.” *Steel Co.*, 523 U.S. at 102. “Such a meaning is fairly implied by the text, since otherwise the purported restriction upon the judicial power would scarcely be a restriction at all.” *Id.* Declining to exercise jurisdiction to entertain a litigant’s claim for which no law can be properly invoked and, as a result, no legally protected interest can be said to have been wrongfully invaded, comports with standing’s role as a limitation on judicial power. A contrary approach to standing would effect an expansion of

judicial power without due regard for the autonomy of co-equal branches of government or the way in which the exercise of judicial power “can so profoundly affect the lives, liberty, and property of those to whom it extends,” *Valley Forge Christian Coll.*, 454 U.S. at 473.¹⁰

Most importantly, this matter poses separation-of-powers concerns. The Supreme Court has observed that the “standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional.” *Raines*, 521 U.S. at 819-20. The Movants bring a constitutional claim that implicates the authorities of co-equal branches of the government. First, the decisions the Movants seek have been classified by the Executive Branch in accordance with its constitutional authorities and the portions of the opinions that the Executive Branch has declassified have already been released. The Supreme Court has stressed that “[t]he President, after all, is the ‘Commander in Chief of the Army and Navy of the United States’” and “[h]is authority to classify and control access to information bearing on national security . . . flows primarily from this constitutional investment of power in the President and exists quite apart from any explicit congressional grant.” *Dep’t of the Navy v. Egan*, 484 U.S. 518, 527 (1988). Accordingly, “[f]or ‘reasons . . . too obvious to call for enlarged discussion,’ *CIA v. Sims*, 471 U.S. 159, 170, 105 S.Ct. 1881, 1888, 85 L.Ed.2d 173 (1985), the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it.” *Egan*, 484 U.S. at 529.

¹⁰ Some might object that litigants should have an opportunity to develop the facts before a court assesses the scope or applicability of an asserted right. *E.g.*, *Judicial Watch*, 432 F.3d at 363 (Williams, J., concurring) (stating that “the use of the phrase ‘legally protected’ to require showing of a substantive right would thwart a major function of standing doctrine—to avoid premature judicial involvement in resolution of issues on the merits”). This case does not implicate those concerns. No amount of factual development would alter the outcome of the question of whether the First Amendment applies and affords a qualified right of access to classified, ex parte FISA proceedings.

“[U]nless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs.” *Id.* In this case, the Movants seek access to information contained in this Court’s opinions that the Executive Branch has determined is classified national security information.

Second, in the exercise of its constitutional authorities to make laws, *see United States v. Kebodeaux*, 133 S. Ct. 2496, 2502 (2013) (discussing Congress’s broad authority to make laws pursuant to the Constitution’s Necessary and Proper Clause), Congress has directed by statute that “[t]he record of proceedings under [FISA], including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence,” 50 U.S.C.

§ 1803(c). While Congress has also established means by which certain opinions of this Court are to be subject to a declassification review and made public, it has made Executive Branch officials acting independently of the Court responsible for these actions. *See infra* Part V.

To be clear, the classified material the Movants’ seek is not subject to sealing orders entered by this Court. *See* Movants’ Reply In Supp. of Their Mot. for Release of Ct. Records 16 (requesting that the Court “unseal” the judicial opinions and release them “with only those redactions essential to protect information that the Court determines, after independent review, to warrant continued sealing”). No such orders were imposed in the cases in which the sought-after judicial opinions were issued; consequently, no question about the propriety of a sealing order is at play in this matter. The entirety of the information sought by the Movants is classified information redacted from public FISC opinions that is being withheld by the Executive Branch pursuant to its independent classification authorities and remains subject to the statutory mandate that the FISC maintain its records under the aforementioned security procedures. Adjudication

of the Movants' motion could therefore require the Court to delve into questions about the constitutionality, pursuant to the First Amendment, of the Executive Branch's national security classification decisions or the scope and constitutional validity of the statute's mandate that this Court maintain material under the required security procedures.

Together, these considerations commend the path paved by the majority of jurisdictions, which have held that an interest is not "legally protected" for the purpose of establishing standing when the constitutional, statutory or common-law source of the interest does not apply or does not exist. It bears emphasizing that the only interest the Movants identify to establish standing in this case is a qualified right to access judicial opinions. *Mot. for Release of Ct. Records 1, 2, 10*. The Movants claim that this interest is legally protected by the First Amendment. *Id.* at 10. The Movants further assert that this legally protected interest—that is, the qualified right to access judicial documents as protected by the First Amendment—was invaded when they were denied access to this Court's judicial opinions addressing the legality of bulk data collection, thereby causing injury. *Id.* Accordingly, the question for the Court is whether the First Amendment applies.

IV.

Access to judicial records is not expressly contemplated by the First Amendment, which states that “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.” U.S. CONST. amend. I. The Supreme Court, however, has inferred that, in conjunction with the Fourteenth Amendment, “[t]hese expressly guaranteed freedoms share a common core purpose of assuring freedom of communication on matters relating to the functioning of government.” *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 575 (1980) (plurality opinion). The Supreme Court has further explained that “[i]n guaranteeing freedoms such as those of speech and press, the First Amendment can be read as protecting the right of everyone to attend trials so as to give meaning to these explicit guarantees” and “[w]hat this means in the context of trials is that the First Amendment guarantees of speech and press, standing alone, prohibit government from summarily closing courtroom doors which had long been open to the public at the time that Amendment was adopted.” *Id.*

In *Richmond Newspapers*, the Supreme Court “firmly established for the first time that the press and general public have a constitutional right of access to criminal trials.” *Globe Newspaper Co v. Superior Court*, 457 U.S. 596, 603 (1982). The Supreme Court has advised, however, that, “[a]lthough the right of access to criminal trials is of constitutional stature, it is not absolute,” *id.* at 607, but “may be overcome only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest,” *Press-Enter. Co. v. Superior Court*, 464 U.S. 501, 510 (1984) (“*Press-Enterprise I*”). The Supreme Court has extended this qualified First Amendment right of public access only to

criminal trials, *Richmond Newspapers*, 448 U.S. at 580, the voir dire examination of jurors in a criminal trial, *Press-Enterprise I*, 464 U.S. at 508-13, and criminal preliminary hearings “as they are conducted in California,” *Press-Enter. Co. v. Superior Court*, 478 U.S. 1, 13 (1986) (“*Press-Enterprise II*”). Most circuit courts, though, “have recognized that the First Amendment right of access extends to civil trials and some civil filings.” *ACLU v. Holder*, 673 F.3d 245, 252 (4th Cir. 2011). To date, however, the Supreme Court has never “applied the *Richmond Newspapers* test outside the context of criminal judicial proceedings or the transcripts of such proceedings.” *Ctr. for Nat’l Sec. Studies v. U.S. Dep’t of Justice*, 331 F.3d 918, 935 (D.C. Cir. 2003). Nor has “the Supreme Court . . . ever indicated that it would apply the *Richmond Newspapers* test to anything other than criminal judicial proceedings.” *Id.* (emphasis in original).

“In *Press-Enterprise II*, the Supreme Court first articulated what has come to be known as the *Richmond Newspapers* ‘experience and logic’ test, by which the Court determines whether the public has a right of access to ‘criminal proceedings.’”¹¹ *Id.* at 934. The “experience” test questions “whether the place and process have historically been open to the press and general public.” *Press-Enterprise II*, 478 U.S. at 8. The “logic” test asks “whether public access plays a significant positive role in the functioning of the particular process in question.” *Id.*

This is not the first occasion on which the Court has confronted the question of whether a qualified First Amendment right of access applies to this Court’s judicial records. Nearly a decade ago, the ACLU sought by motion the release of this Court’s “orders and government

¹¹ In addition to the *Richmond Newspapers* “experience and logic” tests, the Second Circuit has also “endorsed” a “second approach” that holds that “the First Amendment protects access to judicial records that are ‘derived from or a necessary corollary of the capacity to attend the relevant proceedings.’” *In re N.Y. Times Co. to Unseal Wiretap & Search Warrant Materials*, 577 F.3d 401, 409 (2d Cir. 2009) (quoting *Hartford Courant Co. v. Pellegrino*, 380 F.3d 83, 93 (2d Cir. 2004)).

pleadings regarding a program of surveillance of suspected international terrorists by the National Security Agency (NSA) that had previously been conducted without court authorization.” *In re Motion for Release of Court Records*, 526 F. Supp. 2d at 485. Assuming, for the sake of argument, that a qualified First Amendment right of access might extend to judicial proceedings other than criminal proceedings, the Court applied the requisite “experience” and “logic” tests acknowledged by the Supreme Court in *Press-Enterprise II* to determine whether such a right attached to the FISA electronic surveillance proceedings in which the sought-after orders and pleadings were filed. *Id.* at 491-97.

Considering the “experience” test first, the Court in *In re Motion for Release of Court Records* noted that “[t]he FISC ha[d] no . . . tradition of openness”; it “ha[d] never held a public hearing in its history”; a “total of two opinions ha[d] been released to the public in nearly three decades of operation”; the Court “ha[d] issued literally thousands of classified orders to which the public has had no access”; there was “no tradition of public access to government briefing materials filed with the FISC” or FISC orders; and the publication of two opinions of broad legal significance failed to establish a tradition of public access given the fact that “the FISC ha[d] . . . issued other legally significant decisions that remain classified and ha[d] not been released to the public . . .” 526 F. Supp. 2d at 492-93. Accordingly, the Court determined that “the FISC is not a court whose place or process has historically been open to the public” and the “experience” test was not satisfied. *Id.* at 493.

As far as the “logic” test was concerned, although the Court in *In re Motion for Release of Court Records* agreed that public access might result in a more informed understanding of the Court’s decision-making process, provide a check against “mistakes, overreaching or abuse,” and benefit public debate, *id.* at 494, it found that “the detrimental consequences of broad public

access to FISC proceedings or records would greatly outweigh any such benefits” and would actually imperil the functioning of the proceedings:

The identification of targets and methods of surveillance would permit adversaries to evade surveillance, conceal their activities, and possibly mislead investigators through false information. Public identification of targets, and those in communication with them, would also likely result in harassment of, or more grievous injury to, persons who might be exonerated after full investigation. Disclosures about confidential sources of information would chill current and potential sources from providing information, and might put some in personal jeopardy. Disclosure of some forms of intelligence gathering could harm national security in other ways, such as damaging relations with foreign governments.

Id. The Court cautioned that “[a]ll these possible harms are real and significant, and, quite frankly, beyond debate,” *id.*, and “the national security context applicable here makes these detrimental consequences even more weighty,” *id.* at 495. In addition, after rejecting the ACLU’s argument that the Court should conduct an independent review of the Executive Branch’s classification decisions under a non-deferential standard, the Court identified numerous ways that “the proper functioning of the FISA process would be adversely affected if submitting sensitive information to the FISC could subject the Executive Branch’s classification [decisions] to a heightened form of judicial review”:

The greater risk of declassification and disclosure over Executive Branch objections would chill the government’s interactions with the Court. That chilling effect could damage national security interests, if, for example, the government opted to forgo surveillance or search of legitimate targets in order to retain control of sensitive information that a FISA application would contain. Moreover, government officials might choose to conduct a search or surveillance without FISC approval where the need for such approval is unclear; creating such an incentive for government officials to avoid judicial review is not preferable. *See Ornelas v. United States*, 517 U.S. 690, 699, 116 S.Ct. 1657, 134 L.Ed.2d 911 (1996) (noting strong Fourth Amendment preference for searches conducted pursuant to a warrant and adopting a standard of review that would provide an incentive for law enforcement to seek warrants). Finally, in cases that are submitted, the free flow of information to the FISC that is needed for an *ex parte* proceeding to result in sound decision[-]making and effective oversight could also be threatened.

Id. at 496. Finding that the weight of all these harms counseled against public access, the Court adopted the reasoning of other courts that “have found that there is no First Amendment right of access where disclosure would result in a diminished flow of information, to the detriment of the process in question,” *id.*, and remarked that this reasoning “compels the conclusion that the ‘logic test’ . . . is not satisfied here,” *id.* at 497.

Because both the “experience” and “logic” tests were “unsatisfied,” the Court concluded that “there [was] no First Amendment right of access to the requested materials.” *Id.* The Court also declined to exercise its own discretion to “undertake the searching review of the Executive Branch’s classification decisions requested by the ACLU, because of the serious negative consequences that might ensue” *Id.* The Court noted, however, that “[o]f course, nothing in this decision forecloses the ACLU from pursuing whatever remedies may be available to it in a district court through a FOIA request addressed to the Executive Branch.” *Id.*

In the motion that is now pending, the Movants acknowledge the decision in *In re Motion for Release of Court Records* but argue that the decision erred by (1) “limiting its analysis to whether two previously published opinions of this Court ‘establish a tradition of public access’” and (2) “concluding that public access would ‘result in a diminished flow of information, to the detriment of the process in question.’” Mot. for Release of Ct. Records 21 (quoting *In re Motion for Release of Court Records*, 526 F. Supp. 2d at 493, 496). Taking these two arguments in order, the first argument is premised on a misreading of the Court’s analysis and an overly broad framing of the legal question. While examining the experience prong of *Richmond Newspapers*, the Court did not “limit” its analysis to two previously-published opinions; to the contrary, the Court made clear that its rationale for holding that there was no tradition of public access to FISC electronic surveillance proceedings was demonstrated by, as stated above, the lack of any

public hearing in the (at that point) approximately 30 years in which the FISC had been operating and the fact that, with *the exception of only two published opinions*, the entirety of the court's proceedings, which consisted of the issuance of thousands of judicial orders, was classified and unavailable to the public. *In re Motion for Release of Court Records*, 526 F. Supp. 2d at 492. In other words, at that time, a minimum of 99.98% of FISC proceedings was classified and nonpublic. It would be an understatement to say that such a percentage reflected a tradition of no public access. Indeed, the Court found that "the ACLU's First Amendment claim runs counter to a long-established and virtually unbroken practice of excluding the public from FISA applications and orders" *Id.* at 493.

The Movants gain no traction challenging *In re Motion for Release of Court Records* by suggesting that the framing of the "experience" test should be enlarged to posit whether public access historically has been available to any "judicial opinions interpreting the meaning and constitutionality of public statutes," Mot. for Release of Ct. Records 14, rather than focusing on whether *FISC proceedings* historically have been accessible to the public. Such an expansive framing of the type or kind of document or proceeding at issue plainly would sweep too broadly because it would encompass grand jury opinions, which often interpret the meaning and constitutionality of public statutes but arise from grand jury proceedings, which are a "paradigmatic example" of proceedings to which no right of public access applies, *In re Boston Herald, Inc.*, 321 F.3d 174, 183 (1st Cir. 2003) (quoting *Press-Enterprise II*, 478 U.S. at 9), and a "classic example" of a judicial process that depends on secrecy to function properly, *Press-Enter. II*, 478 U.S. at 9. As demonstrated by the decision in *Press-Enterprise II*, the Supreme Court certainly contemplated the consideration of narrower subsets of legal documents and proceedings in light of the fact that it entertained the question of whether the First Amendment

right of access applied to a subset of judicial hearing transcripts—i.e., “the transcript of a preliminary hearing growing out of a criminal prosecution,” 478 U.S. at 3—and never intimated that its analysis should (or could) extend to transcripts of *all* judicial hearings growing out of a criminal prosecution. Furthermore, to the extent the Movants take issue with the Court’s formulation of the “experience” test on the ground that it focused too narrowly on FISC practices, Mot. for Release of Ct. Records 21 (arguing that the experience test “does not look to the particular practice of any one jurisdiction”), the fact of the matter is that FISA mandates that the FISC “shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States,” 50 U.S.C. § 1803(a)(1), so the FISC’s virtually-exclusive¹² jurisdiction over such proceedings is a construct of Congress and, thereby, the American people.¹³ The Movants offer no authority to support a suggestion that the concentration of FISC proceedings in one judicial forum detracts from the legitimacy or correctness of applying the “experience” test to FISC proceedings rather than a broader range of proceedings. Accordingly, *In re Motion for Release of Court Records* properly framed the “experience” test to examine whether FISC proceedings—proceedings that relate to applications made by the Executive Branch for the issuance of court orders approving authorities covered exclusively by FISA—have historically been open to the press and general public.

¹² See 50 U.S.C. §§ 1803(a), 1823(a), 1842(b)(1), 1861(b)(1)(A), 1881b(a), 1881c(a)(1). Although applications seeking pen registers, trap-and-trace devices, or certain business records for foreign intelligence purposes may be submitted by the government to a United States Magistrate Judge who has been publicly designated by the Chief Justice of the United States to have the power to hear such applications, FISA makes clear that the United States Magistrate Judge will be acting “on behalf of” a judge of the FISC. 50 U.S.C. §§ 1842(b)(2), 1861(b)(1)(B). In practice, no United States Magistrate Judge has been designated to entertain such applications.

¹³ Although FISC proceedings occur in a single judicial forum, the district court judges designated to comprise the FISC are from at least seven of the United States judicial circuits across the country. 50 U.S.C. § 1803(a)(1).

Attending to the “logic” prong of the constitutional analysis, the Movants argue that the Court “erred in concluding that public access would ‘result in a diminished flow of information, to the detriment of the process in question.’” Mot. for Release of Ct. Records 21 (quoting *In re Motion for Release of Court Records*, 526 F. Supp. 2d at 496). The Movants neglect, however, to explain why they believe this conclusion was flawed; nor do they otherwise refute the Court’s identification of the detrimental effects that could cause a diminished flow of information as a result of public access, see *In re Motion for Release of Court Records*, 526 F. Supp. 2d at 494-96. Instead, the Movants offer the conclusory statement that “disclosure of the requested opinions would serve weighty democratic interests by informing the governed about the meaning of public laws enacted on their behalf.” Mot. for Release of Ct. Records 21. While it undoubtedly is the case that access to judicial proceedings and opinions plays an important, if not imperative, role in furthering the public’s understanding about the meaning of public laws, the Movants cannot ignore the Supreme Court’s instruction that, “[a]lthough many governmental processes operate best under public scrutiny, it takes little imagination to recognize that there are some kinds of government operations that would be totally frustrated if conducted openly.” *Press-Enter. II*, 478 U.S. at 8-9. *In re Motion for Release of Court Records* identified detrimental consequences that could be anticipated if the public had access to open FISC proceedings, some of which the Court noted were “comparable to those relied on by courts in finding that the ‘logic’ requirement for a First Amendment right of access was not satisfied regarding various types of proceedings and records” and the others were described as “distinctive to FISA’s national security context.” 526 F. Supp. 2d at 494. These detrimental consequences, which are quoted above, were deemed to outweigh any benefits public access would add to the functioning of such proceedings, *id.*, and the Court emphasized that “the national security

context applicable here makes these detrimental consequences even more weighty,” *id.* at 495. Because the Movants made no attempt to dispute or discredit these detrimental effects, the resulting diminished flow of information that public access would have on the functioning of FISC proceedings, or the weight the Court gave to the detrimental effects, this Court is left to view their argument as simply a generalized assertion that they disagree with *In re Motion for Release of Court Records*.¹⁴ That disagreement being duly noted, the Movants have not made a persuasive case that the result was wrong. Consequently, this Court has no basis to disclaim the conclusion in *In re Motion for Release of Court Records* that the ‘logic’ test was “not satisfied[,]” *id.* at 497, and, indeed, agrees with it.

Although the records to which the ACLU sought access in *In re Motion for Release of Court Records* implicated only electronic surveillance proceedings pursuant to 50 U.S.C. §§ 1804-1805, *id.* at 486, the analysis applying *Richmond Newspapers*’ “experience” and “logic” tests involved reasoning that more broadly concerned all classified, ex parte FISC proceedings regardless of statutory section. *Id.* 491-97. Notwithstanding the passage of time, that analysis retains its force and relevance.¹⁵ The Court also sees no meaningful difference between the

¹⁴ The Movants specify four ways public access to FISC judicial opinions is “important to the functioning of the FISA system,” Mot. for Release of Ct. Records 17-20; however, the Movants never discuss these benefits vis-à-vis the detrimental effects identified by *In re Motion for Release of Court Records*.

¹⁵ Although there have been several public proceedings since *In re Motion for Release of Court Records* was decided, *see, e.g.*, Misc. Nos. 13-01 through 13-09, available at <http://www.fisc.uscourts.gov/public-filings>, the statistical significance of those public proceedings makes no material difference to the question of whether FISA proceedings historically have been open to the public, especially when considered in light of the many thousands more classified and ex parte proceedings that have occurred since that case was concluded. Furthermore, by and large, those public proceedings have been in the nature of this one whereby, in the wake of the unauthorized disclosures about NSA programs, private parties moved the Court for access to judicial records or for greater transparency about the number of orders issued by the FISC to providers. They are therefore distinguishable from the type of

application of the “experience” and “logic” tests to FISC proceedings versus the application of these tests to sealed wiretap applications pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20. Like FISC proceedings, Title III wiretap applications are “subject to a statutory presumption *against* disclosure,”¹⁶ “have not historically been open to the press and general public,” and are not subject to a qualified First Amendment right of access, *In re N.Y. Times Co. to Unseal Wiretap & Search Warrant Materials*, 577 F.3d 401, 409 (2d Cir. 2009) (emphasis in original). Accordingly, persuaded by *In re Motion for Release of Court Records*, this Court adopts its analysis and, for the reasons stated therein, as well as those discussed above, holds that a First Amendment qualified right of access does not apply to the FISC proceedings that resulted in the issuance of the judicial opinions the Movants now seek, which consist of proceedings pursuant to 50 U.S.C. § 1842 (pen registers and trap and trace devices for foreign intelligence and international terrorism investigations) and 50 U.S.C. § 1861 (access to certain business records for foreign intelligence and international terrorism investigations).

proceedings relevant to the instant motion and to *In re Motion for Release of Court Records*, namely *ex parte* proceedings involving classified government requests for authority to conduct electronic surveillance or other forms of intelligence collection.

¹⁶ Title III mandates that wiretap “[a]pplications made and orders granted under this chapter shall be sealed by the judge.” 18 U.S.C. § 2518(8)(b). As discussed *supra*, FISA mandates that “[t]he record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.” 50 U.S.C. § 1803(c).

V.

As already noted, the only law the Movants cite as the source for their claimed right of public access to FISC judicial opinions is the First Amendment. If any other legal bases existed to secure constitutional standing for these Movants, they were obligated to present them. Because the First Amendment qualified right of access does not apply to the FISC proceedings at issue in this matter, the Movants have no legally protected interest and cannot show that they suffered an injury in fact for the purpose of meeting their burden to establish standing under Article III.¹⁷

To be sure, the Court does not reach this result lightly. However, application of the Supreme Court's test to determine whether a First Amendment qualified right of access attaches to the FISC proceedings at issue in this matter leads to the conclusion that it does not. Absent some other legal basis to establish standing, this means the Court has no jurisdiction to consider causes of action such as this one whereby individuals and organizations who are not parties to FISC proceedings seek access to classified judicial records that relate to electronic surveillance, business records or pen register and trap-and-trace device proceedings. Notably, the D.C. Circuit has advised that "[e]ven if holding that [the litigant] lacks standing meant that no one could initiate" the cause of action at issue "it would not follow that [the litigant] (or anyone else) must have standing after all. Rather, in such circumstance we would infer that 'the subject matter is committed to the surveillance of Congress, and ultimately to the political process.'" *Sargeant*,

¹⁷ The Court's decision involves scrutiny of whether the First Amendment qualified right of access applies, but only as part of the assessment of whether the Movants have standing under Article III. Because they do not, the Court dismisses their Motion for lack of jurisdiction without, strictly speaking, ruling on the merits of their asserted cause of action. Moreover, in the absence of jurisdiction, the Court may not consider any other legal arguments or requests for relief that were advanced in the motion.

130 F.3d at 1070 (quoting *Richardson*, 418 U.S. at 179). Indeed, “[t]he assumption that if [the litigants] have no standing to sue, no one would have standing, is not a reason to find standing.” *Schlesinger v. Reservists Comm. to Stop the War*, 418 U.S. 208 (1974).

Evidence that public access to opinions arising from classified, ex parte FISC proceedings is best committed to the political process is demonstrated by Congress’s enactment of the *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015* (“USA FREEDOM Act of 2015”), Pub. L. 114-23, 129 Stat. 268 (2015), which, after considerable public debate, made substantial amendments to FISA. One such amendment, which is found in § 402 of the USA FREEDOM Act and codified at 50 U.S.C. § 1872(a), added an entirely new provision for the public disclosure of certain FISC judicial opinions. Consequently, FISA now states that “the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court . . . that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term ‘specific selection term’, and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.” 50 U.S.C. § 1872(a). Although the Movants characterize the enactment of this provision of the USA FREEDOM Act as evidence that “favors disclosure of FISC opinions” and bolsters their argument that “public access would improve the functioning of the process in question,” Notice of Supplemental Authority 2 (Dec. 4, 2015), the Court does not believe that this provision alters the First Amendment analysis. FISC proceedings of the type at issue historically have not been, nor presently will be, open to the press and general public given that no amendment to FISA altered the statutory mandate for such proceedings to occur ex parte and

pursuant to the aforementioned security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence. Furthermore, although Congress had the opportunity to do so, it made no amendment to FISA that established a procedure by which the public could seek or obtain access to FISC records directly from the Court. Rather, after informed debate, Congress deemed public access as contemplated by 50 U.S.C. § 1872(a) to be the means that, all things considered, best served the totality of the American people's interests. Accordingly, the USA FREEDOM Act enhances public access to significant FISC decisions, as provided by § 1872(a), and ensures that the public will have a more informed understanding about how FISA is being construed and implemented, which appears to be at the heart of the Movants' interest. Mot. for Release of Ct. Records 2 (stating that "Movants' current request for access to opinions of this Court evaluating the legality of bulk collection seeks to vindicate the public's overriding interest in understanding how a far-reaching federal statute is being construed and implemented, and how constitutional privacy protections are being enforced").

CONCLUSION

For the foregoing reasons, the Court will dismiss for lack of jurisdiction the pending MOTION OF THE AMERICAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF THE NATION'S CAPITAL, AND THE MEDIA FREEDOM AND INFORMATION ACCESS CLINIC FOR THE RELEASE OF COURT RECORDS. A separate order will accompany this Opinion.

January 25th, 2017



ROSEMARY M. COLLYER
Presiding Judge, United States Foreign
Intelligence Surveillance Court

JAN 25 2017

UNITED STATES

LeeAnn Flynn Hall, Clerk of Court

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE OPINIONS & ORDERS OF THIS COURT
ADDRESSING BULK COLLECTION OF DATA
UNDER THE FOREIGN INTELLIGENCE
SURVEILLANCE ACT.

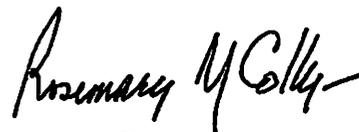
Docket No. Misc. 13-08

ORDER

For the reasons set forth in the accompanying Opinion, it hereby is **ORDERED** that the MOTION OF THE AMERICAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF THE NATION'S CAPITAL, AND THE MEDIA FREEDOM AND INFORMATION ACCESS CLINIC FOR THE RELEASE OF COURT RECORDS is **DISMISSED** for lack of jurisdiction.

SO ORDERED.

January 25th, 2017



ROSEMARY M. COLLYER
Presiding Judge, United States Foreign
Intelligence Surveillance Court

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

IN RE OPINIONS & ORDERS OF THIS COURT)
ADDRESSING BULK COLLECTION OF DATA)
UNDER THE FOREIGN INTELLIGENCE)
SURVEILLANCE ACT)

Docket No. Misc. 13-08

**THE UNITED STATES' LEGAL BRIEF TO THE EN BANC COURT
IN RESPONSE TO THE COURT'S ORDER OF MARCH 22, 2017**

The Presiding Judge's opinion in this case persuasively explains that, because movants have not established an injury to a *legally protected* interest that is applicable here, movants lack Article III standing, and therefore this Court lacks jurisdiction over this action. While two prior opinions of this Court have found jurisdiction over similar actions, neither of those opinions analyzed the question addressed here. The Presiding Judge's opinion is the first from this Court to address this issue, and it does so thoroughly and correctly. The en banc Court should similarly find that there is no Article III jurisdiction here.

BACKGROUND

It is well-settled that there is no First Amendment public right of access to the proceedings, records, and rulings of this Court. *See In re Opinions & Orders of this Court Addressing Bulk Collection of Data under the Foreign Intelligence Surveillance Act*, 2017 WL 427591, at *19-21 (FISA Ct. Jan. 25, 2017); *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, 2014 WL 5442058, at *4 n.10 (FISA Ct. Aug. 7, 2014); *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, 2008 WL 9487946, at *3 (FISA Ct. Aug. 27, 2008); *In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 492-97 (FISA Ct. 2007). Indeed, the en banc Court in this case recognized this principle in the course of

ordering briefing. *See* Order 1, Mar. 22, 2017 (ordering briefing on “the question of whether Movants established Article III standing notwithstanding that a First Amendment qualified right of access does not apply to the judicial opinions they seek”). This conclusion stems from a straightforward application of the Supreme Court’s decision in *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1 (1986). *See also* *Dhiab v. Trump*, __ F.3d __, 2017 WL 1192911, at *5 (D.C. Cir. Mar. 31, 2017) (Op. of Randolph, J.) (observing that “from the beginning of the republic to the present day, there is no tradition of publicizing secret national security information involved in civil cases, or for that matter, in criminal cases,” as the “tradition is exactly the opposite”).

This case, however, is the first in which the Court has considered the related but distinct question of whether, given that it is plain under this Court’s precedent that they lack any First Amendment right of access or other legal right to the material they seek, movants may nonetheless claim an injury to a “legally protected right” as is necessary for Article III standing and thus subject-matter jurisdiction.

I. Prior Decisions of the Court

The first time this Court addressed an argument that the First Amendment provided a right of access to its proceedings and records, the Court rejected the movant’s argument on the merits without addressing the question of Article III standing. *See In re Motion for Release of Court Records*, 526 F. Supp. 2d 484 (FISA Ct. 2007). Applying the standards set forth in *Press-Enterprise*, the Court found both that the movant’s claim ran “counter to a long-established and virtually unbroken practice of excluding the public from FISA applications and orders,” 526 F. Supp. 2d at 493, and that access would not be logical because the “detrimental consequences” from public access “would greatly outweigh any” benefits, *id.* at 494. The Court’s opinion in that case includes a jurisdictional analysis, but that analysis addresses only whether the FISC’s

specialized jurisdiction, as delineated by Congress in the Foreign Intelligence Surveillance Act, permitted it to adjudicate the case. *Id.* at 486-87. The opinion in that case did not address Article III standing.

In a subsequent case, in which three movants claimed a First Amendment right to certain opinions of this Court, the Court addressed a different aspect of Article III standing than the one being considered here, namely whether the movants' claimed injuries were sufficiently concrete and particularized. *See In re Orders of this Court Interpreting Section 215 of the Patriot Act*, 2013 WL 5460064, at *2-4 (FISA Ct. Sept. 13, 2013). The Court found that two of the movants had sufficiently particularized injuries because "access to the [opinions] would assist" them in public debates. *Id.* at *4. The Court dismissed the third movant because the record contained "no information as to how the release of the opinions would aid [that entity's] activities, or how the failure to release them would be detrimental." *Id.* at *4 n.13.¹ The Court did not address whether any injury that may have existed was an injury to a legally protected interest.

II. Procedural Background

In the instant case, three movants sought access to "opinions addressing the legal basis for the 'bulk collection' of data." Mot. for the Release of Court Records I, Nov. 6, 2013. Movants argued that they had Article III standing because they had "a concrete and particularized injury." *Id.* at 10. They asserted a First Amendment right of access to the opinions, notwithstanding earlier decisions from this Court holding that there is no First Amendment right of access to FISC proceedings and rulings. *See id.* at 12-24. Finally, they

¹ Subsequently, the third movant provided a declaration that explained how the documents sought would advance its mission, and the Court reinstated it as a party. *See* Opinion and Order at 10, *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, Misc. 13-02 (FISA Ct. Aug. 7, 2014), available at http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Order-6_0.pdf.

argued that, in implementing the purported constitutional right of access, the Court should first invoke FISC Rule 62(a), order a declassification review, and then set up another round of briefing to adjudicate the government's classification decisions. *Id.* at 24-25.

In its responsive brief, the government noted that the opinions sought by movants had all been identified (there were four) and publicly released, with only classified material redacted. *United States' Opp'n to Mot.* 1-2, Dec. 6, 2013. The government argued that the movants lacked standing to seek an additional classification review or FISC publication because Rule 62(a) provided the movants with no rights. *Id.* at 2-4. The government further observed that both FISC Rule 3 and the FISC's own holdings preclude the Court from ordering the release of information that the executive branch has deemed classified. *Id.* at 4-7. The government noted that Congress has provided a mechanism for judicial review of classification decisions in the Freedom of Information Act ("FOIA"), pursuant to which appropriate review occurs in a district court. *Id.* at 4.

In reply, movants once again asserted their First Amendment arguments, characterizing both Rule 62(a) and FOIA as not "adequate." Reply 3, Dec. 20, 2013.

In an extensive opinion written by the Presiding Judge, the Court addressed for the first time the question of whether, in the absence of any First Amendment or other right of access to FISC opinions, movants can establish an injury to a legally protected interest as is required for Article III standing. Surveying numerous cases from the Supreme Court and circuit courts, this Court observed that "the Supreme Court and a majority of federal jurisdictions have concluded that an interest is not 'legally protected' or cognizable for the purpose of establishing standing when its asserted legal source—whether constitutional, statutory, common law or otherwise—does not apply or does not exist." 2017 WL 427591, at *8. As this Court has previously held

that there is no First Amendment right of access to this Court's proceedings, records, and rulings, and movants had identified no other legal right to the classified material sought, movants could identify no injury to a legally protected interest and thus lacked Article III standing. *Id.* at *9-15.

Movants filed a motion to alter or amend the Court's judgment. Movants' Mot. to Alter or Amend the J. & for Joint Briefing with Case No. Misc. 16-01, Feb. 17, 2017 ("Mot. to Alter or Amend"). They argued that the Presiding Judge's opinion "runs contrary to previous decisions of this Court," *id.* at 4, although the two previous decisions movants cited had not considered the legal question at issue here. *See supra* Part I. Movants further appeared to argue that, even if their First Amendment claim is meritless, they should be able to use their assertion of such a claim as a basis for Article III standing, and then use the resultant jurisdiction to ask the court to release the material sought as a matter of "discretion[]." *Id.* at 5-6.

While the Court has not ruled on the Motion to Alter or Amend, it issued an order calling for en banc review "on the ground that it is necessary to secure or maintain uniformity of the court's decisions." Order 1, Mar. 22, 2017. The Court's en banc order states that it will only be reconsidering the standing question and will not be revisiting the line of cases that have consistently held that there is no First Amendment right of access to FISC proceedings, records, and rulings. *Id.* at 1 n.1.

ARGUMENT

It has long been recognized that "[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 37 (1976). The doctrine of standing is "an essential and unchanging part of the case-or-controversy requirement of Article III." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560

(1992). To establish standing, movants must establish three elements, one of which is injury in fact. “To establish injury in fact, a plaintiff must show [*inter alia*] that he or she suffered ‘an invasion of a legally protected interest.’” *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan*, 504 U.S. at 560).

I. Movants Lack Standing to Assert a First Amendment Claim

As the Presiding Judge’s opinion correctly holds, “when the source of the legal interest . . . does not apply or does not exist, the litigant has not established a colorable claim to a right that is ‘legally protected’ or ‘cognizable’ for the purpose of establishing an injury in fact that satisfies Article III’s standing requirement.” 2017 WL 427591, at *13 (citing cases). Thus, because this Court has previously held that there is no First Amendment right of access to the proceedings, records, or rulings of this Court, movants have no “legally protected interest” that has been injured. Without an injury to a legally protected interest, they lack Article III standing.

While the fact that a litigant may ultimately lose on the merits does not preclude a finding of standing, a litigant must do more than cite a rule of law and identify some relief it would like in order to establish jurisdiction. Rather, there must be an actual legal right that could plausibly apply under the circumstances alleged or presented. As the Seventh Circuit has explained, “the Supreme Court’s standing doctrine requires litigants to establish an injury to an interest that the law protects when it is *wrongfully* invaded, and this is quite different from requiring them to establish a *meritorious* legal claim.” *Bond v. Utreras*, 585 F.3d 1061, 1073 (7th Cir. 2009) (internal quotation marks omitted) (emphasis in original). In other words, to establish standing, a plaintiff need not establish wrongfulness – *i.e.*, that its legal right was unlawfully invaded – but it must establish that there exists an applicable legal right that might plausibly have been invaded.

Thus, a plaintiff invoking the Freedom of Information Act to obtain government agency records will generally have standing even if it ultimately turns out that the documents are properly exempt from disclosure; by contrast, a plaintiff who invokes FOIA to demand original artwork from the National Gallery of Art would lack standing, as the rights conveyed by FOIA plainly do not apply to such artwork. Similarly, a plaintiff asserting a First Amendment right to protest on a public sidewalk near a government building would likely have standing, while a plaintiff asserting a First Amendment right to sit inside the Oval Office or to attend a Supreme Court deliberative conference would not.

The application of this principle here is straightforward. The movants lack an injury to a legally protected interest because they base their claim on a First Amendment right of access that simply does not exist in this context. To be sure, the First Amendment provides rights to movants. And those rights include a right of access to certain places. But, as this Court has repeatedly held, the First Amendment right of access does not extend to proceedings or rulings of the FISC. *See* Order 1, Mar. 22, 2017 (“[A] First Amendment qualified right of access does not apply to the judicial opinions [the Movants] seek.”). Where, as here, a movant’s claim “has no foundation in law, he has no legally protected interest and thus no standing to sue.” *Claybrook v. Slater*, 111 F.3d 904, 907 (D.C. Cir. 1997).

Movants are similarly situated to the plaintiffs in the cases described in the Presiding Judge’s opinion in this case, in which courts found a lack of any legally protected interest, and therefore a lack of Article III standing. *See* 2017 WL 427591, at *9-13. For example, in *McConnell v. FEC*, certain plaintiffs sought to advance an equal protection right that applied in some circumstances, but not in the circumstances at issue in that case. 540 U.S. 93, 227 (2003), *overruled in part on other grounds*, *Citizens United v. FEC*, 558 U.S. 310 (2010). The Supreme

Court examined “the nature and source of the claim asserted,” and found that because the asserted right did not apply, the claim of injury was “not to a legally cognizable right.” *Id.* (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975)). Thus, those plaintiffs lacked standing. *Id.*

In *Bond v. Utreras*, an intervenor asserted an interest similar to the one asserted by movants here, namely a right of access to documents related to a judicial proceeding. *See* 585 F.3d 1061 (7th Cir. 2009). The Seventh Circuit acknowledged the existence of a “general right of public access to judicial records,” but found that, because that right did not extend to the records sought by the intervenor (unfiled discovery documents), the intervenor had “no injury to a legally protected interest and therefore no standing.” *Id.* at 1074, 1078. Similarly, in *Griswold v. Driscoll*, plaintiffs, like movants here, alleged a violation of their First Amendment rights. 616 F.3d 53 (1st Cir. 2010). In an opinion by Retired Justice Souter, the court held that because the First Amendment did not apply to the material at issue, the plaintiffs established neither standing nor a claim. *Id.* at 56, 60.

McConnell v. FEC, *Bond v. Utreras*, and *Griswold v. Driscoll* are just three of the many cases that, as this Court correctly found, support the holding in the Presiding Judge’s opinion. In their motion to alter or amend the judgment, movants cited two cases that they contend are contrary. *See* Mot. to Alter or Amend 5.² But these cases are consistent with the Presiding Judge’s opinion. In each of the cases relied on by movants, the court found that the asserted right did exist and did apply. *See Carlson v. United States*, 837 F.3d 753, 759 (7th Cir. 2016); *Doe v. Public Citizen*, 749 F.3d 246, 264 (4th Cir. 2014). It was on this basis that the court in *Carlson* distinguished *Bond v. Utreras*. *See* 837 F.3d at 760. *Carlson* and *Doe* are likewise

² Movants also argued that their injury “is concrete and particularized.” Mot. To Alter or Amend 4 (citing cases). This argument is a *non sequitur*. Movants injury is insufficient, not because it is generalized or abstract, but because it is not an injury to a legally protected interest.

distinguishable from this case because here, movants have not asserted a right that exists and applies in these circumstances.

II. To the Extent They Assert Any Other Claims, Movants Lack Both Standing and a Cause of Action

In its order inviting en banc briefing, the Court observed that “the First Amendment qualified right of access was the only ground on which Movants asserted standing.” Order 1 n.1, Mar.22, 2017. The government agrees with this observation, but it appears that movants may not. In their motion to alter or amend, movants referred to “all of Movants’ claims,” and challenged what they described as the Court’s conclusion that “in the absence of a viable First Amendment claim, Movants also lack standing to seek relief under Rule 62 [of this Court’s rules] and the Court’s inherent supervisory powers over its own records.” Mot. to Alter or Amend 1, 5. The arguments that movants put forward in this regard are wrong.

Because “standing is not dispensed in gross,” *Lewis v. Casey*, 518 U.S. 343, 358 n.6 (1996), movants “must demonstrate standing for each claim [they] seek[] to press” and “for each form of relief” they seek. *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) (quotation marks omitted). Thus, whether or not movants have standing to assert their First Amendment claim (and they do not), they have to separately establish standing for each additional claim they might assert in this or any case. Because neither this Court’s inherent supervisory powers nor Rule 62 provide any cause of action or legal rights to movants, neither provides a legally protected interest as would be necessary for Article III standing.

The Court’s inherent supervisory powers obviously provide no rights to movants (or anyone else) and cannot support a suit or motion by movants. An opposite conclusion would mean that anyone could file an action in any court to ask the court to take nearly any action with regard to its employees or cases. Movants rely on *In re Motion for Release of Court Records*,

526 F. Supp. 2d 484 (FISA Ct. 2007), but that case provides no support to their position. There, the Court held that it had inherent “jurisdiction in the first instance to adjudicate a claim of right to the court’s” records even though no statute provided such jurisdiction. *Id.* at 487. The inherent jurisdiction was thus jurisdiction to adjudicate a claim of right, but this inherent jurisdiction did not supply either the claim or the right.³

Rule 62 similarly grants movants no rights and no cause of action. That rule provides:

The Judge who authored an order, opinion, or other decision may *sua sponte* or on motion by a party request that it be published. Upon such request, the Presiding Judge, after consulting with other Judges of the Court, may direct that an order, opinion or other decision be published. Before publication, the Court may, as appropriate, direct the Executive Branch to review the order, opinion, or other decision and redact it as necessary to ensure that properly classified information is appropriately protected pursuant to Executive Order 13526 (or its successor).

FISC Rule 62(a).

Movants, of course, are neither the authoring judge of any opinion nor parties to any of the underlying cases at issue. *See In re Orders*, 2013 WL 5460064, at *5 (holding that “the term ‘party’ in Rule 62(a) refers to a party to the proceeding that resulted in the ‘opinion, order, or other decision’ being considered for publication”). Thus, movants can claim no “legally protected interest” stemming from Rule 62. Without such an interest, they can have no standing to invoke the rule. Additionally, the rule does not provide them with any cause of action.

Movants’ argument that this Court’s holding in this case “render[s] the relief afforded by Rule 62 all but illusory,” *Mot. to Alter or Amend* 6, misunderstands the nature of Rule 62. It is a rule of procedure for litigation pending before the Court, not a substantive right for the general

³ Notably, the Court in that case specifically declined to rule on whether it possessed “residual discretion” to release any records. The Court held that even if it had such discretion, it would decline to exercise it “because of the serious negative consequences that might ensue.” 526 F. Supp. 2d at 497. The Court ruled against the movants as to all claims. *See id.*

public. Like most rules of procedure, it governs the parties in cases and does not provide rights or a cause of action to other individuals or entities.

Movants also argue that this Court's holding is "in tension with the canon of constitutional avoidance, because it would require the FISC to resolve constitutional questions (as it did here) before considering the non-constitutional ground for relief presented by Movants." *Id.* But there is no "non-constitutional ground for relief" here, because Rule 62 does not provide any rights or cause of action to movants. Moreover, the canon of constitutional avoidance does not allow a court to assert jurisdiction in instances where Article III of the Constitution does not permit it.⁴

⁴ There is an additional basis for rejecting any "claim" for discretionary dissemination. All of the unclassified material sought in this case has been released. The only remaining responsive material is classified. This Court does not release classified material to the public. FISC Rule 3; *cf. Dhiab*, 2017 WL 1192911, at *5 ("One may be confident that over many years none of the members of our court, past or present, ever supposed that in complying with [rules governing handling of classified material], we were somehow violating the Constitution.").

Of course, "there is no role for this Court independently to review, and potentially override, Executive Branch classification decisions." *Motion for Release*, 526 F. Supp. 2d at 491; *accord Dep't of the Navy v. Egan*, 484 U.S. 518, 529 (1988) ("For reasons too obvious to call for enlarged discussion, the protection of classified information must be committed to the broad discretion of the agency responsible.") (citation, quotation marks, and alteration omitted); *Bismullah v. Gates*, 501 F.3d 178, 187-88 (D.C. Cir. 2007) ("[I]t is within the role of the executive to acquire and exercise the expertise of protecting national security [and] [i]t is not within the role of the courts to second-guess executive judgments made in furtherance of that branch's proper role.").

CONCLUSION

For the foregoing reasons, and the reasons stated in the Presiding Judge's opinion in this case, movants lack Article III standing, and this action should be dismissed for want of jurisdiction.

April 17, 2017

Respectfully submitted,

MARY B. MCCORD
Acting Assistant Attorney General
for National Security

STUART EVANS
Deputy Assistant Attorney General
National Security Division

/s/ Jeffrey M. Smith
JEFFREY M. SMITH
U.S. Department of Justice
National Security Division
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Phone: (202) 514-5600
Fax: (202) 514-8053

Attorneys for the United States of America

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the foregoing was served by the Government via first class mail on this 17th day of April 2017, addressed to:

Patrick Toomey
ACLU Foundation
125 Broad St., 18th Floor
New York, NY 10004

Arthur B. Spitzer
ACLU Foundation of D.C.
4301 Connecticut Ave., N.W.
Suite 434
Washington, DC 20008

David A. Schulz
Media Freedom & Information Access Clinic
Yale Law School
P.O. Box 208215
New Haven, CT 06520

Counsel for Movants

/s/ Jeffrey M. Smith

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

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT
2017 MAY -1 PM 2:28
LEEANN FLYNN HALL
CLERK OF COURT

IN RE OPINIONS & ORDERS OF THIS COURT)
ADDRESSING BULK COLLECTION OF DATA) Docket No. Misc. 13-08
UNDER THE FOREIGN INTELLIGENCE)
SURVEILLANCE ACT)
_____)

**THE UNITED STATES' RESPONSE TO
MOVANT'S EN BANC OPENING BRIEF**

The question before the en banc Court is “whether Movants established Article III standing notwithstanding that a First Amendment right of access does not apply to the judicial opinions they seek.” Order 1 (Mar. 22, 2017). The answer is straightforward: movants have not established Article III standing because they cannot identify a *legally protected* interest given that the right they claim does not apply. Movants seek to resist this obvious conclusion by suggesting that their underlying argument – that there is a First Amendment right of public access to Foreign Intelligence Surveillance Court (FISC) proceedings and records, including the classified material at issue in this case – is open for debate. But as the question before the en banc Court makes clear, movants’ First Amendment argument, which was never colorable, is foreclosed. As such, they have no legally protected interest and thus no standing.

I. Movants Lack an Injury to a Legally Protected Interest

As movants concede, *see* Movants’ Br. 10, the Supreme Court has held that there is no federal jurisdiction over a claim that is “insubstantial, implausible, foreclosed by prior decisions of this Court, or otherwise completely devoid of merit.” *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 89 (1998) (quotation marks omitted). Thus, to have standing, movants must establish “an injury to an interest that the law protects when it is wrongfully invaded.” *Bond v. Utreras*, 585 F.3d 1061, 1073 (7th Cir. 2009) (emphasis omitted). Movants have not established

such a legally protected interest. Rather, the interest they posit – a supposed First Amendment right of access to proceedings, records, and rulings of this Court – is implausible in light of binding Supreme Court caselaw and is foreclosed by prior opinions of this Court. Indeed, that claim’s lack of merit is part of the premise pursuant to which this Court accepted en banc review.

Movants rely on *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1 (1986), but that opinion provides for a First Amendment right of access to judicial proceedings only where both (1) “the place and process have historically been open to the press and general public” (the “experience” test), and (2) “public access plays a significant positive role in the functioning of the particular process in question” (the “logic” test). *Id.* at 8. Any claim that there is a tradition of public access to “proceedings that relate to applications made by the Executive Branch for the issuance of court orders approving authorities covered exclusively by” the Foreign Intelligence Surveillance Act (“FISA”), *In re Opinions & Orders of this Court Addressing Bulk Collection of Data under the Foreign Intelligence Surveillance Act*, 2017 WL 427591, at *19 (FISA Ct. Jan. 25, 2017), is both baseless and foreclosed. And any argument that it would be logical to open up to the public classified proceedings or documents concerning foreign intelligence gathering is insubstantial, given the prospect of harms to national security that “are real and significant, and, quite frankly, beyond debate.” *In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 494 (FISA Ct. 2007).

The insubstantiality of movants’ First Amendment argument has been explained by this Court multiple times. The Court first rejected this argument a decade ago when one of the movants here, the American Civil Liberties Union (ACLU), asserted it in an effort to obtain public access to FISC proceedings and rulings, including rulings that “include legal analysis and legal rulings concerning the meaning of FISA.” *Id.* at 493 (quoting brief of ACLU). This Court

explained that “the ACLU’s First Amendment claim runs counter to a long-established and virtually unbroken practice of excluding the public from FISA applications and orders.” *Id.* The Court further explained that the public access sought by the ACLU failed the “logic” test because it could assist adversaries in avoiding surveillance, seriously harm those targeted for surveillance, chill cooperation with investigators, damage relations with foreign governments, “chill the government’s interactions with the Court,” and threaten “the free flow of information to the FISC that is needed for an ex parte proceeding to result in sound decisionmaking and effective oversight.” *Id.* at 494-96; accord *In re Motion for Release of Court Records*, Misc. 07-01, at 6-7 (FISA Ct. Feb. 8, 2008); *In re Proceedings Required by § 702 of the FISA Amendments Act of 2008*, 2008 WL 9487946, at *3-4 (FISA Ct. Aug. 27, 2008).

Even before the Presiding Judge’s opinion in this case, it was clear and established that the purported First Amendment right of access to FISC proceedings and records did not exist. In that opinion, the Presiding Judge explained that movant’s attempt to resist the Court’s earlier holdings was “premised on a misreading of the Court’s analysis and an overly broad framing of the legal question.” *In re Opinions & Orders*, 2017 WL 427591, at *19. The Presiding Judge further explained that the correct framing of the “experience” test was whether “proceedings that relate to applications made by the Executive Branch for the issuance of court orders approving authorities covered exclusively by FISA” have “historically been open to the press and general public.” *Id.* They have not; indeed, the record “reflect[s] a tradition of no public access.” *Id.* Regarding the “logic” test the Presiding Judge noted that movants have failed “to explain why they believe [the Court’s earlier] conclusion was flawed” and failed to “refute the Court’s identification of the detrimental effects that could cause a diminished flow of information as a

result of public access,” instead offering only “a generalized assertion that they disagree.” *Id.* at *20 (citing *Motion for Release*, 526 F. Supp. 2d at 494-96).

Movants’ underlying First Amendment argument was insubstantial from its inception, and it is now foreclosed. The question before the *en banc* Court is whether, given that it is established that there is no First Amendment right of access to FISC proceedings, records, and rulings, movants have nevertheless established “an invasion of a *legally protected* interest.” *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)) (emphasis added). They have not because the interest they assert – public access to FISC proceedings and records – is not *legally protected*. See *In re Opinions & Orders*, 2017 WL 427591, at *16-21.

Movants cite to the D.C. Circuit’s recent decision in *Dhiab v. Trump*, ___ F.3d ___, 2017 WL 1192911 (D.C. Cir. Mar. 31, 2017). That case further undermines movants’ First Amendment argument. See *id.* at *5 (Op. of Randolph, S.J.) (observing that “from the beginning of the republic to the present day, there is no tradition of publicizing secret national security information involved in civil cases, or for that matter, in criminal cases,” as the “tradition is exactly the opposite”). Movants point out that in *Dhiab*, the request for classified material was rejected on the merits, not for lack of standing. Movant’s Br. 8. True, but that is because the claim in *Dhiab* was not clearly foreclosed by *Press-Enterprise* and other precedent, as the claim here is. Cf. *Bond*, 585 F.3d at 1073 (explaining that “the Supreme Court’s standing doctrine requires litigants to establish an injury to an interest that the law protects when it is *wrongfully* invaded, and this is quite different from requiring them to establish a *meritorious* legal claim”) (quotation marks omitted).

In light of *Press-Enterprise* and this Court's line of cases described above, Movants' asserted First Amendment right of access to FISC proceedings, records, and rulings "has no foundation in law." *Claybrook v. Slater*, 111 F.3d 904, 907 (D.C. Cir. 1997). As such, movants have "no legally protected interest and thus no standing to sue." *Id.*

Movants' appeal to what they call "compelling legal and practical reasons" to reject their claim on the merits rather than on jurisdictional grounds, *see* Movants' Br. 13, fares no better. The canon of constitutional avoidance has no application here. Both the question of Article III jurisdiction and the scope of the First Amendment are constitutional questions, and both must be addressed. As the government explained in its opening brief, there are no nonconstitutional bases for relief here. *See* Gov't Br. 9-11. Nor is the "burden of proof" a relevant consideration. The question whether movants' First Amendment claim is insubstantial or foreclosed is a purely legal one on which neither party bears a burden to prove disputed facts.

II. Movants' Misunderstand the Constitutional Power To Classify and To Protect Sensitive National Security Information

Movants' contention that Executive Branch classification should have no "significance" to the judiciary, Movant's Br. 18, is dangerously misguided. The Executive Branch has an inherent constitutional power "to classify and control access to information bearing on national security." *Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988). And "[f]or 'reasons too obvious to call for enlarged discussion, the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it.'" *Id.* at 529 (quoting *CIA v. Sims*, 471 U.S. 159, 170 (1985)) (alteration omitted). Preventing access to properly classified information is a "compelling interest." *Id.* at 527 (quotation marks omitted). This executive branch constitutional prerogative is routinely and uniformly respected by the judiciary, and rightly so. *See, e.g., NCRI v. Dep't of*

State, 251 F.3d 192, 209-10 (D.C. Cir. 2001) (determinations about access to classified information are “within the privilege and prerogative of the executive, and we do not intend to compel a breach in the security which that branch is charged to protect”). Apart from the deferential standard applied in cases such as those brought pursuant to the Freedom of Information Act (“FOIA”), courts have long recognized that classification decisions are committed to the executive branch. *See, e.g., Egan*, 484 U.S. at 529; *Bismullah v. Gates*, 501 F.3d 178, 187-88 (D.C. Cir. 2007); *McGehee v. Casey*, 718 F.2d 1137, 1147-50 & n.22 (D.C. Cir. 1983) (holding that the court’s role was limited to “merely . . . determin[ing] that the CIA properly classified the deleted items,” as the court “cannot second-guess” the executive branch’s national security judgments).

The cases relied on by movants are not to the contrary. In *In re Washington Post Co.*, the court imposed procedural requirements for closing a sentencing hearing and sealing documents in a criminal case after determining that those procedures would *not* “create an unacceptable risk” of the “inappropriate disclosure of classified information,” an important consideration given that such “disclosure of classified information could endanger the lives of both Americans and their foreign informants.” 807 F.2d 383, 391 (4th Cir. 1986). In *United States v. Rosen*, the court recognized that, “[o]f course, classification decisions are for the Executive Branch,” but held that the presence of classified information in a case would not justify “effectively clos[ing] portions” of a jury trial. 487 F. Supp. 2d 703, 717, 720 (E.D. Va. 2007). In neither case did the court overrule any classification decision or order the release of any classified information, and both courts observed that classified court records and rulings could be sealed from the public. *See Washington Post*, 807 F.2d at 391; *Rosen*, 487 F. Supp. 2d at 706, 720.

CONCLUSION

For the reasons stated above, those stated in the government's April 17, 2017 submission, and those explained in the Presiding Judge's opinion in this case, movants lack Article III standing, and this action should be dismissed for want of jurisdiction.

May 1, 2017

Respectfully submitted,

DANA J. BOENTE
Acting Assistant Attorney General
for National Security

STUART EVANS
Deputy Assistant Attorney General
National Security Division

/s/ Jeffrey M. Smith
JEFFREY M. SMITH
U.S. Department of Justice
National Security Division
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Phone: (202) 514-5600
Fax: (202) 514-8053

Attorneys for the United States of America

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2013 DEC -6 PM 4: 50 UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT
LEE ANN FLYNN HALL
CLERK OF COURT

WASHINGTON, D.C.

Filed with Classified
Information Security Officer

CISO

Date

12/6/13

IN RE OPINIONS AND ORDERS OF THIS
COURT ADDRESSING BULK COLLECTION OF
DATA UNDER THE FOREIGN INTELLIGENCE
SURVEILLANCE ACT

Docket No.: Misc. 13-08

**THE UNITED STATES' OPPOSITION TO THE
MOTION OF THE AMERICAN CIVIL LIBERTIES
UNION, ET AL., FOR THE RELEASE OF COURT RECORDS**

JOHN P. CARLIN
Acting Assistant Attorney General
for National Security

J. BRADFORD WIEGMANN
Deputy Assistant Attorney General

TASHINA GAUHAR
Deputy Assistant Attorney General

NICHOLAS J. PATTERSON
U.S. Department of Justice
National Security Division
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Phone: (202) 514-5600
Fax: (202) 514-8053

Attorneys for the United States of America

The American Civil Liberties Union and two other entities (hereinafter, “ACLU”) seek the publication of opinions of this Court addressing “the legal basis for the ‘bulk collection’ of data by the United States government under the Foreign Intelligence Surveillance Act (‘FISA’), 50 U.S.C. § 1861 *et seq.*, including but not limited to 50 U.S.C. § 1842.” Mot. at 1. The ACLU’s motion should be dismissed because the relevant opinions have been subjected to classification review and the unclassified portions released, and there is no basis for the Court to order a new classification review.

ARGUMENT

I. The ACLU’s Motion Should Be Dismissed Because Declassified Versions of the Requested Opinions Have Already Been Released.

The ACLU’s motion should be dismissed because this Court and the Government have already released declassified versions of the opinions that the Government has determined are responsive to the ACLU’s motion after the Government conducted a classification review with the objective to release as much information in the opinions as possible consistent with national security. A new classification review would duplicate the result of the thorough review the Government already conducted.

After a review of this Court’s opinions, the Government has identified four responsive opinions that address the legal basis for the “bulk collection” of data by the United States Government under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, including but not limited to 50 U.S.C. § 1842. After a classification review conducted by the Executive Branch consistent with Executive Order 13,526 (Dec. 29, 2009), two of the opinions were released by the Executive Branch and two others were published by this Court. They are:

- (1) the Court's Opinion (J. Kollar-Kotelly) granting the Government's application seeking the collection of bulk electronic communications metadata pursuant to Section 402 of the Foreign Intelligence Surveillance Act, the Pen Register and Trap and Trace provision. (Released by the Executive Branch on November 18, 2013), *available at* <http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf>.
- (2) the Court's Opinion (J. Bates) granting the Government's application seeking to reinstate the National Security Agency's bulk electronic communications metadata program following the Government's suspension of the program for several months to address compliance issues identified by the Government and brought to the Court's attention. (Released by the Executive Branch on November 18, 2013), *available at* <http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf>.
- (3) the Court's Opinion (J. McLaughlin) reauthorizing the collection of bulk telephony metadata under the "business records" provision of the Foreign Intelligence Surveillance Act and re-affirming that the bulk telephony metadata collection is both lawful and constitutional. (Published by this Court on October 18, 2013), *available at* <http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf>.
- (4) the Court's Opinion (J. Eagan) reauthorizing the collection of bulk telephony metadata under Section 215 of the USA PATRIOT Act and affirming that the bulk telephony metadata collection is both lawful and constitutional. (Published by this Court on September 17, 2013), *available at* <http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf>.

Because the Government has already conducted a thorough classification review of these opinions, there is no basis to require the Government to review them again.

II. The Court Should Not Order the Government to Conduct New Classification Reviews of the Opinions.

A. The ACLU does not have standing to seek declassification.

Although this Court has inherent authority to require a classification review of its own opinions as a matter of discretion, and can order such a review *sua sponte*, that authority should be exercised in a manner that is consistent with FISA and this Court's rules. FISA does not provide third parties with the right to seek disclosure of classified FISC records. *In re Mot. for*

Release of Ct. Records, 526 F. Supp. 2d 484, 491 (Foreign Intel. Surv. Ct. 2007). Under United States Foreign Intelligence Surveillance Court (“FISC”) Rule of Procedure 62(a) (“FISC Rule”), only a “party” may move the Court for publication of an opinion.¹ This Court recently concluded that “the term ‘party’ in Rule 62(a) refers to a party to the proceeding that resulted in the ‘opinion, order, or other decision’ being considered for publication.” *In re Orders of this Ct. Interpreting Section 215 of the Patriot Act*, Docket No. Misc. 13-02, Opinion and Order, at 11 (Foreign Intel. Surv. Ct. Sept. 13, 2013), *available at* <http://www.uscourts.gov/uscourts/courts/fisc/misc-13-02-order-130813.pdf>. The ACLU is not a party to any of the proceedings that generated the relevant opinions and, therefore, does not have standing to move for publication of the opinions.

FISC Rule 62(a)’s limitation on who can move for publication of an order, opinion, or other decision is in accord with the fact that a comprehensive statutory regime—the Freedom of Information Act (“FOIA”)—governs requests for documents classified by and in the possession of the Executive Branch. *See In re Release*, 526 F. Supp. 2d at 491 n.18, 496 n.32. As this Court has recognized, although this Court has supervisory power over its own records and could

¹ **Rule 62. Release of Court Records**

(a) Publication of Opinions. The judge who authored an order, opinion, or other decision may *sua sponte* or on motion by a party request that it be published. Upon such request, the Presiding Judge, after consulting with other Judges of the Court, may direct that an order, opinion or other decision be published. Before publication, the Court may, as appropriate, direct the Executive Branch to review the order, opinion, or other decision and redact it as necessary to ensure that properly classified information is appropriately protected pursuant to Executive Order 13526 (or its successor).

FISC Rule of Procedure 62(a).

conduct a review “under the same standards as a district court would in FOIA litigation,” “there would be no point in this Court’s merely duplicating the judicial review that the ACLU, and anyone else, can obtain by submitting a FOIA request to the Department of Justice for these same records.” *Id.* at 496 n.32.

The Court should insist that the ACLU respect, and not through its motion attempt to circumvent, the FOIA process enacted by Congress. Accordingly, the Government submits that the Court should not exercise its inherent discretion to determine whether to order a declassification review in this case. FOIA carefully prescribes a process whereby parties must first seek administrative review of FOIA requests before bringing litigation, and FOIA includes additional exemptions beyond the classification exemptions that would overlap with a declassification review ordered by the FISC. Such duplicative processes therefore raise administrative concerns, and the FISC should resist invitations to serve as an alternative forum for FISC-related matters that can and should be resolved through the FOIA process established by Congress.

B. This Court traditionally does not involve itself with the Executive Branch's classification decisions.

The ACLU seeks an order giving it full access to the opinions or, in the alternative, requiring the Government to justify any redactions to the Court as necessary to prevent a substantial probability of harm to a compelling interest. The ACLU also seeks the right to contest redactions. The ACLU invokes the First Amendment, but the First Amendment does not justify judicial (or ACLU) involvement in Executive Branch classification decisions.

Putting aside the fact that this Court has repeatedly rejected arguments that litigants such as the ACLU have a First Amendment right to access classified FISA court records,² the Court does not interfere with the Government's classification process and classification decisions. Under FISC Rule 62(a), the Court is empowered only to "direct the Executive Branch to review the [opinion] and redact it as necessary to ensure that properly classified information is appropriately protected." This limitation on the Court's discretion is consistent with the requirement that, "[i]n all matters, the Court and its staff shall comply with the security measures established pursuant to [Congressional mandate], as well as Executive Order 13526." FISC Rule 3; *see also* FISC Rule 62(b) (mandating that a release of FISC records must be conducted "in conformance with the security measures referenced in Rule 3"). Executive Order 13,526 "prescribes a uniform system for classifying, safeguarding, and declassifying national security information," and under that system only certain designated Executive Branch officials can classify or declassify national security information. *See* Executive Order 13,526.

Consistent with the Court's Rules of Procedure, the Court's decisions also make clear that the Court does not involve itself with the Executive Branch's declassification decisions. Indeed, "if the FISC were to assume the role of independently making declassification and

² *See In re Mot. for Release of Ct. Records*, 526 F. Supp. 2d 484 (Foreign Intel. Surv. Ct. 2007); *In re Mot. for Release of Ct. Records*, Memorandum Opinion, Docket No. Misc. 07-01 (Foreign Intel. Surv. Ct. Feb. 8, 2008), available at <http://www.uscourts.gov/uscourts/courts/fisc/misc-13-02-us-opposition-130705.pdf> (Appendix A to *In re Orders Issued by This Ct. Interpreting Section 215 of the PATRIOT Act*, Docket No. Misc. 13-02, The United States' Opposition to the Motion of the American Civil Liberties Union, *et al.*, for the Release of Court Records (Foreign Intel. Surv. Ct. July 5, 2013)). In this Court's most recent Opinion and Order involving the ACLU, the Court chose not to "reach[] the merits of the [ACLU's] asserted right of public access under the First Amendment." *See In re Orders of this Ct. Interpreting Section 215 of the PATRIOT Act*, Docket No. Misc. 13-02, Opinion and Order, at 17 (Foreign Intel. Surv. Ct. Sept. 13, 2013).

release decisions . . . there would be a real risk of harm to national security interests and ultimately to the FISA process itself.” *In re Release*, 526 F. Supp. 2d at 491. “FISC judges do not make classification decisions and are not intended to become national security experts.” *Id.* at 495 n.31 (citing H.R. Rep. No. 95-1283, pt. 1, at 25-26 (1978)). And, while FISC judges may have “more expertise in national security matters than a typical district court judge, that expertise [does] not equal that of the Executive Branch, which is constitutionally entrusted with protecting the national security.” *Id.* Thus, this Court has recognized that “there is no role for this Court independently to review, and potentially override, Executive Branch classification decisions.” *Id.* at 491.³ This Court recently reiterated that “[i]t is fundamentally the Executive Branch’s responsibility to safeguard sensitive national security information.” *In re Mot. for Consent to Disclosure of Ct. Records*, Docket No. Misc. 13-01, Opinion and Order, at 6 (Foreign Intel. Surv. Ct. June 12, 2013) (citing *Department of Navy v. Egan*, 484 U.S. 518, 527-29 (1988)), available at www.uscourts.gov/uscourts/courts/fisc/misc-13-01-opinion-order.pdf. Thus, this Court should deny the ACLU’s First Amendment classification review request and the ACLU’s request to contest any redactions.

For these reasons, the Court should deny the ACLU’s request for new classification reviews of the relevant opinions. There is no need for this Court to order new classification reviews of the relevant opinions because the Government recently conducted thorough classification reviews of these opinions and made “public as much information as possible about certain sensitive intelligence collection programs undertaken under the authority of the Foreign Intelligence Surveillance Act (FISA) while being mindful of the need to protect national

³ This is not to say that Executive Branch classifications are never judicially reviewable. The proper means to obtain such review is through a FOIA request and subsequent action in district court. See *In re Release*, 526 F. Supp. 2d at 491 n.18, 496 n.32.

security.”⁴ Release of these documents reflected the Executive Branch’s continued commitment to making information about intelligence collection publicly available when appropriate and consistent with the national security of the United States.

CONCLUSION

For the reasons stated above, the ACLU’s Motion should be denied.

December 6, 2013

Respectfully submitted,

JOHN P. CARLIN
Acting Assistant Attorney General
for National Security

J. BRADFORD WIEGMANN
Deputy Assistant Attorney General

TASHINA GAUHAR
Deputy Assistant Attorney General

/s/ Nicholas J. Patterson

NICHOLAS J. PATTERSON
U.S. Department of Justice
National Security Division
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Phone: (202) 514-5600
Fax: (202) 514-8053

Attorneys for the United States of America

⁴ *DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)*, available at <http://icontherecord.tumblr.com/post/60867560465/dni-clapper-declassifies-intelligence-community>. Although this statement was made in reference to the two opinions the Government released, the Government also applied the same standard when conducting the classification review of the two opinions published by this Court.

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the United States' Opposition to the Motion of the American Civil Liberties Union, *et al.*, for the Release of Court Records was served by the Government via Federal Express overnight delivery on this 6th day of December, 2013, addressed to:

Alex Abdo
Brett Max Kaufman
Patrick Toomey
Jameel Jaffer
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
aabdo@aclu.org

Arthur B. Spitzer
American Civil Liberties Union of the
Nation's Capital
4301 Connecticut Avenue, N.W., Suite 434
Washington, DC 20008
artspitzer@aclu-nca.org

David A. Schulz
Media Freedom and Information Access Clinic
Yale Law School
40 Ashmun Street, 4th Floor
New Haven, CT 06511
david.schulz@yale.edu

Gregory L. Diskant
Benjamin S. Litman
Richard I. Kim
Patterson Belknap Webb & Tyler LLP
1133 Avenue of the Americas
New York, NY 10036
blitman@pbwt.com

/s/ Nicholas J. Patterson
Nicholas J. Patterson

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



Docket Number: PR/TT 

MEMORANDUM OPINION

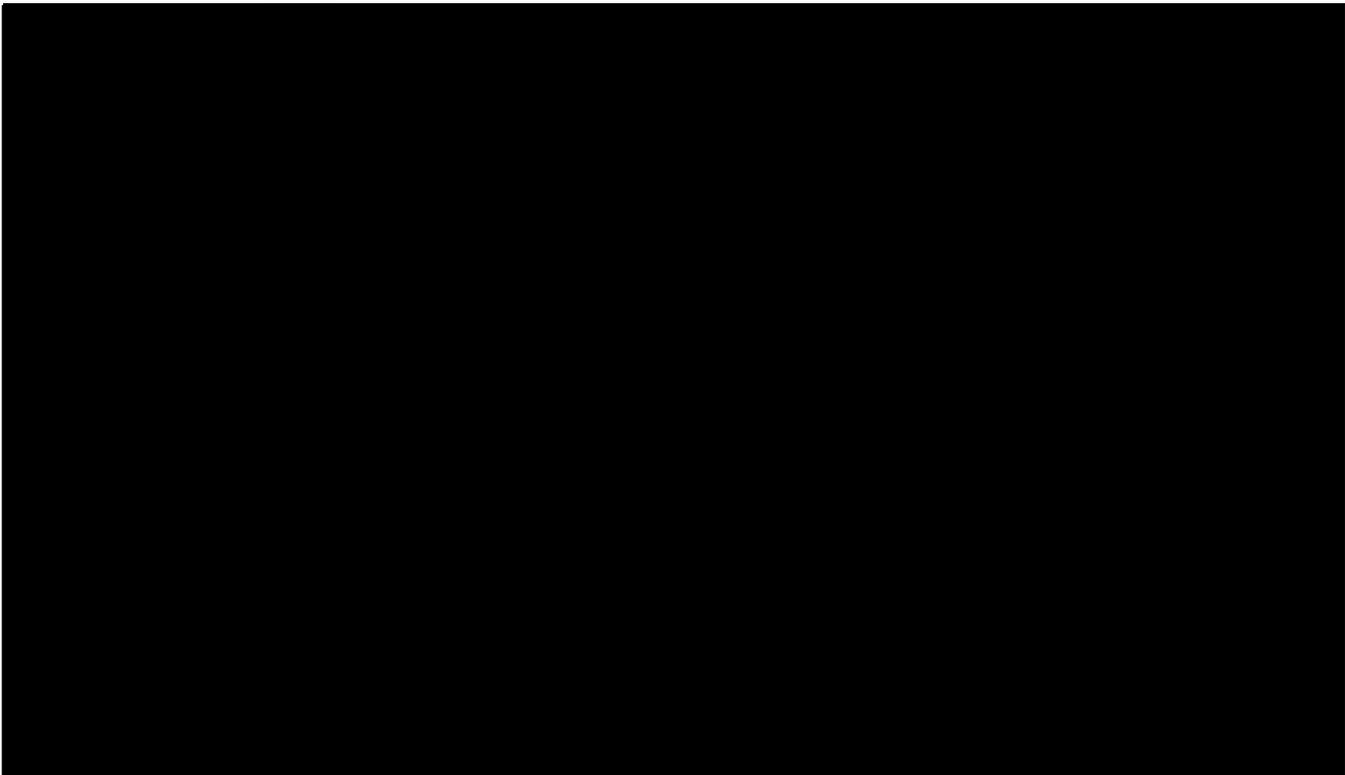
This matter is before the Court upon the government's application to re-initiate in expanded form a pen register/trap and trace (PR/TT) authorization for the National Security Agency (NSA) to engage in bulk acquisition of metadata¹ about Internet communications. The government's application also seeks Court authorization to query and use information previously obtained by NSA, regardless of whether the information was authorized to be acquired under

¹ When used in reference to a communication, "metadata" is information "about the communication, not the actual communication itself," including "numbers dialed, the length of a call, internet protocol addresses, e-mail addresses, and similar information concerning the delivery of the communication rather than the message between two parties." 2 Wayne R. LaFave, Jerold H. Israel, Nancy J. King & Orin S. Kerr, Criminal Procedure § 4.6(b) at 476 (3d ed. 2007).

prior bulk PR/TT orders of the Foreign Intelligence Surveillance Court (FISC or “Court”) or exceeded the scope of previously authorized acquisition. For the reasons explained herein, the government’s application will be granted in part and denied in part.

I. History of Bulk PR/TT Acquisitions Under the Foreign Intelligence Surveillance Act

From [REDACTED], NSA was authorized, under a series of FISC orders under the PR/TT provisions of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1841-1846, to engage in the bulk acquisition of specified categories of metadata about Internet communications. Although the specific terms of authorization under those orders varied over time, there were important constants. Notably, each order limited the authorized acquisition to [REDACTED] categories of metadata.² As detailed herein, the government acknowledges that



NSA exceeded the scope of authorized acquisition continuously during the more than [REDACTED] years of acquisition under these orders.

In addition, each order authorized NSA analysts to access the acquired metadata only through queries based on validated “seed” accounts, *i.e.*, Internet accounts for which there was a reasonable articulable suspicion (“RAS”) that they were associated with a targeted international terrorist group; for accounts used by U.S. persons, RAS could not be based solely on activities protected by the First Amendment.³ The results of such queries provided analysts with information about the [REDACTED] of contacts and usage for a seed account, as reflected in the collected metadata, which in turn could help analysts identify previously unknown accounts or persons affiliated with a targeted terrorist group. *See* [REDACTED] Opinion at 41-45. Finally, each bulk PR/TT order included a requirement that NSA could disseminate U.S. person information to other agencies only upon a determination by a designated NSA official that it is related to counterterrorism information and is necessary to understand the counterterrorism information or to assess its importance.⁴

²(continued)



The current application relies on this prior framework, but also seeks to expand authorization in ways that test the limits of what the applicable FISA provisions will bear. It also raises issues that are closely related to serious compliance problems that have characterized the government's implementation of prior FISC orders. It is therefore helpful at the outset to summarize both the underlying rationale of the prior authorizations and the government's frequent failures to comply with their terms.

A. Initial Approval

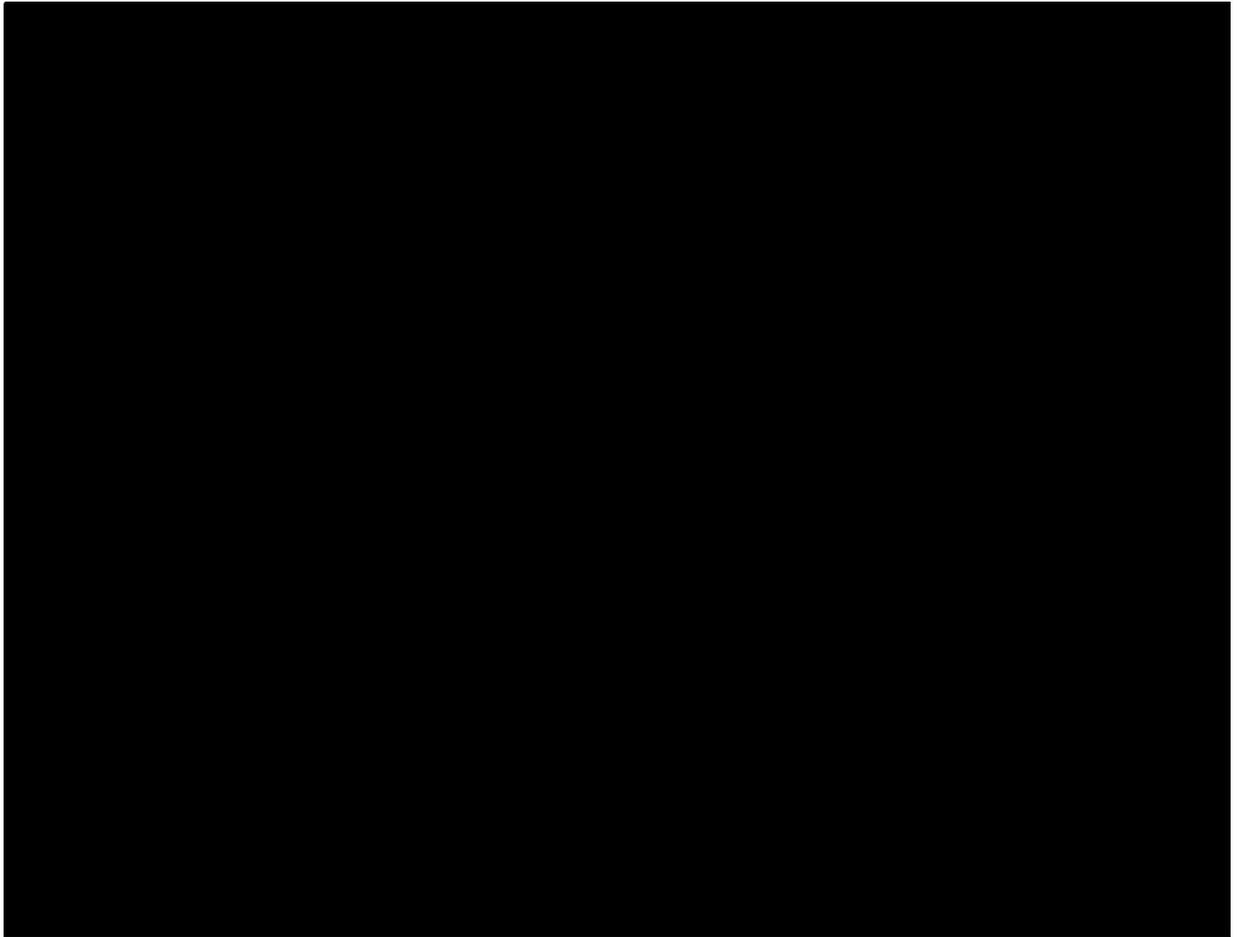
The first application for a bulk PR/TT authorization was granted by the Honorable Colleen Kollar-Kotelly in [REDACTED] Judge Kollar-Kotelly authorized PR/TT surveillance [REDACTED]

[REDACTED]
See [REDACTED] Opinion at 72-80.⁵ When known, the particular customers [REDACTED] [REDACTED] were identified in the Court's order pursuant to 50 U.S.C. § 1842(d)(2)(A)(ii). See [REDACTED] [REDACTED] Opinion at 22-23.

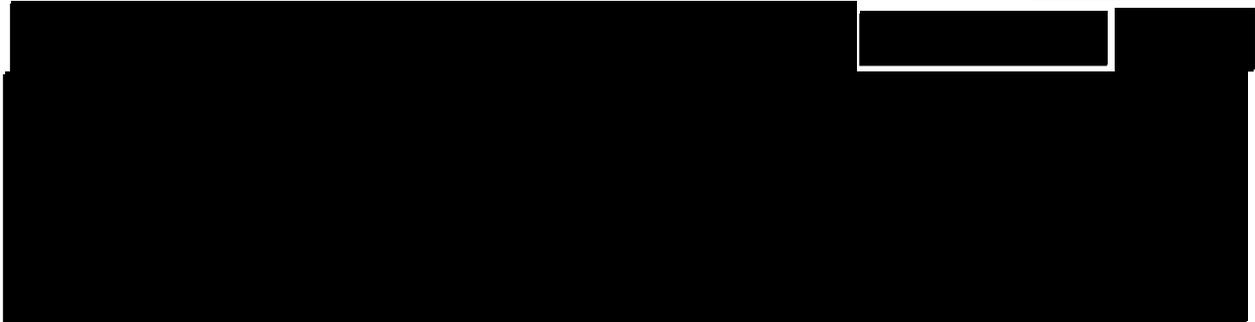
The [REDACTED] Opinion authorized the acquisition of [REDACTED] categories of metadata:

[REDACTED]

[REDACTED]

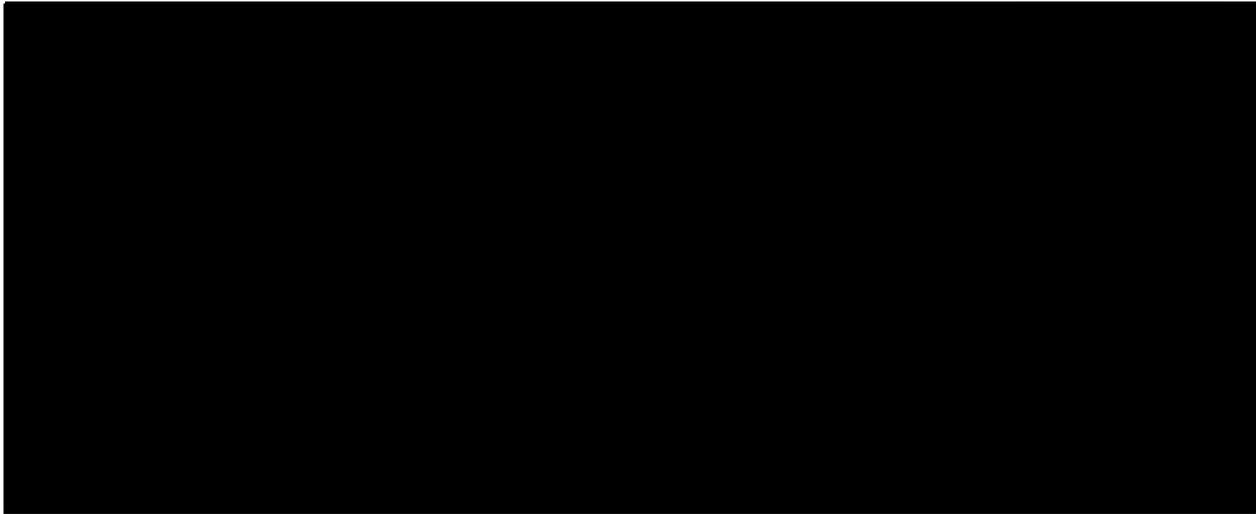


The government proposed to collect these categories of metadata from 





Judge Kollar-Kotelly found that the proposed collection of information within Categories [REDACTED] comported with the applicable statutory definitions of “pen register” and “trap and trace device,”⁷ *id.* at 13-17, and with the Fourth Amendment, *id.* at 58-61. [REDACTED]



The [REDACTED] Opinion stated the Court’s understanding that the application sought authority to obtain only [REDACTED] categories of information and specified that it authorized “only the collection of information in Categories [REDACTED]” *Id.* at 11 (emphasis in original). Each subsequent bulk PR/TT order adopted as its rationale the analysis and conclusions set out in the [REDACTED] Opinion.⁸

⁷ See 18 U.S.C. § 3127(3), (4). These definitions are more fully discussed at pages 25-26, *infra*.

⁸ See *e.g.*, Docket No. PR/TT [REDACTED] Primary Order issued on [REDACTED] at 5; Docket (continued...)

It was anticipated that the authorized PR/TT surveillance would “encompass [REDACTED]

[REDACTED]

[REDACTED]

Opinion at 39-40 (internal quotations omitted).

Pursuant to 50 U.S.C. § 1842(c)(2), the initial application included a certification that the information likely to be obtained was relevant to an ongoing investigation to protect against international terrorism, which was not being conducted solely upon the basis of activities protected by the First Amendment. Docket No. PR/TT [REDACTED] Application filed [REDACTED]

[REDACTED]

⁹ Bulk PR/TT surveillance was first approved in support of investigations of [REDACTED] and the collected metadata could only be accessed through queries based on seed accounts for which there was RAS that the account was associated with [REDACTED] July [REDACTED] Opinion at 72, 83. The range of terrorist organizations for which a RAS determination could support querying the metadata was [REDACTED]

[REDACTED]

The present description of these Foreign Powers is contained in the Declaration of Michael E. Leiter, Director of the National Counterterrorism Center (NCTC), filed in docket number [REDACTED] which is incorporated by reference in the current application. See Docket No. PR/TT [REDACTED] Application filed [REDACTED] at 2.

(██████████ Application”), at 26.¹⁰ Judge Kollar-Kotelly found that the sweeping and non-targeted scope of the proposed acquisition was consistent with this certification of relevance.

██████████ Opinion at 49. In making this finding, the Court relied on several factors, including NSA’s efforts “to build a meta data archive that will be, in relative terms, richly populated with ██████████ communications,” at least as compared with the entire universe of Internet communications, ██████████ Opinion at 47,¹¹ and the presence of “safeguards” proposed by the government “to ensure that the information collected will not be used for unrelated purposes,” *id.* at 27, thereby protecting “the continued validity of the certification of relevance,” *id.* at 70. These safeguards importantly included both the limitation that NSA

¹⁰ The government argued that “FISA prohibits the Court from engaging in any substantive review of this certification,” and that “the Court’s exclusive function” was “to verify that it contains the words required” by the statute. ██████████ Opinion at 26. The Court did not find such arguments persuasive. *Id.* However, because the government had in fact provided a detailed explanation of the basis for the certification, the Court did not “decide whether it would be obliged to accept the applicant’s certification without any explanation of its basis” and instead “assume[d] for purposes of this case that it may and should consider the basis” of the certification of relevance. *Id.* at 27-28.

analysts could access the bulk metadata only on the basis of RAS-approved queries, *id.* at 42-43, 56-58, and the rule governing dissemination of U.S. person information outside of NSA, *id.* at 85.

However, the finding of relevance most crucially depended on the conclusion that “the proposed bulk collection . . . is necessary for NSA to employ . . . analytic tools [that] are likely to generate useful investigative leads for ongoing efforts by the [Federal Bureau of Investigation (FBI)] (and other agencies) to identify and track [REDACTED]” *Id.* at 48.

Consequently, “the collection of both a huge volume and high percentage of unrelated communications . . . is necessary to identify the much smaller number of [REDACTED]

[REDACTED] such that the entire mass of collected metadata is relevant to investigating [REDACTED]

[REDACTED] affiliated persons. *Id.* at 48-49; *see also id.* at 53-54 (relying on government’s

explanation why bulk collection is “necessary to identify and monitor [REDACTED] operatives

whose Internet communications would otherwise go undetected in the huge streams of [REDACTED]

communications”).

B. First Disclosure of Overcollection

During the initial period of authorization, the government disclosed that NSA’s acquisitions had exceeded the scope of what the government had requested and the FISC had approved. Insofar as it is instructive regarding the separate form of overcollection that has led directly to the current application, this prior episode is summarized here.

On [REDACTED] the government provided written notice to the FISC that it had exceeded the scope of authorized collection [REDACTED] Docket No. PR/TT [REDACTED] Notice of Compliance Incidents, filed on [REDACTED]. On the same day, Judge Kollar-Kotelly ordered the government to provide additional information about this non-compliance, including a “full description of the scope, nature, and circumstances of any unauthorized collection” [REDACTED] [REDACTED] Docket No. PR/TT [REDACTED] Order Regarding Disclosed Violations Involving [REDACTED] [REDACTED] issued on [REDACTED] Order”), at 6. The government made an interim response to the [REDACTED] Order in the form of a Declaration of [REDACTED] [REDACTED] filed in Docket No. PR/TT [REDACTED] on [REDACTED] (“[REDACTED] Decl.”), and a fuller response in the form of a Declaration of [REDACTED] [REDACTED] filed in Docket No. PR/TT [REDACTED] on [REDACTED] (“[REDACTED] Decl.”).

As described by the government, the unauthorized collection resulted from failures to [REDACTED] in the manner required. [REDACTED] Decl. at 8-11.¹² By the government’s account, the lack of required [REDACTED] did not result from technical difficulty or malfunction, but rather from a failure of “those NSA officials who understood in detail the requirements of the [REDACTED] Opinion] . . . to communicate those requirements effectively

[REDACTED]

to the [REDACTED] . . . who were directly responsible” for implementation. Id. at 5. The government assessed the violations to have been caused by “poor management, lack of involvement by compliance officials, and lack of internal verification procedures – not by bad faith.” Id. at 7.

The Court had specifically directed the government to explain whether this unauthorized collection involved the acquisition of information other than the approved Categories [REDACTED] [REDACTED] Order at 7. In response, the Deputy Secretary of Defense stated that the “Director of NSA has informed me that at no time did NSA collect any category of information . . . other than the [REDACTED] categories of meta data” approved in the [REDACTED] Opinion, but also noted that the NSA’s Inspector General had not completed his assessment of this issue. [REDACTED] [REDACTED] Decl. at 21.¹³ As discussed below, this assurance turned out to be untrue.

Regarding the information obtained through unauthorized collection, the Court ordered the government to describe whether it “has been, or can be, segregated from information that NSA was authorized to collect,” “how the government proposes to dispose of” it, and “how the government proposes to ensure that [it] is not included . . . in applications presented to this Court.” [REDACTED] Order at 7-8. In response, the government stated that, while it was not

¹³ At a hearing on [REDACTED] Judge Kollar-Kotelly referred to this portion of the Deputy Secretary’s declaration and asked: “[C]an we conclude that there wasn’t content here?” [REDACTED] of NSA, replied: “There is not the physical possibility of our having [REDACTED] [REDACTED] Docket Nos. [REDACTED] Transcript of Hearing Conducted [REDACTED] at 16-17.

feasible to segregate authorized collection from unauthorized collection on an item-by-item basis, NSA had eliminated access to the database that contained the entire set of metadata, and repopulated the databases used by analysts to run queries so that they only contained information [REDACTED] that had not been involved in the unauthorized collection. [REDACTED] Decl. at 25-26. The government asserted that, after taking these actions, NSA was “making queries against a database that contain[ed] only meta data that NSA was authorized to collect.” *Id.* at 26. As to information disseminated outside of NSA, the government reported that it had reviewed disseminated NSA reports and concluded that just one report was potentially based on improperly collected information. [REDACTED] Decl. at 9-10. NSA cancelled this report and confirmed that the recipient agencies had purged it from their records. *Id.* at 11.

The initial bulk PR/TT authorization granted by the [REDACTED] Opinion was set to expire on [REDACTED] shortly after the government had disclosed this unauthorized collection. On that date, Judge Kollar-Kotelly granted an application for continued bulk PR/TT acquisition; however, in that application, the government only requested authorization for acquisition [REDACTED] that had not been subject to the [REDACTED] See Docket No. PR/TT [REDACTED] Application filed on [REDACTED] (“[REDACTED] Application”), at 9-15; Primary Order issued on [REDACTED] at 2-5.¹⁴ The government represented that the PR/TT [REDACTED] had “fully complied with the orders of the Court.”

¹⁴ Subsequent applications and orders followed the same approach. See, e.g., Docket No. PR/TT [REDACTED] Application filed on [REDACTED] at 9-13; Primary Order issued on [REDACTED] at 2-5.

Declaration of [REDACTED] at 2-3 (Exhibit C to [REDACTED] Application). The government also described in that application new oversight mechanisms to ensure against future overcollection. [REDACTED] Application at 8-9. These included a requirement that, “at least twice during the 90-day authorized period of surveillance,” NSA’s Office of General Counsel (NSA OGC) “will conduct random spot checks [REDACTED] to ensure that [REDACTED] functioning as authorized by the Court. Such spot checks will require an examination of a sample of data.” *Id.* at 9. The Court adopted this requirement in its orders granting the application, as well as in subsequent orders for bulk PR/TT surveillance.¹⁵

C. Overcollection Disclosed in [REDACTED]

In December [REDACTED] the government reported to the FISC a separate case of unauthorized collection, which it attributed to a typographical error in how a prior application and resulting orders had described communications [REDACTED] See Docket No. PR/TT [REDACTED] Verified Motion for an Amended Order filed on [REDACTED] at 4-6. The government sought a nunc pro tunc correction of the typographical error in the prior orders, which would have effectively approved two months of unauthorized collection. *Id.* at 7. The government represented that, with regard to prior collection [REDACTED] it could not

¹⁵ See [REDACTED]

“accurately segregate” information that fell within the scope of the prior orders from those that did not. Id.

The FISC approved prospective collection [REDACTED] on the terms requested by the government when it granted a renewal application [REDACTED]. See Docket No. PR/TT [REDACTED] Primary Order issued on [REDACTED] at 5-6. However, the FISC withheld nunc pro tunc relief for the previously collected information, and NSA removed from its systems all data collected [REDACTED] under the prior order. See Docket [REDACTED] [REDACTED] at 18.

D. Non-Compliance Disclosed [REDACTED]

The next relevant compliance problems surfaced in [REDACTED] and involved three general subjects: (1) accessing of metadata; (2) disclosure of query results and information derived therefrom; and (3) overcollection. These compliance disclosures generally coincided with revelations about similar problems under a separate line of FISC orders providing for NSA’s bulk acquisition of metadata for telephone communications pursuant to 50 U.S.C. § 1861.¹⁶

1. Accessing Metadata

On January [REDACTED] the government disclosed that NSA had regularly accessed the bulk telephone metadata using a form of automated querying based on telephone numbers that had not been approved under the RAS standard. See Docket No. BR 08-13, Order Regarding

¹⁶ The Section 1861 orders, like the bulk PR/TT orders, permit NSA analysts to access the bulk telephone metadata only through queries based on RAS-approved telephone numbers. See, e.g., Docket No. [REDACTED], at 7-10.

Preliminary Notice of Compliance Incident Dated [REDACTED] issued on [REDACTED] at 2-3. The Honorable Reggie B. Walton of this Court ordered the government to verify that access to the bulk PR/TT metadata complied with comparable restrictions, noting “the similarity between the querying practices and requirements employed” in both contexts. See Docket No. PR/TT [REDACTED] Order issued on [REDACTED] at 1.

In response, the government reported that it had identified, and discontinued, a non-automated querying practice for PR/TT metadata that it had concluded was non-compliant with the required RAS approval process. See Docket No. PR/TT [REDACTED] Government’s Response to the Court’s Order Dated [REDACTED] filed on [REDACTED] at 2-6 ([REDACTED] Response”).¹⁷ The government’s [REDACTED] Response also described additional oversight and

¹⁷ This practice involved an analyst running a query using as a seed “a U.S.-based e-mail account” that had been in direct contact with a properly validated seed account, but had not itself been properly validated under the RAS approval process. [REDACTED] Response at 2-3. When he granted renewed authorization for bulk PR/TT surveillance on [REDACTED], Judge Walton ordered the government not to resume this practice without prior Court approval. See Docket No. PR/TT [REDACTED] Primary Order issued [REDACTED] at 10.

In its response, the government also described an automated means of querying, which it regarded as consistent with the applicable PR/TT orders. This form of querying involved the determination that an e-mail address satisfied the RAS standard, but for the lack of a connection to one of the Foreign Powers (e.g, there were sufficient indicia that the user of the e-mail address was involved in terrorist activities, but the user’s affiliation with a particular group was unknown). See Declaration of Lt. Gen. Keith B. Alexander, Director of NSA, at 8 (attached at Tab 1 to [REDACTED] Response) ([REDACTED] Alexander Decl.”). In the event that such an e-mail address was in contact with a RAS-approved seed account on an NSA “Alert List,” that e-mail address would itself be used as a seed for automatic querying, on the theory that the requisite nexus to one of the Foreign Powers had been established. Id. at 8-9. The government later reported that it had discontinued this practice, see Docket No. PR/TT [REDACTED] NSA 90-Day (continued...)

compliance measures being taken with regard to the bulk PR/TT program, see [REDACTED] Response at 6-7, which Judge Walton adopted as requirements in his order authorizing continued bulk PR/TT surveillance on [REDACTED]. See Docket No. PR/TT [REDACTED] Primary Order issued [REDACTED] at 13-14. Finally, the government's response noted the commencement by NSA of a "complete ongoing end-to-end system engineering and process review (technical and operational) of NSA's handling of PR/TT metadata to ensure that the material is handled in strict compliance with the terms of the PR/TT Orders and the NSA's descriptions to the Court." [REDACTED] Alexander Decl. at 16.¹⁸

¹⁷(...continued)

Report filed [REDACTED] at 8 (Exhibit B to Application), and the Court ordered the government not to resume it without prior Court approval. See Docket No. PR/TT [REDACTED] Primary Order issued [REDACTED] at 10.

¹⁸ On [REDACTED] the government provided written notice of a separate form of unauthorized access relating to the use by NSA technical personnel of bulk PR/TT metadata to identify [REDACTED] which they then employed for "metadata reduction and management activities" in other data repositories. See Docket No. PR/TT [REDACTED] Preliminary Notice of Compliance Incident filed on [REDACTED] at 2-3. The government assessed this practice to be inconsistent with restrictions on accessing and using bulk PR/TT metadata. *Id.* at 3. On [REDACTED] Judge Walton issued a supplemental order which, *inter alia*, directed the government to discontinue such use or show cause why continued use was necessary and appropriate. See Docket No. PR/TT [REDACTED] Supplemental Order issued on [REDACTED] Order"), at 4. In response, the government described the deleterious effects that would likely result from discontinuing the use of [REDACTED] derived from the bulk PR/TT metadata. See Docket No. PR/TT [REDACTED] Declaration of [REDACTED] NSA, filed on [REDACTED] at 1-3, 6 [REDACTED] Decl."). On [REDACTED] Judge Walton approved the continuation of NSA's use of [REDACTED] Docket No. PR/TT [REDACTED] Supplemental Order issued on [REDACTED] at 2-3. In addition, with regard to a then-recent misstatement by the government concerning when NSA had terminated automatic querying of the bulk PR/TT metadata, see [REDACTED] (continued...)

2. Disclosure of Query Results and Information Derived Therefrom

Also in the ██████████ Order, the Court noted recent disclosure of the extent to which NSA analysts who were not authorized to access the PR/TT metadata directly nonetheless received unminimized query results. ██████████ Order at 2. The Court permitted the continuance of this practice for a 20-day period, but provided that such sharing shall not continue thereafter “unless the government has satisfied the Court, by written submission, that [it] is necessary and appropriate.” *Id.* at 4. In response, the government stated that “NSA’s collective expertise in [the targeted] Foreign Powers resides in more than one thousand intelligence analysts,” less than ten percent of whom were authorized to query the PR/TT metadata. ██████████, ██████████ Declaration at 7-8. Therefore, the government posited that sharing “unminimized query results with non-PR/TT-cleared analysts is critical to the success of NSA’s counterterrorism mission.” *Id.* at 8. Judge Walton authorized the continued sharing of such information within NSA, subject to the training requirement discussed at pages 18-19, *infra*. See Docket Nos. PR/TT ██████████ & BR 09-06, Order issued on ██████████ Order”), at 7.

On ██████████ the government submitted a notice of non-compliance regarding dissemination of information outside of NSA that resulted from NSA’s placing of query results into a database accessible by other agencies’ personnel without the determination, required for

¹⁸(...continued)
██████████ Order at 2, the Court ordered NSA not to “resume automated querying of the PR/TT metadata without the prior approval of the Court.” *Id.* at 3.

any U.S. person information, that it related to counterterrorism information and was necessary to understand the counterterrorism information or assess its importance. See Docket No. PR/TT [REDACTED] Preliminary Notice of Compliance Incident filed on [REDACTED] Between [REDACTED] and [REDACTED] approximately 47 analysts from the FBI, the Central Intelligence Agency (CIA), and the National Counterterrorism Center (NCTC) queried this database in the course of their responsibilities and accessed unminimized U.S. person information. See Docket No. PR/TT [REDACTED] Report of the United States filed on [REDACTED] Report”), Exhibit A, Declaration of Lt. Gen. Keith B. Alexander, Director, NSA, at 11-13. NSA terminated access to this database for other agencies’ personnel by [REDACTED] Id. at 12. Based on its end-to-end review, NSA concluded that NSA personnel “failed to make the connection between continued use of the database and the new dissemination procedures required by the Court’s Orders.” Id. at 15.

The government further disclosed that, apart from this shared database, NSA analysts made it a general practice to disseminate to other agencies NSA intelligence reports containing U.S. person information extracted from the PR/TT metadata without obtaining the required determination. See Docket No. PR/TT [REDACTED] Government’s Response to the Court’s Supplemental Order Entered on [REDACTED], filed on [REDACTED] at 2. The large majority of disseminated reports had been written by analysts cleared to directly query the PR/TT metadata. See Docket No. PR/TT [REDACTED] Declaration of [REDACTED] NSA, filed on [REDACTED] [REDACTED], at 2. In response to these disclosures, Judge Walton ordered that, prior to receiving query

results, any NSA analyst must first have received “appropriate and adequate training and guidance regarding all rules and restrictions governing the use, storage, and dissemination of such information.” [REDACTED] Order at 7. He also required the government to submit weekly reports on dissemination, including a certification that the required determination had been made for any dissemination of U.S. person information, and to include “in its submissions regarding the results of the end-to-end review[] a full explanation” of why this dissemination rule had been disregarded. *Id.* at 7-8.

Subsequently, in response to the latter requirement, the government merely stated: “Although NSA now understands the fact that only a limited set of individuals were authorized to approve these releases under the Court’s authorization, it seemed appropriate at the time” to delegate approval authority to others. [REDACTED] Report, Exhibit A, at 17. The government’s explanation speaks only to the identity of the approving official, but a substantive determination regarding the counterterrorism nature of the information and the necessity of including U.S. person information was also required under the Court’s orders. *See* page 3, *supra*. It appears that, for the period preceding the adoption of the weekly reporting requirement, there is no record of the required determination being made by any NSA official for any dissemination. As far as can be ascertained, the requirement was simply ignored. *See* [REDACTED] Report, Exhibit A, at 18-19.

NSA completed its “end-to-end review” of the PR/TT metadata program on [REDACTED], [REDACTED]. *See* [REDACTED] Report, Exhibit B. On [REDACTED], Judge Walton granted an

application for continued bulk PR/TT authorization. In that application, the government represented that “all the technologies used by NSA to implement the authorizations granted by docket number PR/TT [REDACTED] and previous docket numbers only collect, or collected, authorized metadata.” Docket No. PR/TT [REDACTED] Application filed on [REDACTED] [REDACTED] Application”), at 11 n.6 (emphasis in original).

3. Overcollection

Notwithstanding this and many similar prior representations, there in fact had been systemic overcollection since [REDACTED]. On [REDACTED] the government provided written notice of yet another form of substantial non-compliance discovered by NSA OGC on [REDACTED] [REDACTED]¹⁹ this time involving the acquisition of information beyond the [REDACTED] authorized categories. See Docket No. PR/TT [REDACTED] Preliminary Notice of Compliance Incident filed on [REDACTED] at 2. This overcollection, which had occurred continuously since the initial authorization in [REDACTED] [REDACTED] *id.* at 3, included the acquisition of [REDACTED] [REDACTED] *id.* at 2. The government reported that NSA had ceased querying PR/TT metadata and suspended receipt of metadata [REDACTED] [REDACTED] *Id.* The government later advised that this continuous overcollection acquired

¹⁹ Since [REDACTED] NSA OGC had been obligated to conduct periodic checks of the metadata obtained at [REDACTED] to ensure that [REDACTED] were functioning in an authorized manner. See page 13, *supra*.

many other types of data²⁰ and that “[v]irtually every PR/TT record” generated by this program included some data that had not been authorized for collection. [REDACTED] Application, Exhibit D, NSA Response to FISA Court Questions dated [REDACTED] (“[REDACTED] Response”), at 18.

The government has provided no comprehensive explanation of how so substantial an overcollection occurred, only the conclusion that, [REDACTED] [REDACTED] there was a failure to translate the technical requirements” [REDACTED] “into accurate and precise technical descriptions for the Court.” [REDACTED] Report, Exhibit A, at 31. The government has said nothing about how the systemic overcollection was permitted to continue, [REDACTED] [REDACTED] On the record before the Court, the most charitable interpretation possible is that the same factors identified by the government [REDACTED] [REDACTED] remained unabated and in full effect: non-communication with the technical personnel directly responsible [REDACTED] [REDACTED] resulting from poor management. However, given the duration of this problem, the oversight measures ostensibly taken since [REDACTED] to detect overcollection, and the extraordinary

[REDACTED]

fact that NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively. The government has expressed a belief that "the stand-up of NSA's Office of the Director of Compliance in July 2009" will help avoid similar failures in the future, both with respect to explaining to the FISC what NSA actually intends to do and in conforming NSA's actions to the terms of FISC authorizations. Id. at 31-32.

E. Expiration of Bulk PR/TT Authorities

The PR/TT authorization granted in Docket No. PR/TT [REDACTED] was set to expire on [REDACTED]. On [REDACTED] the government submitted a proposed renewal application, which acknowledged [REDACTED] information that may not have been contemplated under prior orders. See Docket No. PR/TT [REDACTED] Supplemental Order issued on [REDACTED] Order"), at 2. The proposed application sought approval [REDACTED] subject to the restrictions that NSA analysts would not query the PR/TT metadata previously received by NSA²¹ and that information prospectively obtained [REDACTED] would be stored [REDACTED] and not [REDACTED] [REDACTED] to access or use. Id. at 2. After Judge Walton expressed concern about the merits of the

²¹ The government requested in its proposed application that, if "immediate access to the metadata repository is necessary in order to protect against an imminent threat to human life," the government would "first notify the Court." [REDACTED] Order at 3. Instead, Judge Walton permitted access to protect against an imminent threat as long as the government provided a report.

proposed application,²² the government elected not to submit a final application. Id. at 3. As a result, the authorization for bulk PR/TT surveillance expired on [REDACTED] judge Walton directed that the government “shall not access the information [previously] obtained . . . for any analytic or investigative purpose” and shall not “transfer to any other NSA facility information . . . currently stored [REDACTED] Id. at 4-5. He also provided that, “[i]n the extraordinary event that the government determines immediate access to the [PR/TT metadata] is necessary in order to protect against an imminent threat to human life, the government may access the information,” and shall thereafter “provide a written report to the Court describing the circumstances and results of the access.” Id. at 5.²³

F. The Current Application

On [REDACTED] the government submitted another proposed application, which in most substantive respects is very similar to the final application now before the Court. Thereafter, on [REDACTED] the undersigned judge met with representatives of the executive branch to explore a number of factual and legal questions presented. The government responded to the Court’s questions in three written submissions,

²² The proposed application did not purport to specify the types of data acquired [REDACTED] or, importantly, to provide a legal justification for such acquisition under a PR/TT order.

²³ In compliance with this requirement, the government has reported that, under this emergency exception, NSA has run queries of the bulk metadata in response to threats stemming from (i) [REDACTED]

[REDACTED] See, e.g., Docket No. PR/TT [REDACTED] Reports filed on [REDACTED] and various reports filed from [REDACTED]

filed on [REDACTED]. The government then submitted its revised, final application on [REDACTED], with those prior written responses attached as Exhibit D.

To enter the PR/TT order requested in the current application, or a modified PR/TT order, the Court must find that the application meets all of the requirements of Section 1842. See 50 U.S.C. § 1842(d)(1). Some of these requirements are plainly met: the government has submitted to a judge of the FISC a written application that has been approved by the Attorney General (who is also the applicant). See [REDACTED] Application at 1, 20; 50 U.S.C. § 1842(a)(1), (b)(1), (c). The application identifies the Federal officer seeking to use the PR/TT devices covered by it as General Keith B. Alexander, the Director of NSA, who has also verified the application pursuant to 28 U.S.C. § 1746 in lieu of an oath or affirmation. See [REDACTED] application at 5, 18; 50 U.S.C. § 1842(b), (c)(1).

In other respects, however, the Court's review of this application is not nearly so straightforward. As a crucial threshold matter, there are substantial questions about whether some aspects of the proposed collection are properly regarded as involving the use of PR/TT devices. There are also noteworthy issues regarding the certification of relevance pursuant to Section 1842(c)(2) and the specifications that the order must include under Section 1842(d)(2)(A), as well as post-acquisition concerns regarding the procedures for handling the metadata. The Court's resolution of these issues is set out below.

In the remainder of this Opinion, the Court will first consider whether the proposed collection involves the use of a PR/TT device within the meaning of the applicable statutory definitions, and whether the data that the government seeks to collect consists of information that may properly be acquired by such a device. Next, the Court will consider whether the application satisfies the statutory relevance standard and contains all the necessary elements. The Court will then address the procedures and restrictions proposed by the government for the retention, use, and dissemination of the information that is collected. Finally, the Court will consider the government's request for permission to use all previously-collected data, including information falling outside the scope of the Court's prior authorizations.

II. The Proposed Collection, as Modified Herein, Involves the Installation and Use of PR/TT Devices

A. The Applicable Statutory Definitions

For purposes of 50 U.S.C. §§ 1841-1846, FISA adopts the definitions of "pen register" and "trap and trace device" set out in 18 U.S.C. § 3127. See 50 U.S.C. § 1841(2). Section 3127 provides 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 . . . ;^[24]

²⁴ The definition excludes any device or process used by communications providers or customers for certain billing-related purposes or "for cost accounting or other like purposes in the ordinary course of business." § 3127(3). These exclusions are not pertinent to this case.

(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 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.^[25]

18 U.S.C. § 2510(12).

(2) “Wire communication” is defined 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.

18 U.S.C. § 2510(1).

²⁵ The other exclusions to this definition at Section 2510(12)(B)-(D) are not relevant to this case.

(3) “Contents” is defined to “include[] any information concerning the substance, purport, or meaning” of a “wire, oral, or electronic communication.” 18 U.S.C. § 2510(8).²⁶

Together, these definitions set bounds on the Court’s authority to issue the requested order because the devices or processes to be employed must meet the definition of “pen register” or “trap and trace device.”

[REDACTED]

As explained by the government, the proposed collection [REDACTED]

[REDACTED]

[REDACTED] Declaration of Gen. Keith B. Alexander,

Director of NSA, at 23-24 (attached as Exhibit A to [REDACTED] Application) ([REDACTED]

Alexander Decl.”). [REDACTED]

[REDACTED]

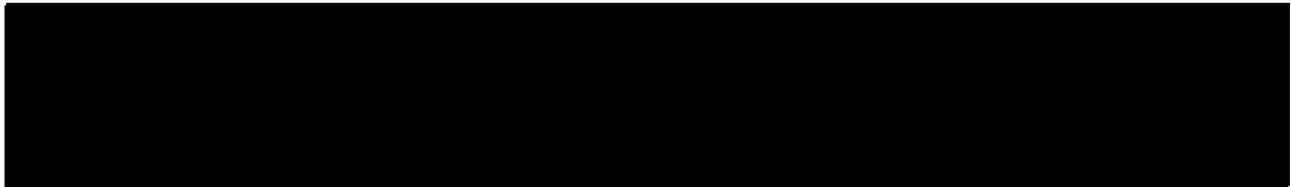
[REDACTED]

²⁶ Different definitions of “wire communication” and “contents” are set forth at 50 U.S.C. § 1801(l) & (n). The definitions in Section 1801, however, apply to terms “[a]s used in this subchapter” – *i.e.*, in 50 U.S.C. §§ 1801-1812 (FISA subchapter on electronic surveillance) – and thus are not applicable to the terms “wire communication” and “contents” as used in the definition of “pen register” and “trap and trace device” applicable to Sections 1841-1846 (FISA subchapter on pen registers and trap and trace devices).



See id., Tab 2, at 1-2 n.2.²⁷

Subject to the following discussion of what types of information may properly be regarded as non-content addressing, routing or signaling information, the Court concludes that this  is consistent with the statutory definitions of “pen register” and, insofar as information about the source of a communication is obtained, “trap and trace device.” Each communication subject to collection is either a wire communication or an electronic



communication under the definitions set forth above.²⁸ The end-result of the collection process²⁹ is that only metadata authorized by the Court for collection is forwarded to NSA for retention and use. [REDACTED]

[REDACTED] Finally, and again subject to the discussion below regarding what types of information may properly be acquired, the Court concludes that the automated processes resulting in the transmission to NSA of information

²⁸ Many of the communications for which information will be acquired will fall within the broad definition of “electronic communication” at 18 U.S.C. § 2510(12). If, however, a covered 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 constitute a “wire communication” under the meaning of Section 2510(1). In either case, the communications subject to collection are “wire or electronic communication[s],” as required in Sections 3127(3) & (4).

²⁹ The term “process,” as used in the definitions of “pen register” and “trap and trace device”, has its “generally understood” meaning of “a series of actions or operations conducing to an end” and “covers software and hardware operations used to collect information.” In re Application of the United States for an Order Authorizing the Installation and Use of a PR/TT Device on E-Mail Account, 416 F. Supp.2d 13, 16 n.5 (D.D.C. 2006) (Hogan, District Judge) (internal quotations and citations omitted).

³⁰ Accord [REDACTED] Opinion at 12-13; In re Application of the United States for an Order Authorizing the Use of Two PR/TT Devices, 2008 WL 5082506 at *1 (E.D.N.Y. Nov. 26, 2008) (Garaufis, District Judge) (recording and transmitting contents permissible under PR/TT order where government computers were configured to immediately delete all contents). But see In re Application of the United States for an Order Authorizing the Use of a PR/TT Device On Wireless Telephone, 2008 WL 5255815 at *3 (E.D.N.Y. Dec. 16, 2008) (Orenstein, Magistrate Judge) (any recording of contents impermissible under PR/TT order, even if deleted before information is provided to investigators).

resulting from [REDACTED] about communications is a form of “record[ing]” or “decod[ing]” permissible under the definition of “pen register.”

C. The Requested Information

The application seeks to expand considerably the types of information authorized for acquisition. Although the government provides new descriptions for the categories of information sought, see [REDACTED] Alexander Decl., Tab 2, they encompass all the types of information that were actually collected (to include unauthorized collection) under color of the prior orders. Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes (“Memorandum of Law”) at 3, submitted as Exhibit B to the [REDACTED] Application.

1. The Proper Understanding of DRAS Information and Contents

The government contends that all of the data requested in this application may properly be collected by a PR/TT device because all of it is dialing, routing, addressing or signaling (“DRAS”) information, and none constitutes contents. Id. at 22. In support of that contention, the government advances several propositions concerning the meaning of “dialing, routing, addressing, or signaling information” and “contents,” as those terms are used in the definitions of “pen register” and “trap and trace device.” While it is not necessary to address all of the government’s assertions, a brief discussion of the government’s proposed statutory construction will be useful in explaining the Court’s decision to approve most, but not all, of the proposed collection.

The government argues that DRAS information and contents are “mutually exclusive categories,” and that Congress intended for DRAS information “to be synonymous with ‘non-content.’” Id. at 23, 51. The Court is not persuaded that the government’s proposed construction can be squared with the statutory text. The definition of pen register covers “a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility . . . , provided, however, that such information shall not include the contents of any communication.” § 3127(3). The structure of the sentence – an affirmative description of the information to be recorded or decoded, followed by a proviso that “such information shall not include the contents of any communication” – does not suggest an intention by Congress to create two mutually exclusive categories of information. Instead, the sentence is more naturally read as conveying two independent requirements – the information to be recorded or decoded must be DRAS information and, whether or not it is DRAS, it must not be contents. The same observations apply to the similarly-structured definition of “trap and trace device.” See 18 U.S.C. § 3127(4) (“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”).

The breadth of the terms used by Congress to identify the categories of information subject to collection and to define “contents” reinforces the conclusion that DRAS and contents are not mutually exclusive categories. As the government observes, see Memorandum of Law at

37, the ordinary meanings of the terms “dialing,” “routing,” addressing,” and “signaling” – which are not defined by the statute – are relatively broad. Moreover, as noted above, the term “contents” is broadly defined to include “any information concerning the substance, purport, or meaning of [an electronic] communication.” 18 U.S.C. § 2510(8) (emphasis added). And “electronic communication,” too, is defined broadly to mean “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” 18 U.S.C. § 2510(12) (emphasis added).

Given the breadth of the terms used in the statute, it is not surprising that courts have identified forms of information that constitute both DRAS and contents. In the context of Internet communications, a Uniform Resource Locator (URL) – “an address that can lead you to a file on any computer connected to the Internet”³¹ – constitutes a form of “addressing information” under the ordinary meaning of that term. Yet, in some circumstances a URL can also include “contents” as defined in Section 2510(8). In particular, if a user runs a search using an Internet search engine, the “search phrase would appear in the URL after the first forward slash” as part of the addressing information, but would also reveal contents, *i.e.*, the “‘substance’ and ‘meaning’ of the communication . . . that the user is conducting a search for information on a particular topic.” In re Application of the United States for an Order Authorizing the Use of a Pen Register and Trap, 396 F. Supp.2d 45, 49 (D. Mass. 2005) (Collins, Magistrate Judge); see

³¹ See Newton’s Telecom Dictionary 971 (24th ed. 2008).

also In re Pharmatrak, Inc., 329 F.3d 9, 16, 18 (1st Cir. 2003) (URLs including search terms are “contents” under Section 2510(8)).³² In the context of telephone communications, the term “dialing information” can naturally be understood to encompass all digits dialed by a caller. However, some digits dialed after a call has been connected, or “cut through,” can constitute “contents” – for example, if the caller is inputting digits in response to prompts from an automated prescription refill system, the digits may convey substantive instructions such as the prescription number and desired pickup time for a refill. Courts accordingly have described post-cut-through digits as dialing information, some of which also constitutes contents. See In re Application of the United States for an Order (1) Authorizing the Installation and Use of a PR/TT Device and (2) Authorizing Release of Subscriber and Other Information, 622 F. Supp.2d 411, 412 n.1, 413 (S.D. Tex. 2007) (Rosenthal, District Judge); In re Application, 396 F. Supp.2d at 48.

In light of the foregoing, the Court rejects the government’s contention that DRAS information and contents are mutually exclusive categories. Instead, the Court will, in accordance with the language and structure of Section 3127(3) and (4), apply a two-part test to

³² But see H.R. Rep. No. 107-236(I), at 53 (2001) (stating that the portion of a URL “specifying Web search terms or the name of a requested file or article” is not DRAS information and therefore could not be collected by a PR/TT device).

the information that the government seeks to acquire and use in this case: (1) is the information DRAS information?; and (2) is it contents?³³

In determining whether or not the types of information sought by the government constitute DRAS information, the Court is guided by the ordinary meanings of the terms “addressing,” “routing,” and “signaling,” and by the context in which the terms are used.³⁴ As the government asserts, “addressing information” may generally be understood to be “information that identifies recipients of communications or participants in a communication” and “may refer to people [or] devices.” Memorandum of Law at 37.³⁵ The Court also agrees with the government that “routing information” can generally be understood to include information regarding “the path or means by which information travels.” Memorandum of Law at 37. As will be explained more fully in the discussion of “communications actions” below, the Court adopts a somewhat narrower definition of “signaling information” than the government. In summary, the Court concludes that signaling information includes information that is utilized in

³³ To decide the issues presented by the application, the Court need not reach the government’s contention that Congress intended DRAS information to include all information that is not contents, or its alternative argument that, if there is a third category consisting of non-DRAS, non-content information, a PR/TT device may properly collect such information. See Memorandum of Law at 49-51.

³⁴ The government does not contend that any of the information sought constitutes only “dialing information,” which it asserts “presumptively relates to telephones.” Memorandum of Law at 37 n.19.

³⁵ See Newton’s Telecom Dictionary at 89 (“An address comprises the characters identifying the recipient or originator of transmitted data.”).

or pertains to (1) logging into or out of an account or (2) processing or transmitting an e-mail or IM communication. See pages 50-56, infra.³⁶

With regard to “contents,” the Court is, of course, bound by the definition set forth in Section 2510(8), which, as noted, covers “any information concerning the substance, purport, or meaning” of the wire or electronic communication to which the information relates. When the communication at issue is between or among end users, application of the definition of “contents” can be relatively straightforward. For an e-mail communication, for example, the contents would most obviously include the text of the message, the attachments, and the subject-line information. In the context of person-to-computer communications like the interactions between a user and a web-mail service provider, however, determining what constitutes contents can become “hazy.” See 2 LaFave, et al. Criminal Procedure § 4.6(b) at 476 (“[W]hen a person sends a message to a machine, the meaning of ‘contents’ is unclear.”). Particularly in the user-to-provider context, the broad statutory definition of contents includes some information beyond what might, in ordinary parlance, be considered the contents of a communication.

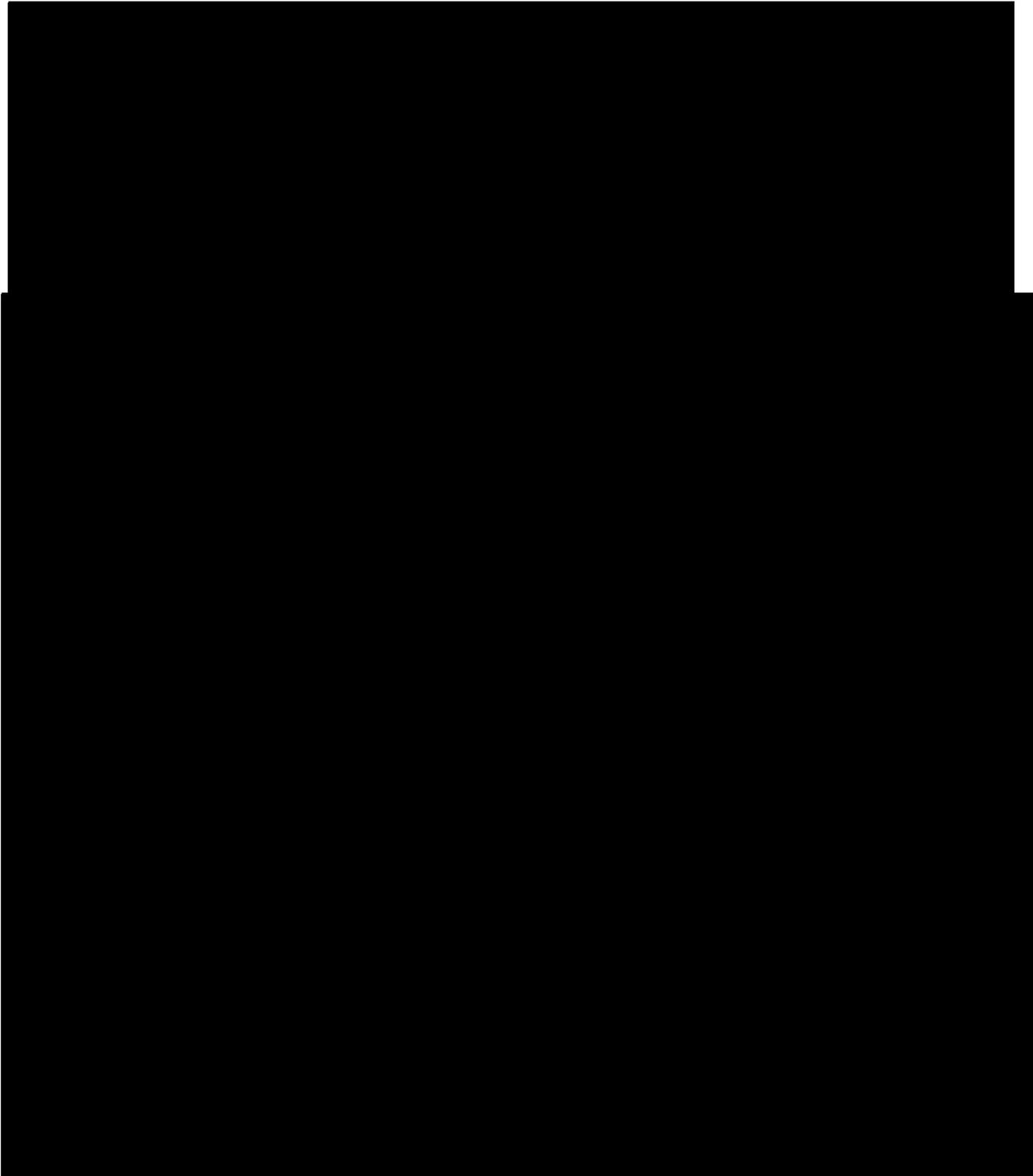
2. The Categories of Metadata Sought for Acquisition

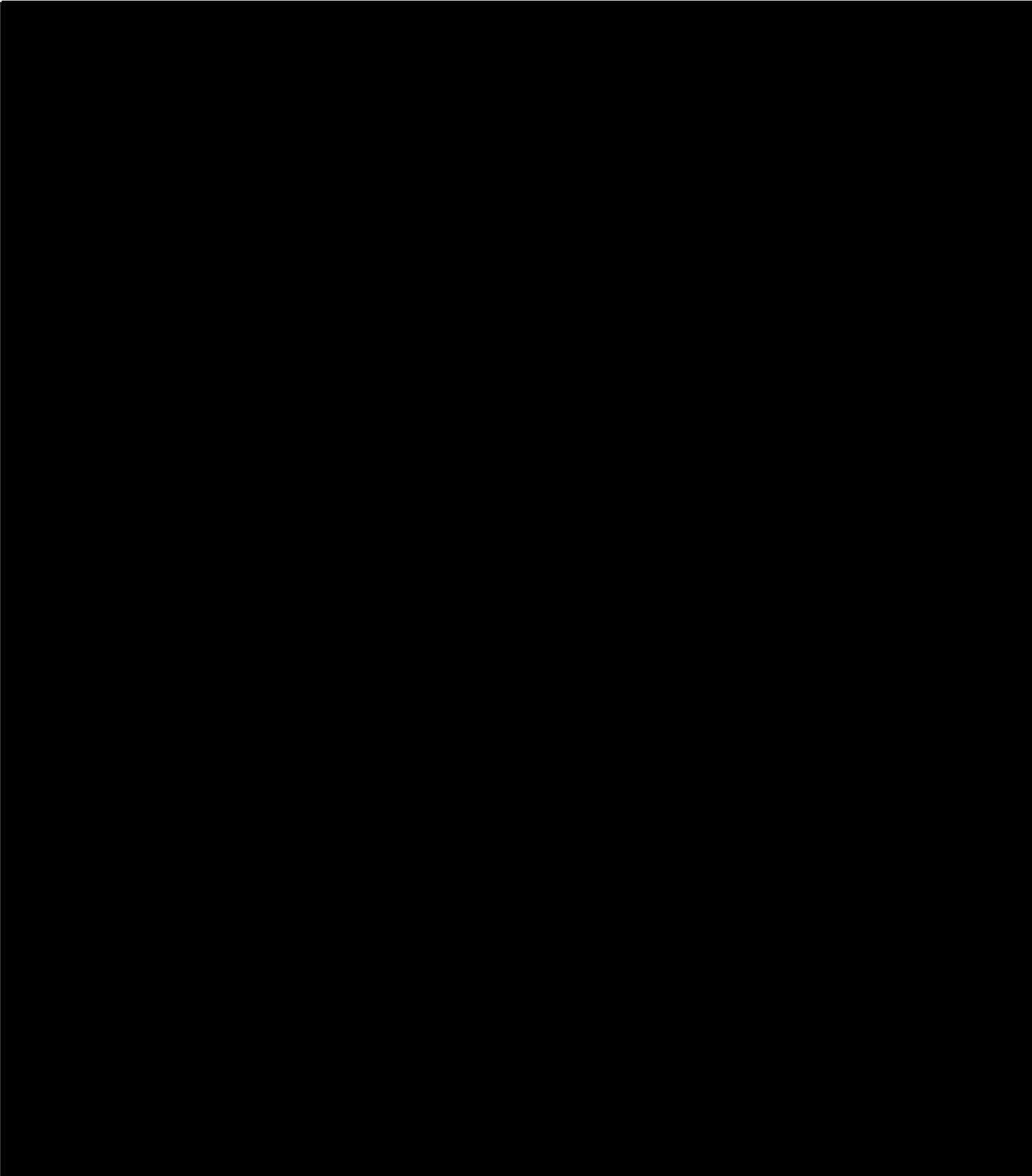
The government requests authority to [REDACTED] categories of

[REDACTED]

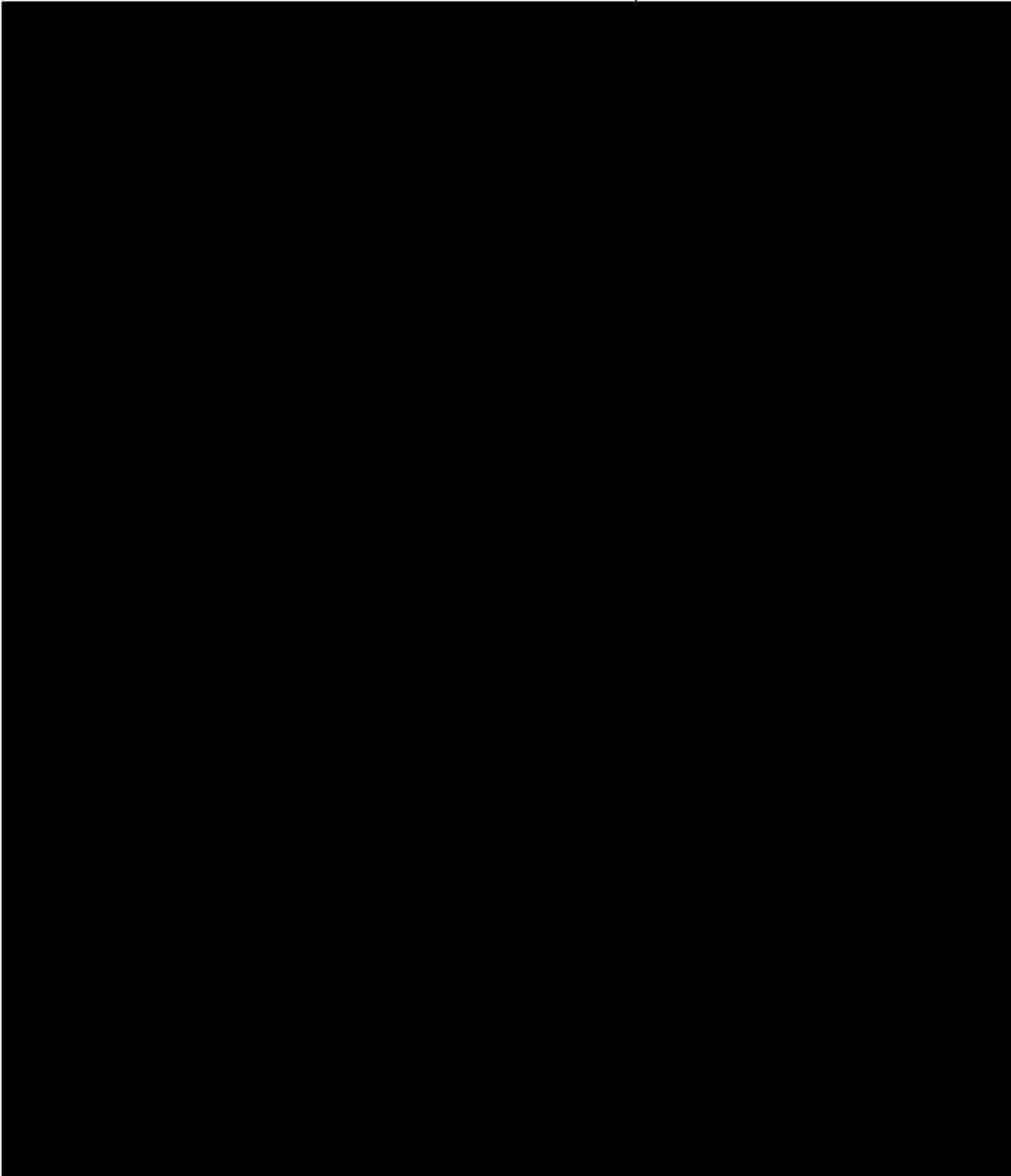
³⁶ For purposes of this Opinion, the term “e-mail communications” refers to e-mail messages sent between e-mail users [REDACTED]

[REDACTED]



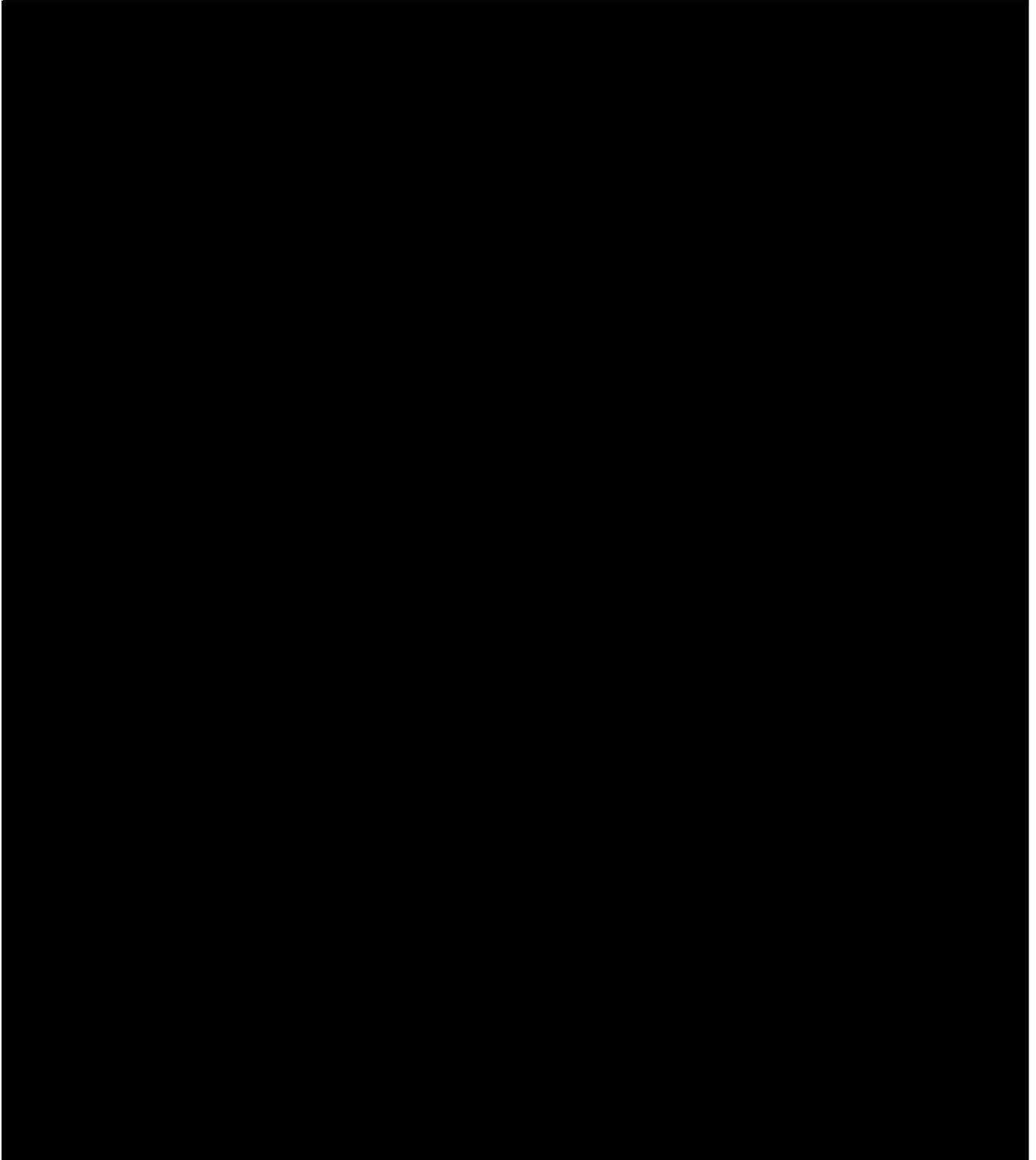


TOP SECRET//COMINT//ORCON,NOFORN



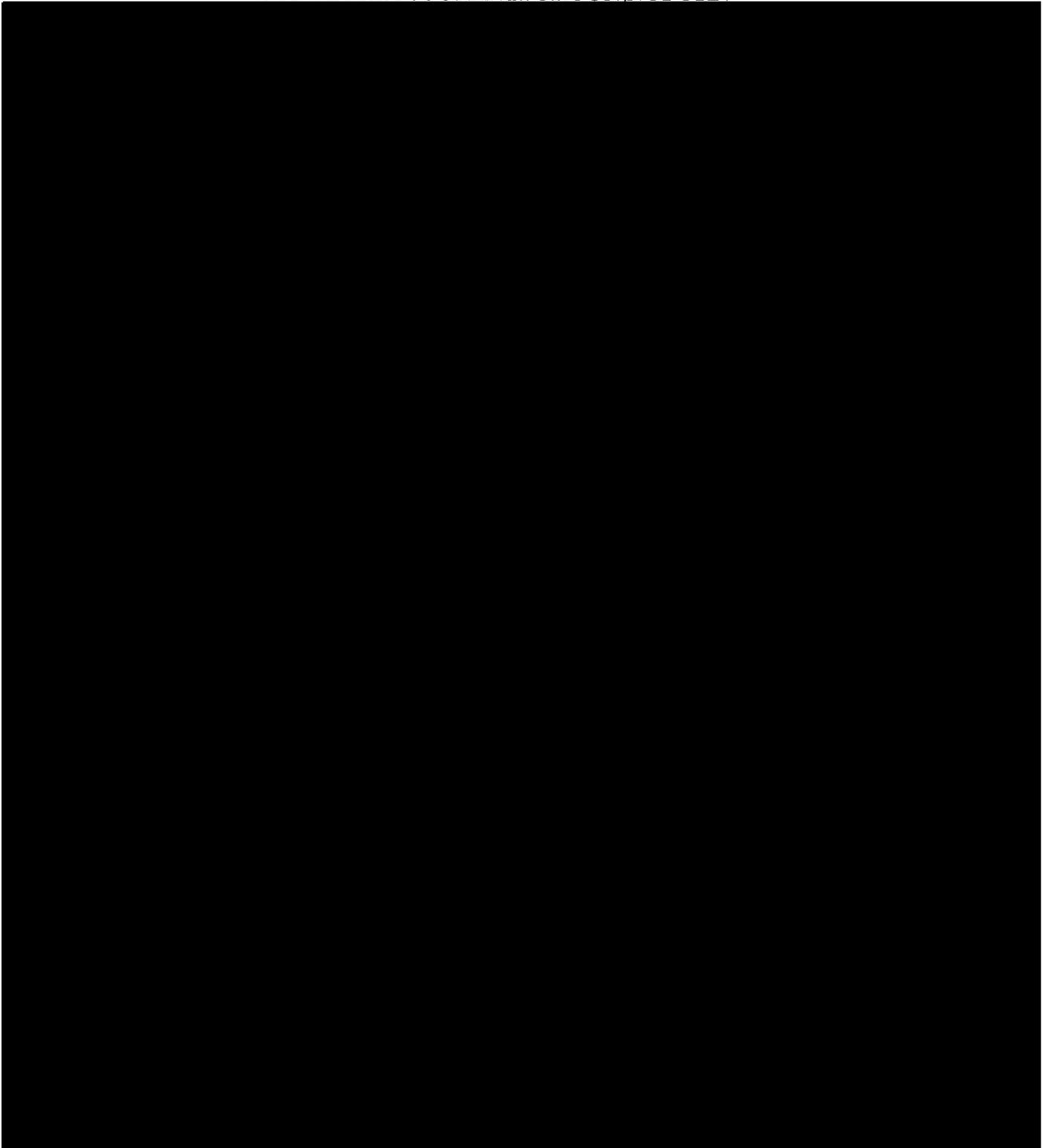
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



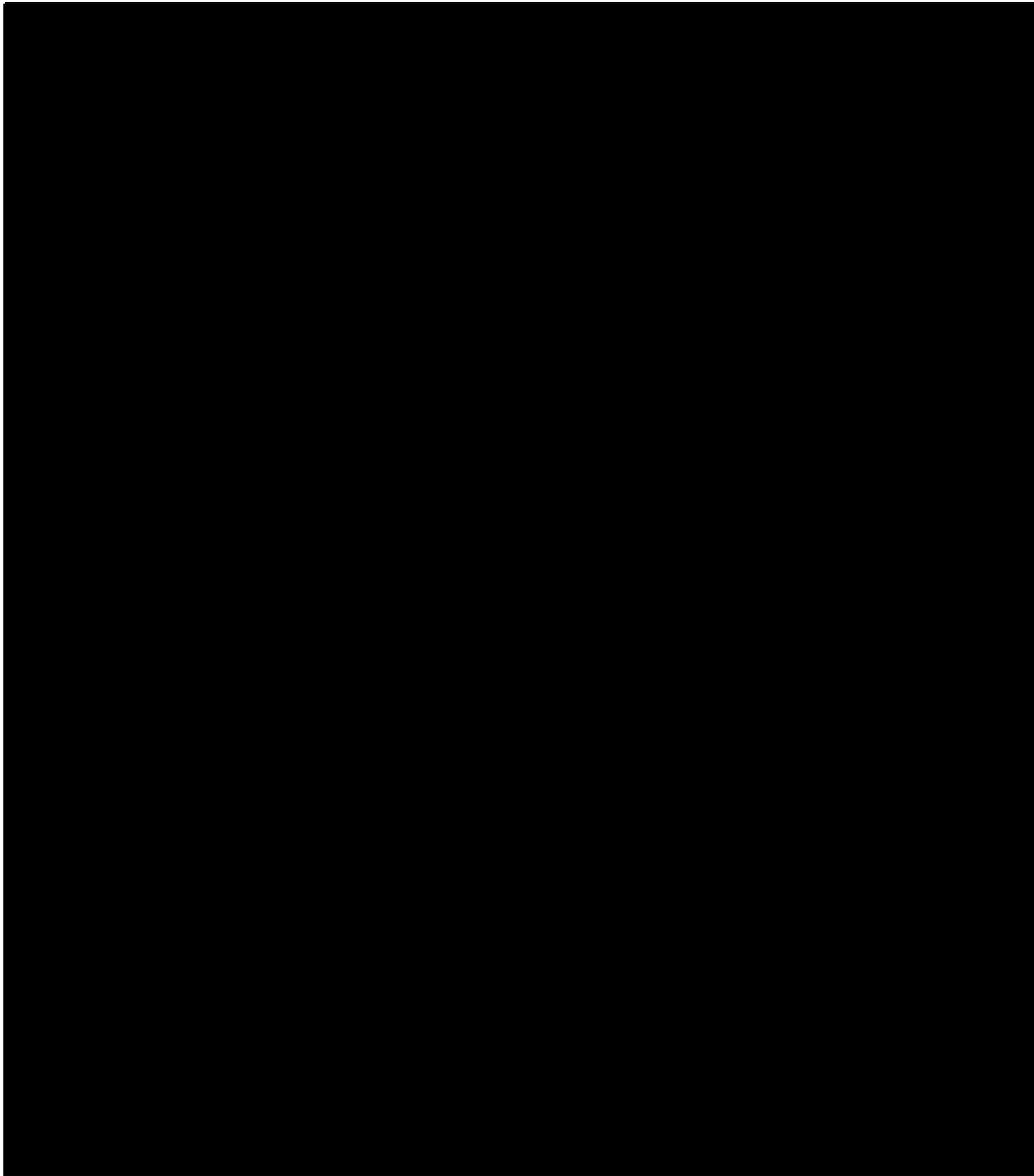
~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN



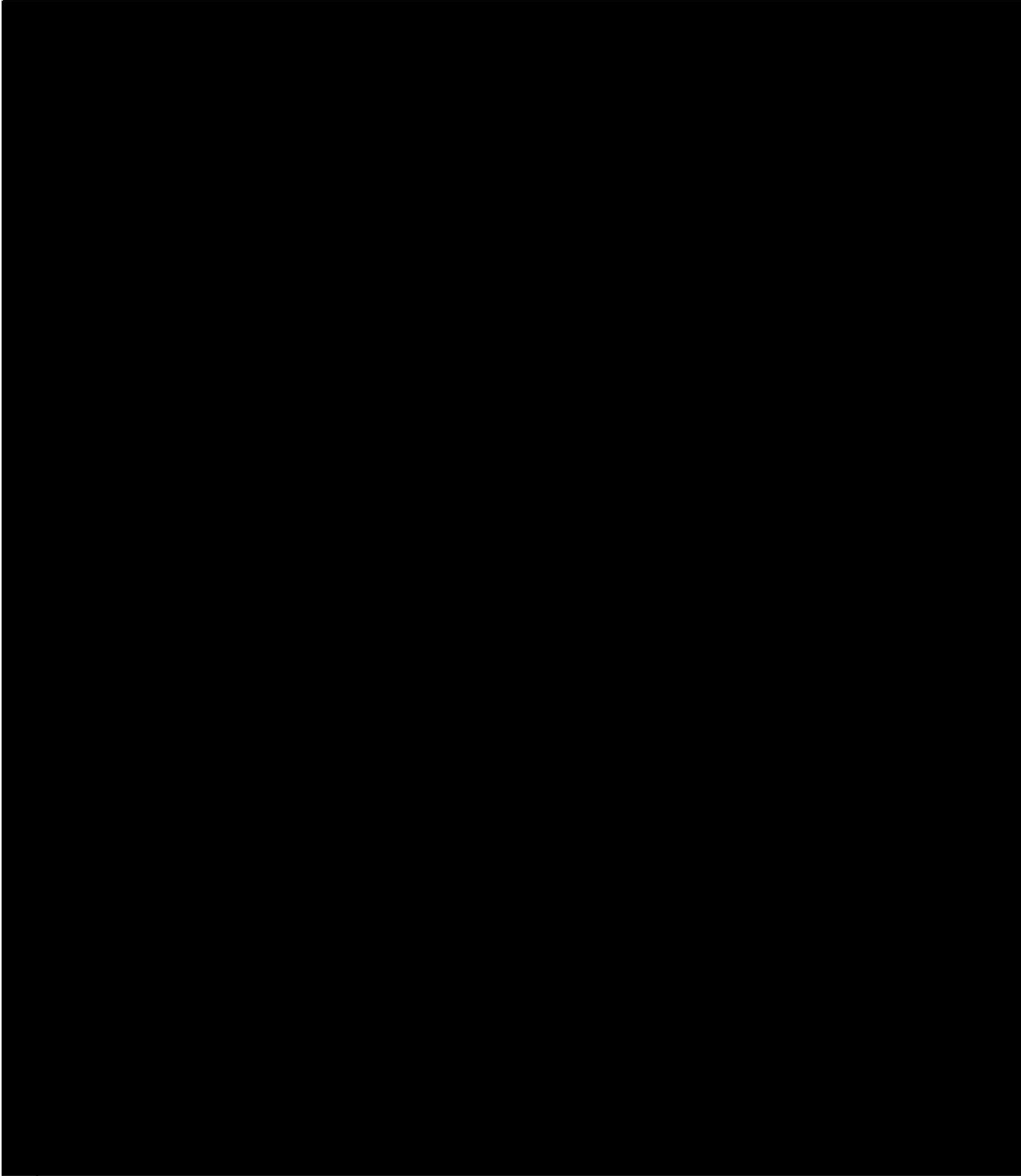
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



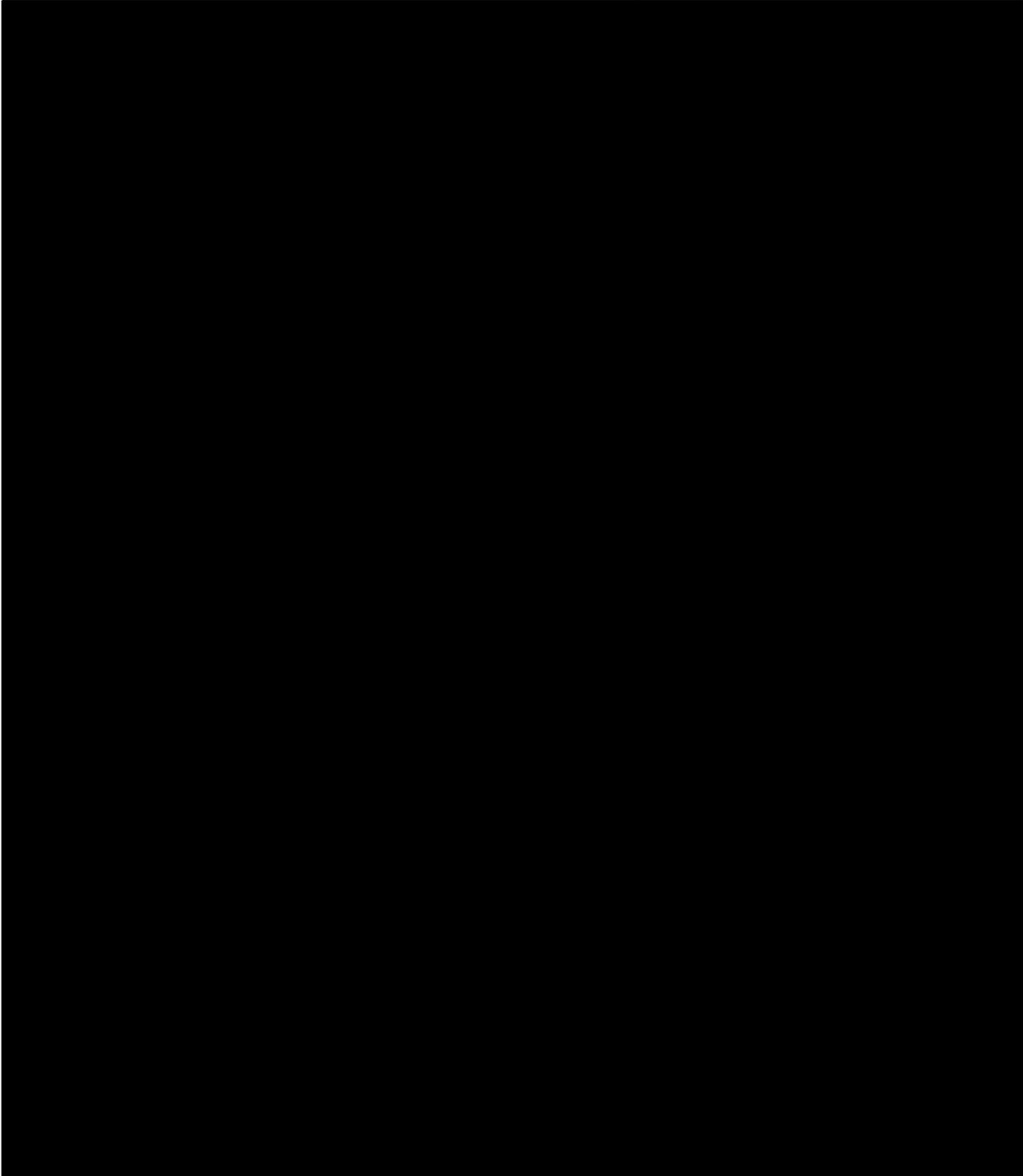
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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

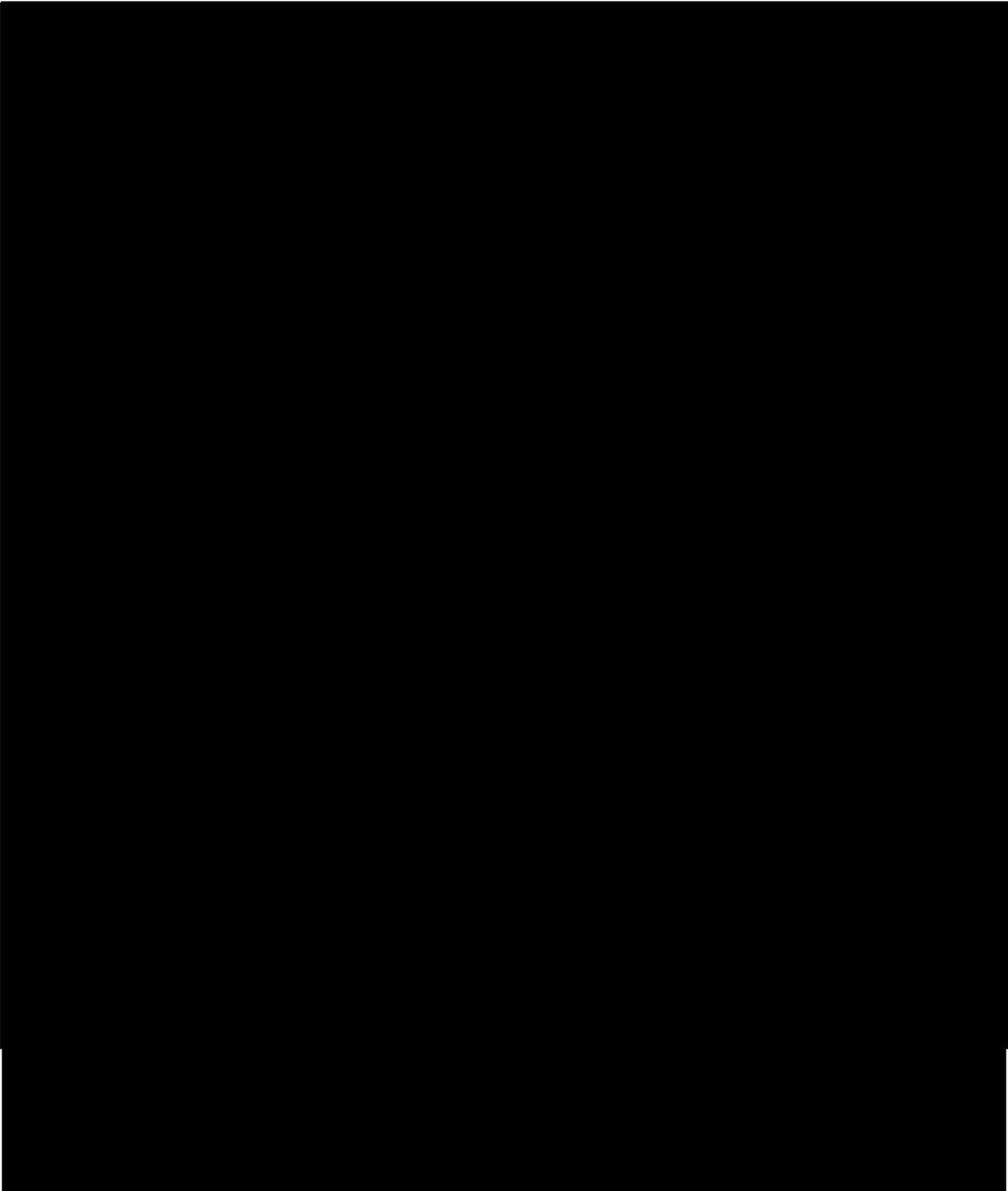


~~TOP SECRET//COMINT//ORCON,NOFORN~~

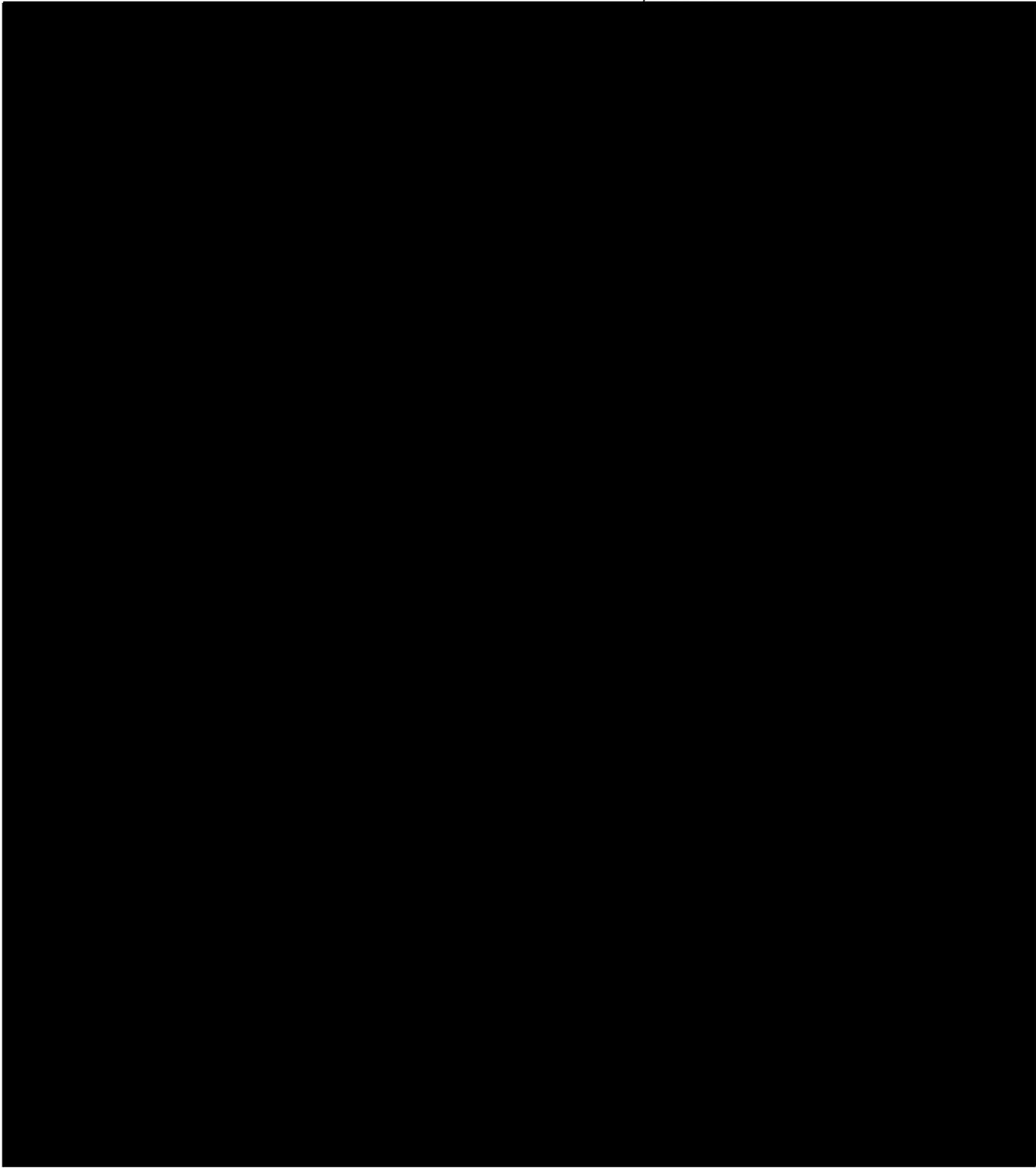
TOP SECRET//COMINT//ORCON,NOFORN



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

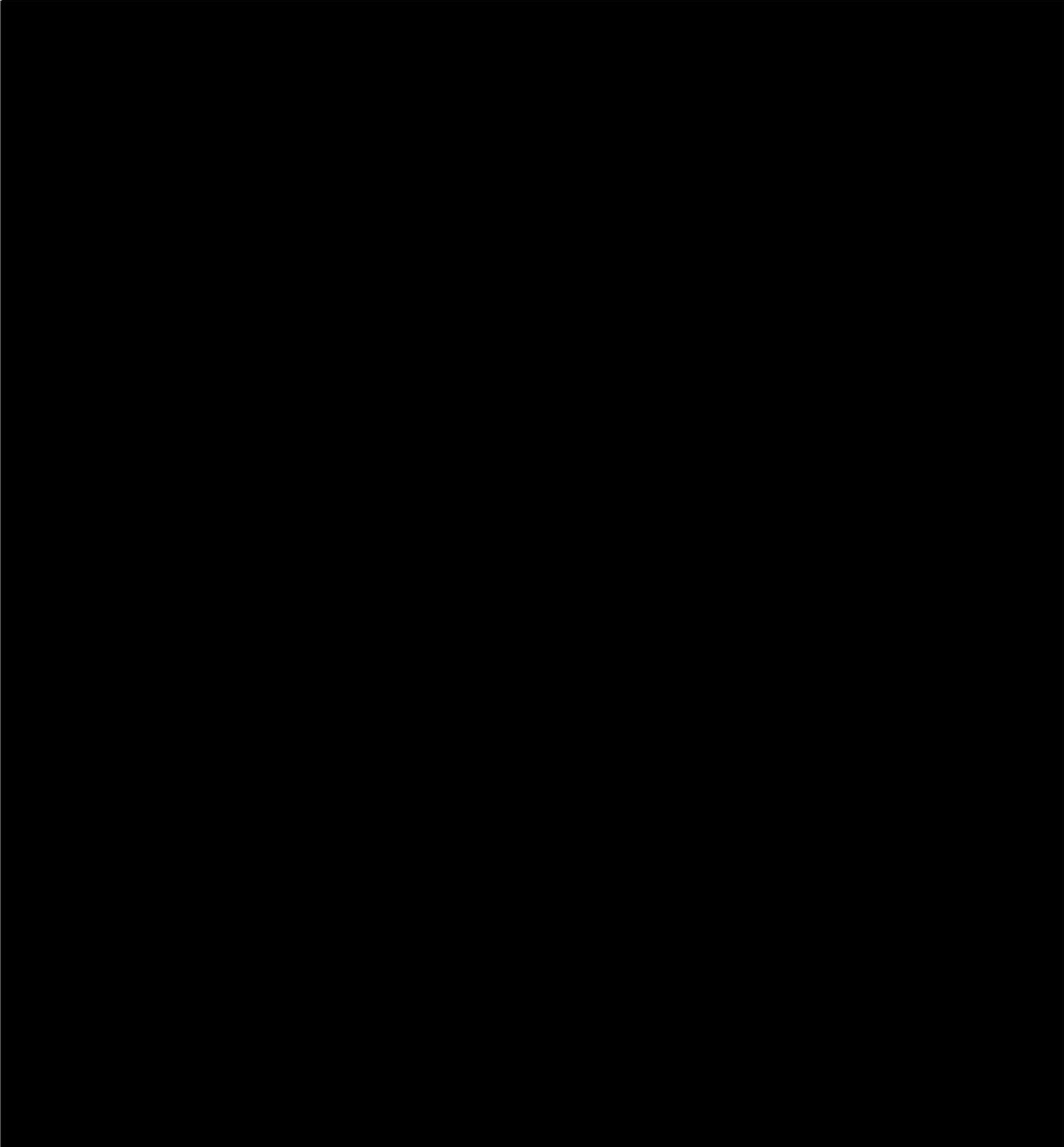


TOP SECRET//COMINT//ORCON,NOFORN



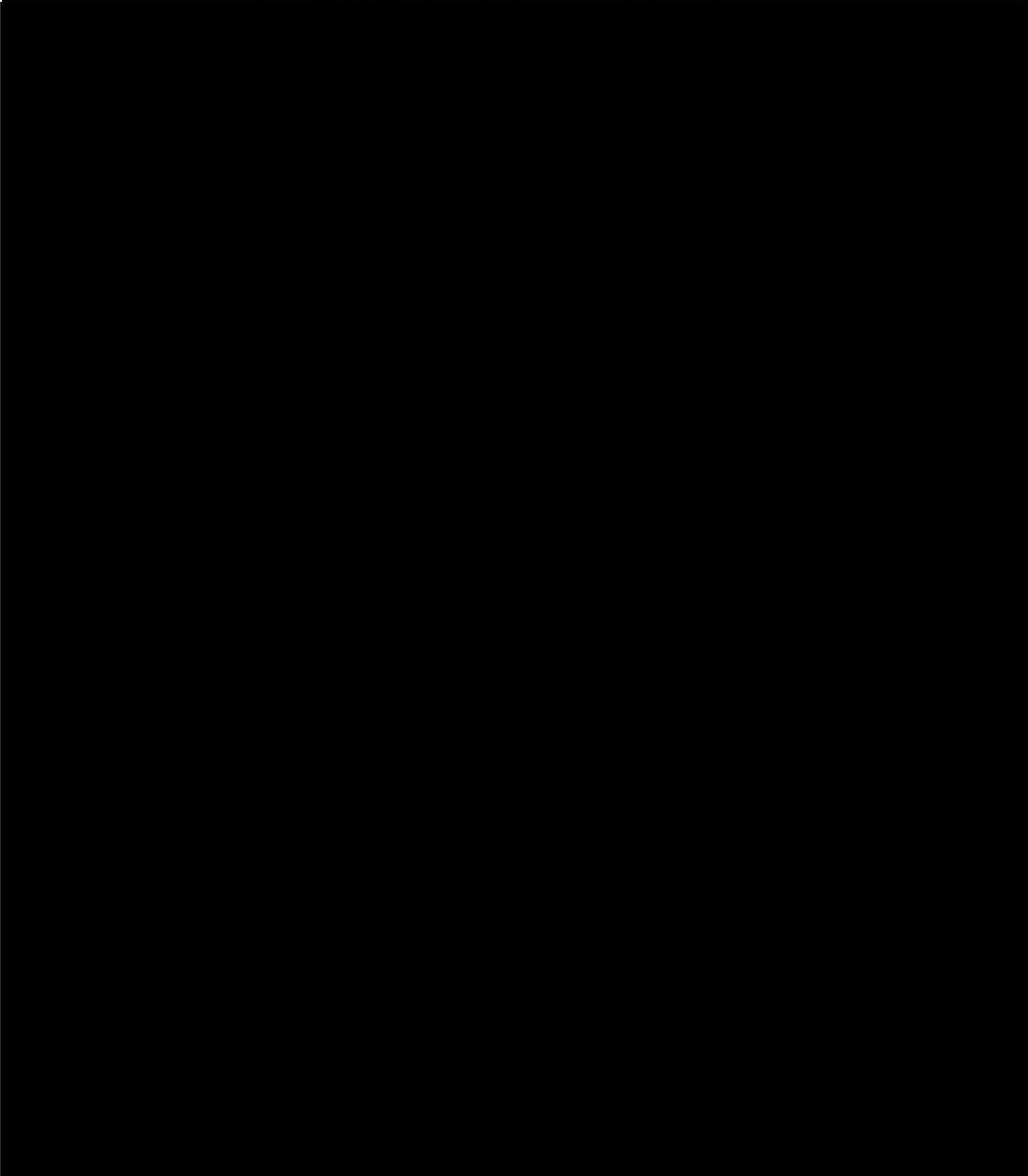
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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

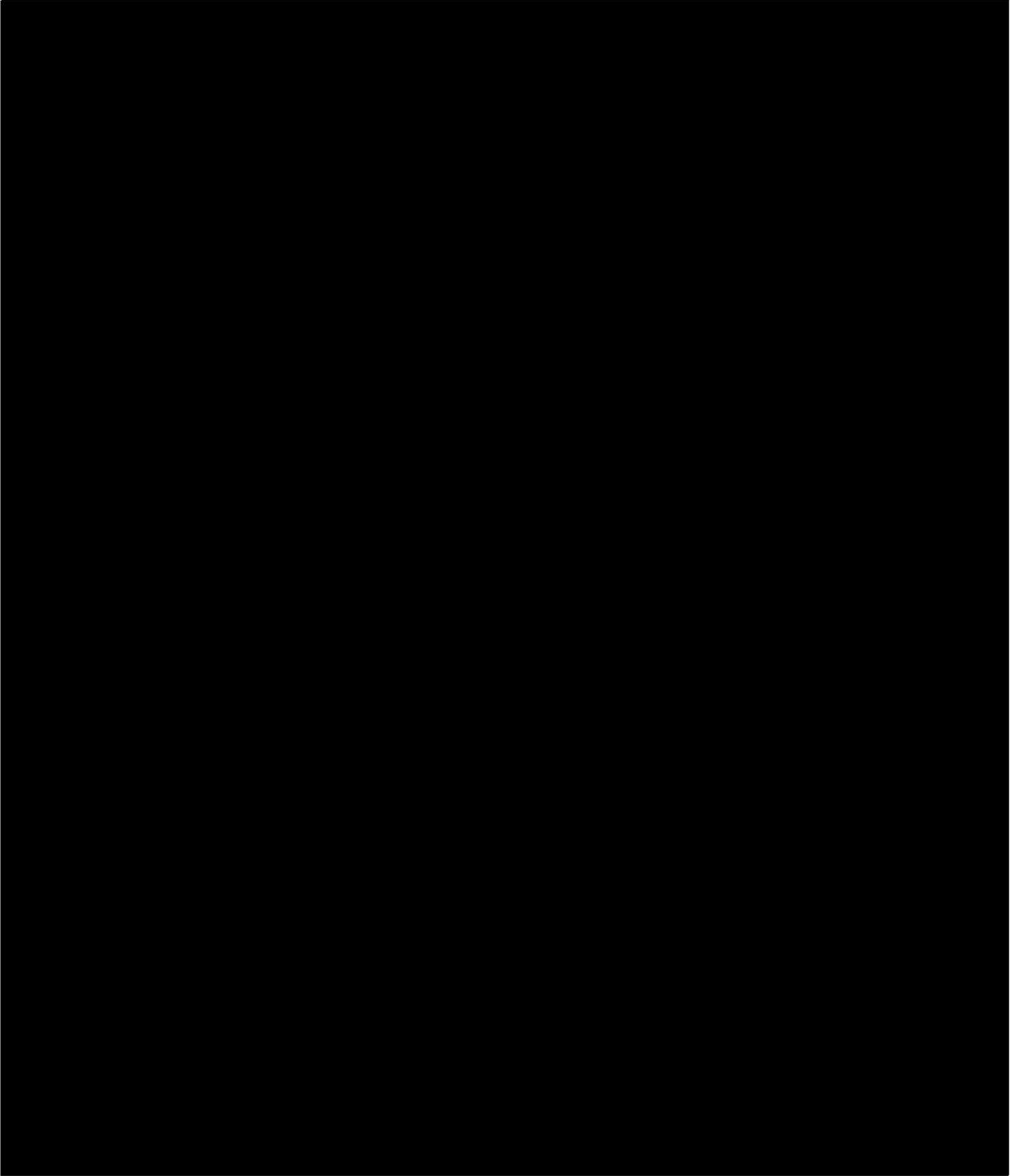


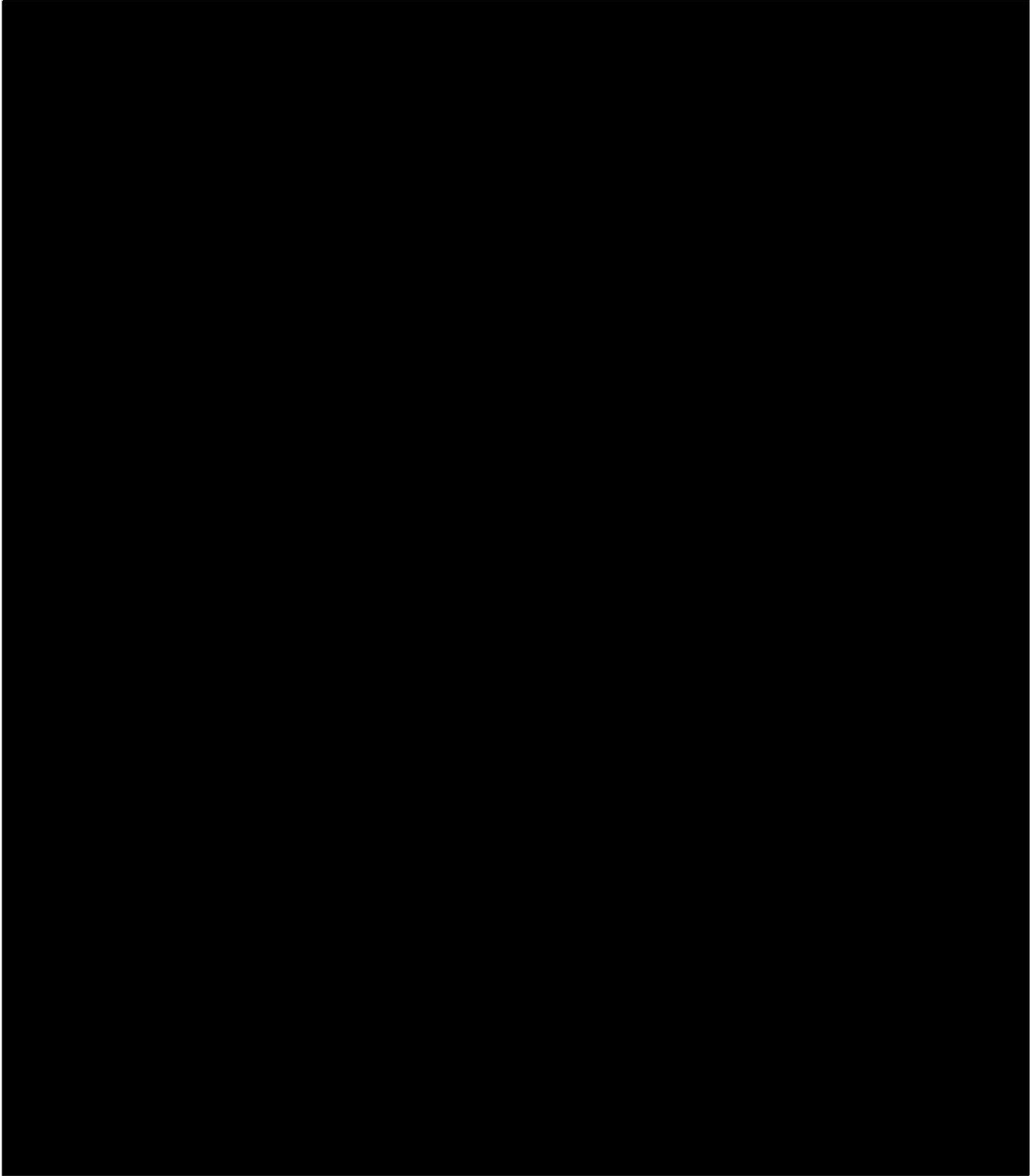
~~TOP SECRET//COMINT//ORCON,NOFORN~~

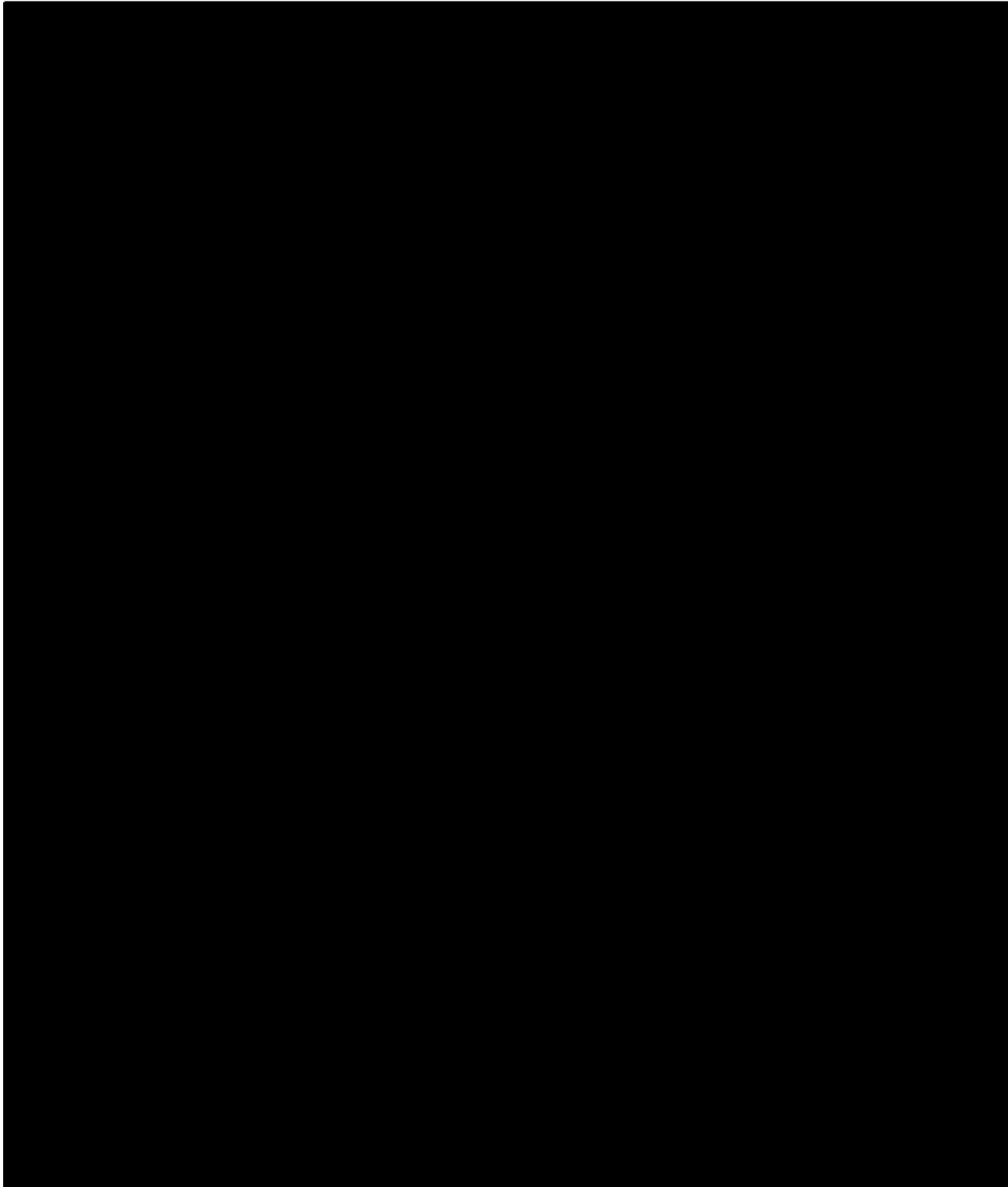
TOP SECRET//COMINT//ORCON,NOFORN

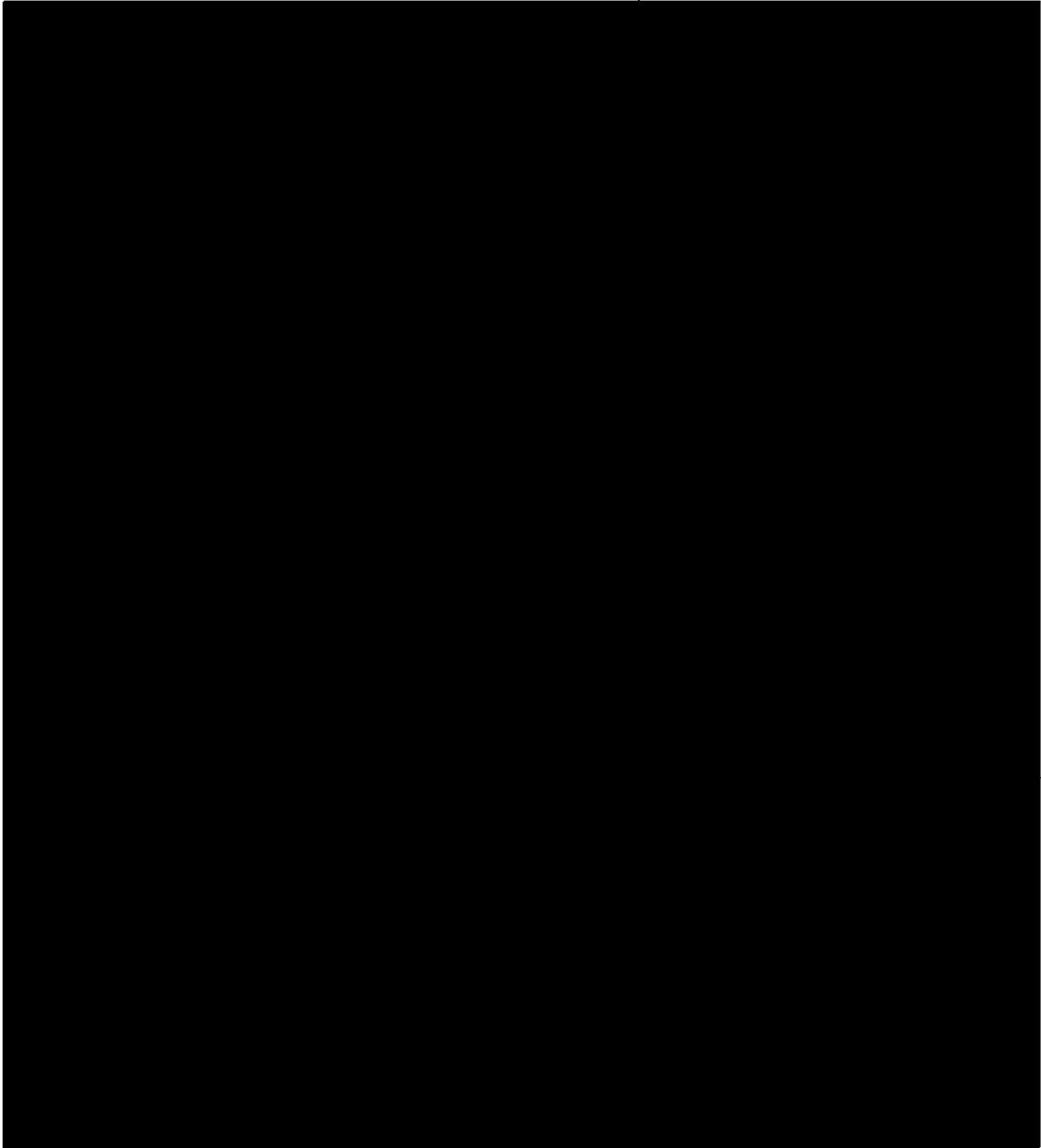


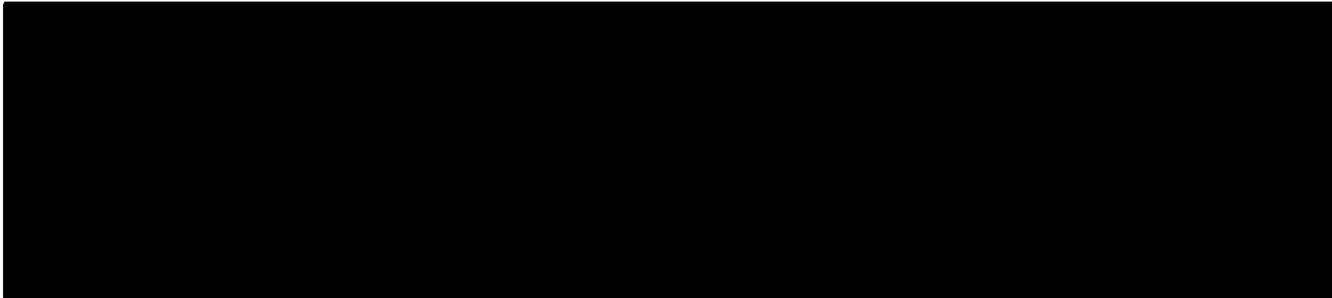
~~TOP SECRET//COMINT//ORCON,NOFORN~~



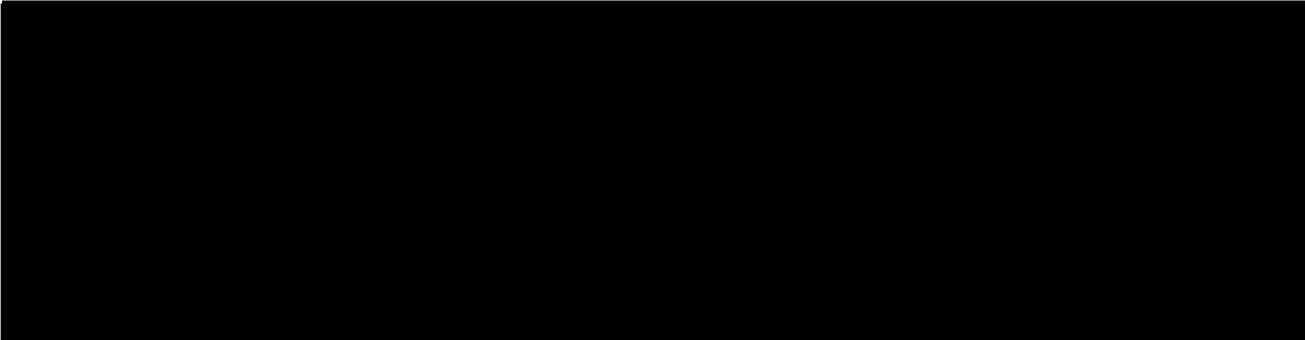








Within the definitions of “pen register” and “trap and trace device,” “signaling information” appears as the fourth and final item in a list of undefined terms that all modify “information”: “dialing, routing, addressing, [and/or] signaling information.” 18 U.S.C. § 3127(3), (4). It is well-established in statutory interpretation that one term appearing within a list may take its meaning from the character of the other listed terms.⁴⁷ Here, the other three terms modifying “information” are not merely “associated with” a communication. Rather, dialing, routing, and addressing information are all types of information that, in the context of a



⁴⁷ See, e.g., Dolan v. United States Postal Serv., 546 U.S. 481, 486-87 (2006) (“‘[A] word is known by the company it keeps’ – a rule that ‘is often wisely applied where a word is capable of many meanings in order to avoid the giving of unintended breadth to the Acts of Congress.’”) (quoting Jarecki v. G.D. Searle & Co., 367 U.S. 303, 307 (1961)); Schreiber v. Burlington Northern, Inc., 472 U.S. 1, 8 (1985) (recognizing the “‘familiar principle of statutory construction that words grouped in a list should be given related meaning’”) (quoting Securities Indus. Ass’n v. Board of Governors, 468 U.S. 207, 218 (1984)).

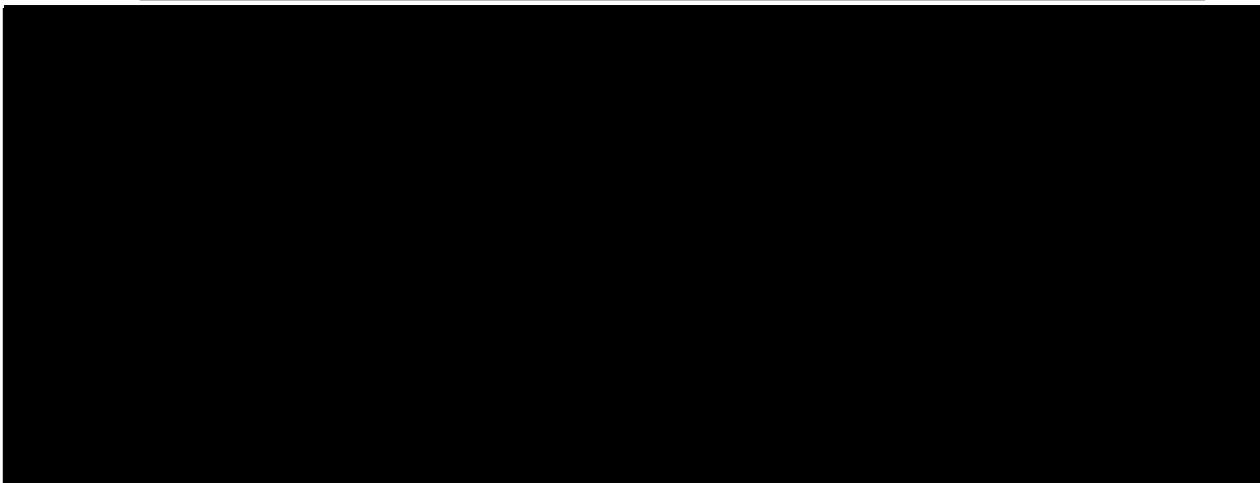
communication, particularly relate to the transmission of the communication to its intended party. By placing “signaling” within the same list of types of communication-related information, Congress presumably intended “signaling information” likewise to relate to the transmission of a communication.

The wording of a related provision lends further support to this interpretation:

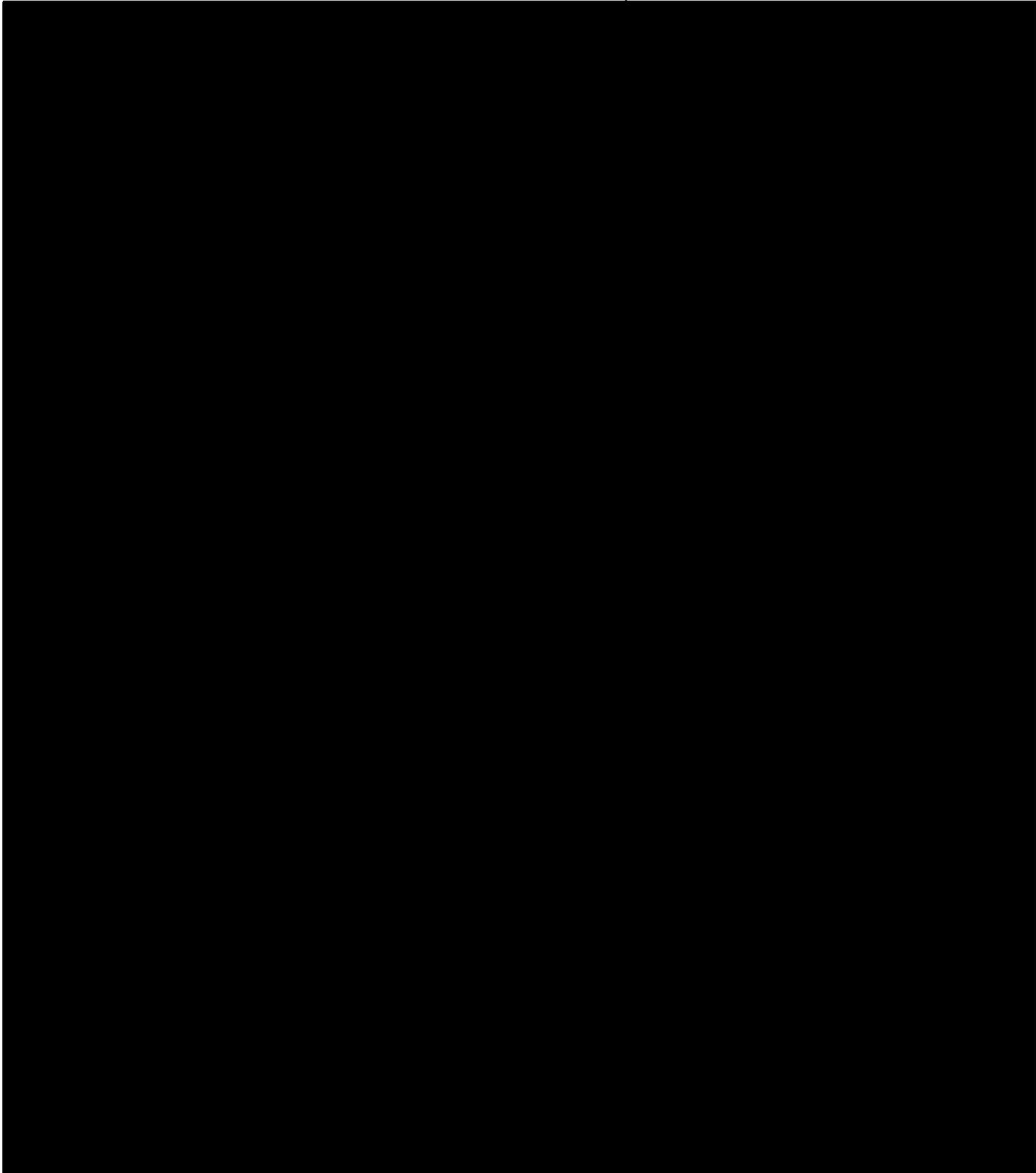
A government agency authorized to install and use a pen register or trap and trace device . . . shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

18 U.S.C. § 3121(c) (emphasis added). Questions of available technology aside, there is no reason to think Congress intended to compel an agency deploying a PR/TT device to try to avoid acquiring data that would constitute DRAS information under the definitions of “pen register” and “trap and trace device.” For this reason, Section 3121(c) strongly suggests that the intended scope of acquisition under a PR/TT device is DRAS information utilized in the processing and transmitting of a communication.⁴⁸

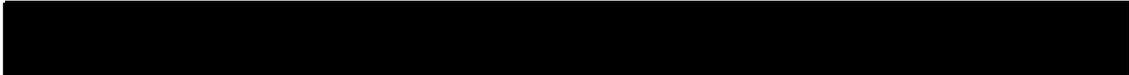
The legislative history relied on by the government, see Memorandum of Law at 52, actually points to a similar conclusion about the intended scope of signaling information to be acquired by a PR/TT device. It states that “orders for the installation of [PR/TT] devices may obtain any non-content information – ‘dialing, routing, addressing, and signaling information’ – utilized in the processing or transmitting of wire and electronic communications.” H.R. Rep. No. 107-236(I), at 53 (emphasis added; footnote omitted). Moreover, the particular types of information mentioned in the legislative history as DRAS information that may be collected by a PR/TT device all pertain to the processing or transmitting of a communication. See, e.g., id. (referencing “attempted connections,” including “busy signals” and “packets that merely request a telnet connection in the Internet context”). The House report states that “non-content information contained in the ‘options field’ of a network packet header constitutes ‘signaling’ information and is properly obtained by an authorized pen register or trap and trace device.” Id. at 53 n.1. 



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



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



b. Contents

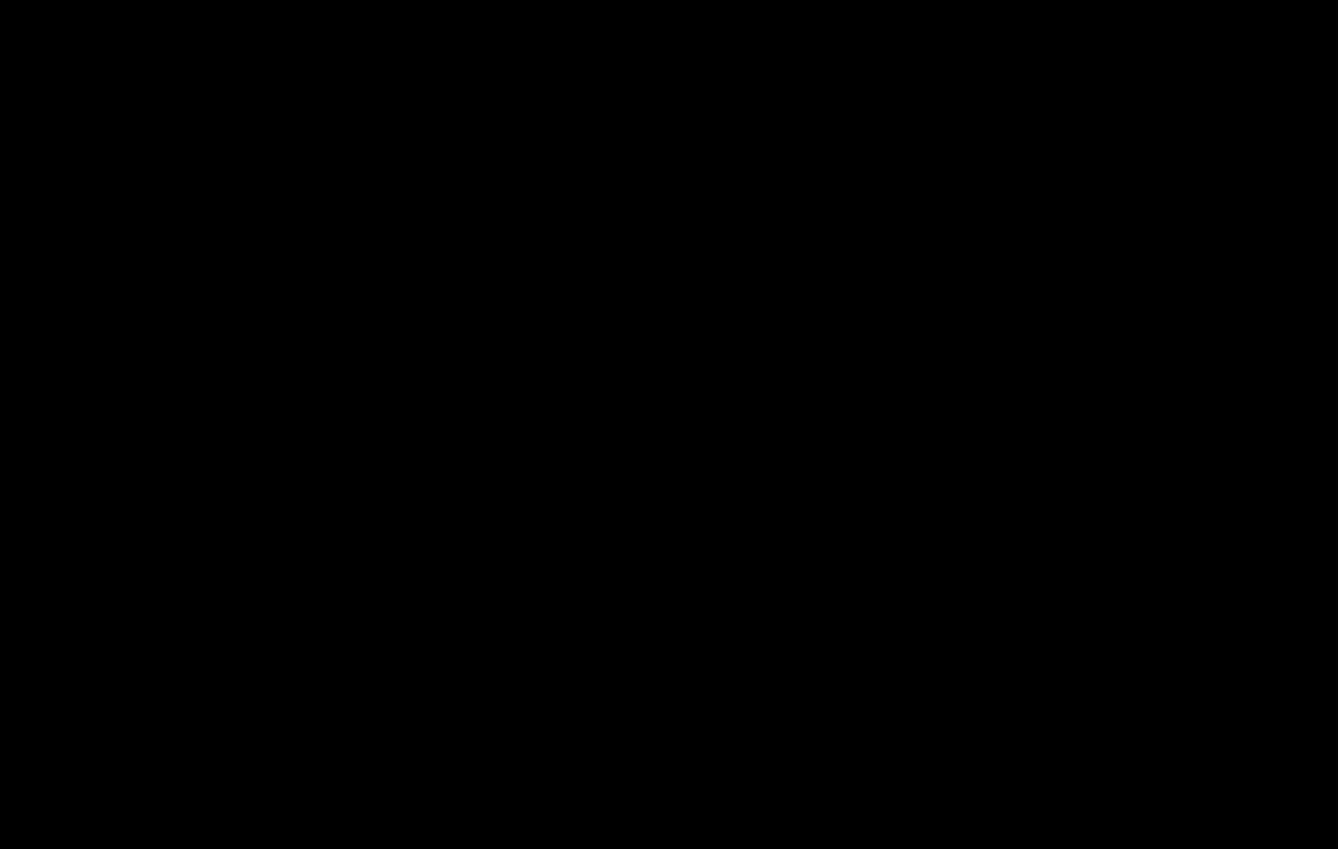
As noted above, “contents,” “when used with respect to any . . . electronic communication, includes any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8) (emphasis added). “Electronic communication” is also defined broadly, so that it encompasses the exchanges of information between account user and provider that are described by communications actions. And of course, the definitions of “pen register” and “trap and trace device” provide that the information acquired “shall not include the contents of any communication,” Section 3127(3) & (4) (emphasis added) – unqualified language that certainly seems to include electronic communications between account users and providers. The combined literal effect of these provisions appears to be that PR/TT devices may not obtain any information concerning the substance, purport, or meaning of any communication, including those between account users and providers, and that communications actions that divulge any such information would be impermissible “contents” for purposes of a PR/TT authorization.

The government does not directly confront the statutory text on this point. It does argue, however, that an expansive, literal understanding of the prohibition on acquiring “contents” would lead to an absurd and unintended restriction on what PR/TT devices can do. Specifically, the government notes that the electronic impulses transmitted by dialing digits on a telephone

⁴⁹ The Court’s understanding of “processing” and “transmitting” e-mail 
 is set forth below. See pages 63-64, infra.

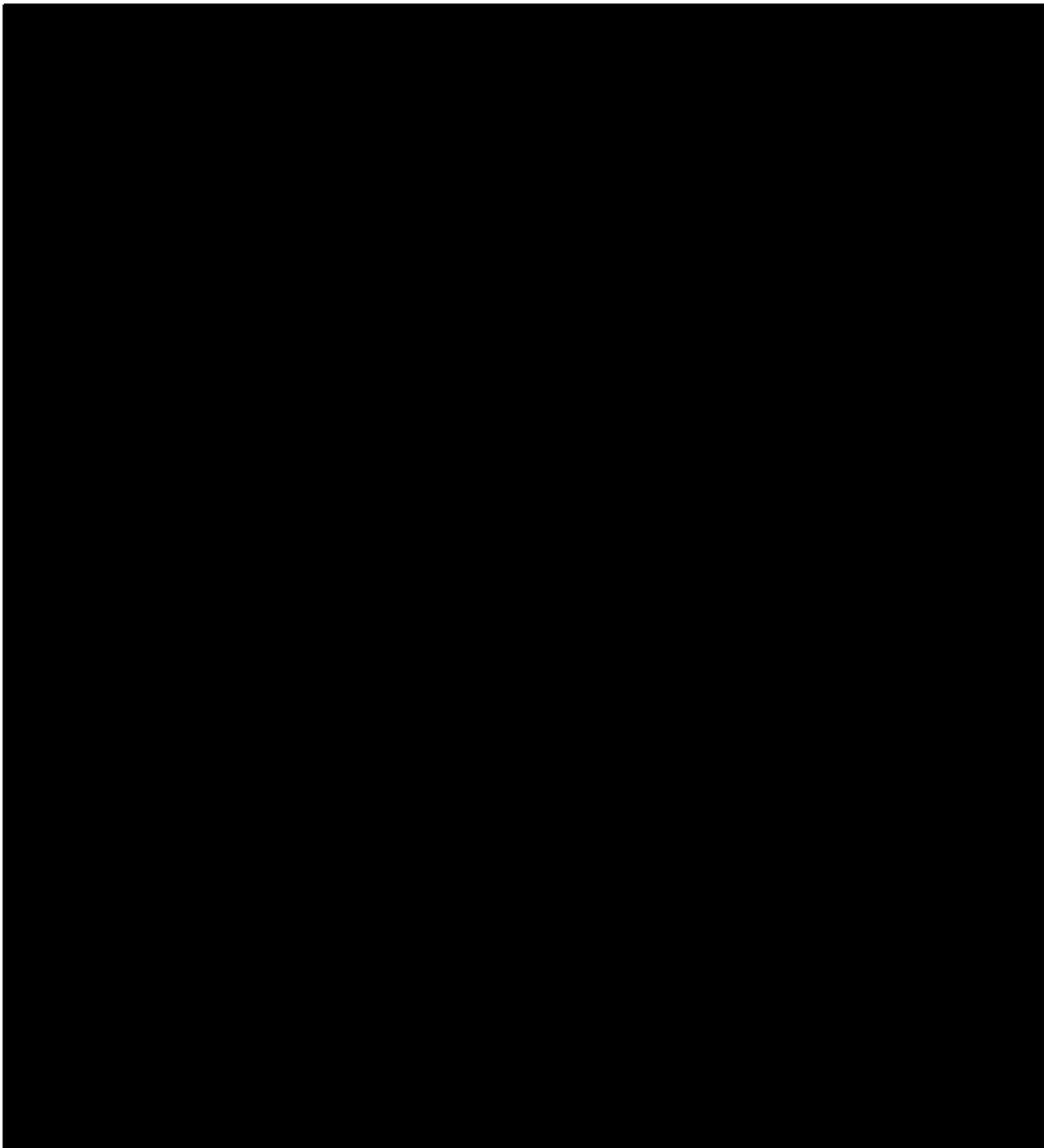
literally qualify as an “electronic communication” under Section 2510(12), but the “import” of that communication – i.e., “place a call from this telephone to the one whose number has been dialed” – has never been understood to be impermissible “contents” under the PR/TT statute.

See [REDACTED] Response at 7.



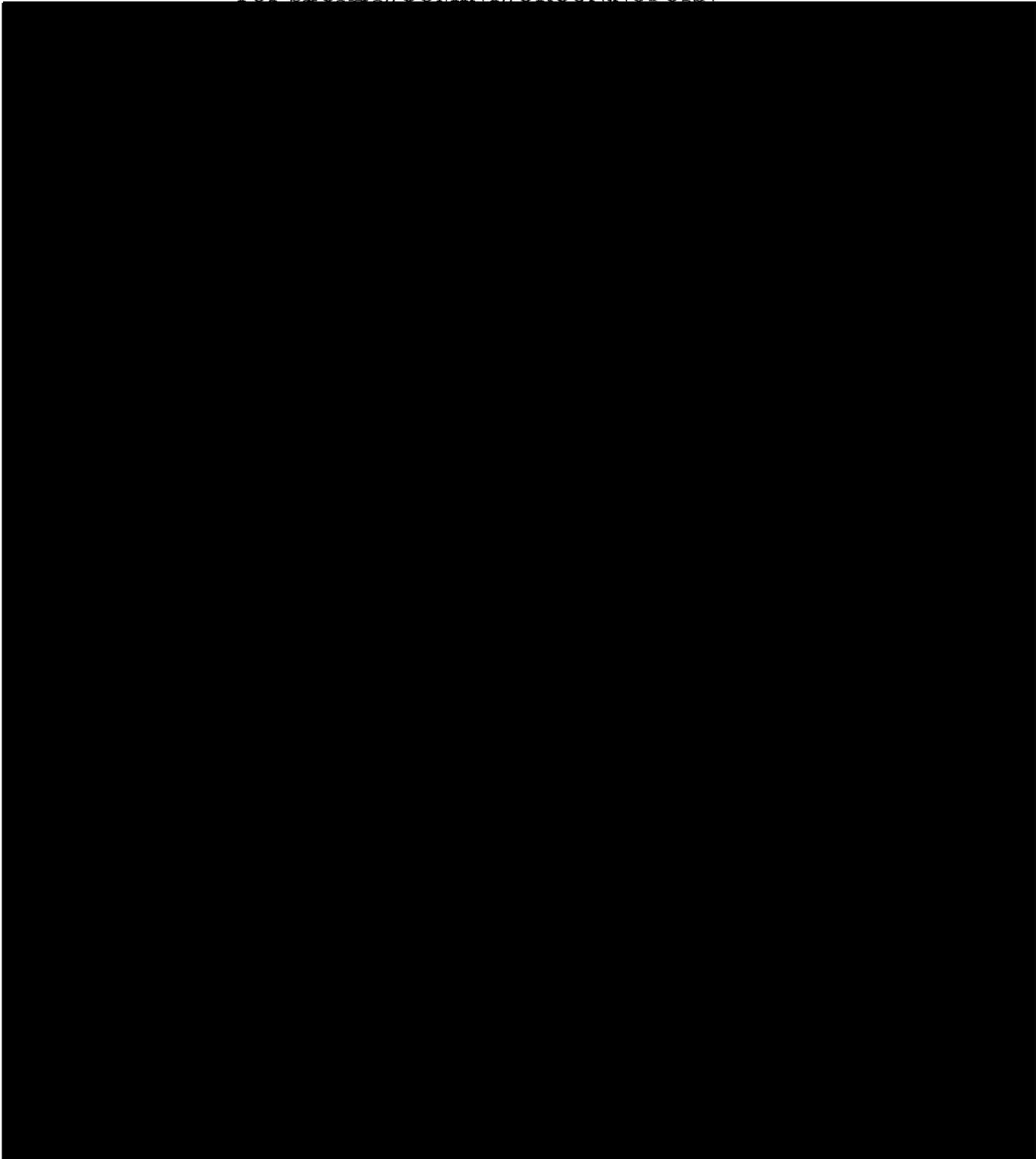
⁵⁰ While Congress sought, in the relevant statutory definitions, to reinforce “a line identical to the constitutional distinction” between contents and non-contents “drawn by the . . . Supreme Court in Smith v. Maryland, 442 U.S. 735, 741-43 (1979),” H.R. Rep. No. 107-236(I), at 53, it also expanded the “pen register” and “trap and trace” definitions to a broad range of Internet communications for which the scope of Fourth Amendment protections is unclear, see, e.g., 2 LaFave, et al. Criminal Procedure § 4.4(a) at 456-57 (the law is “highly unsettled,” with “a range of different ways that courts plausibly could apply the Fourth Amendment to Internet communications”).

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

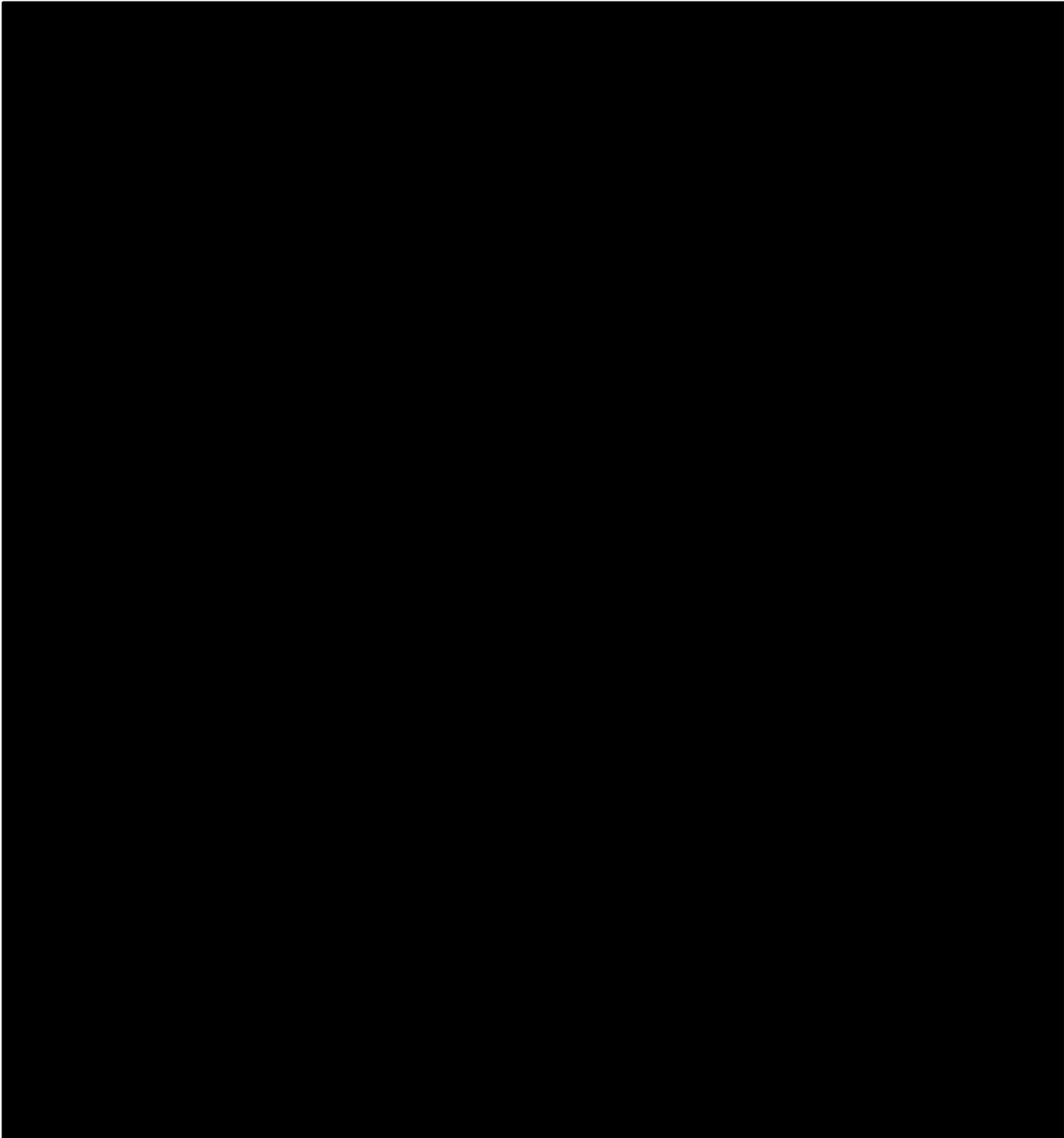


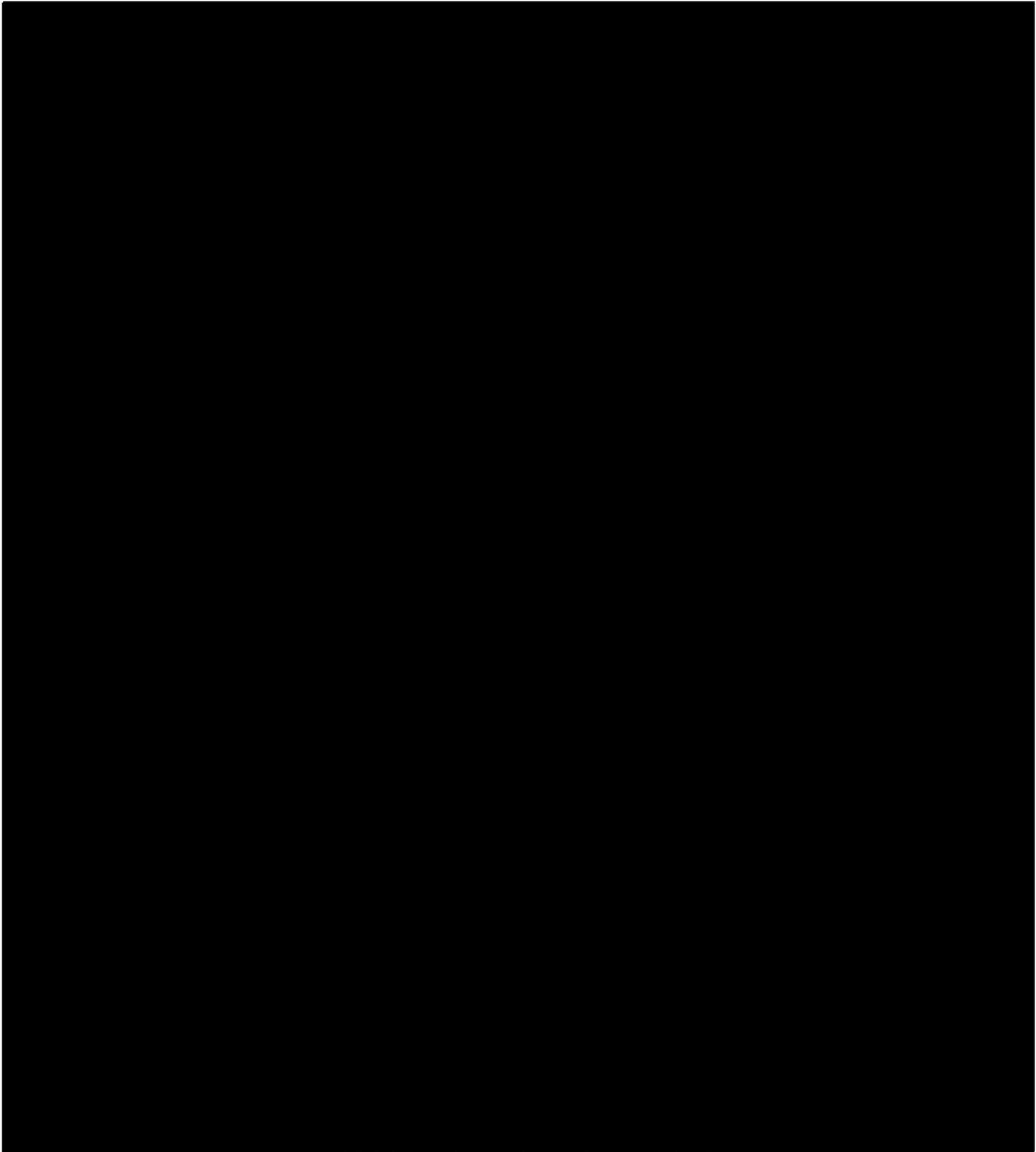
~~TOP SECRET//COMINT//ORCON,NOFORN~~

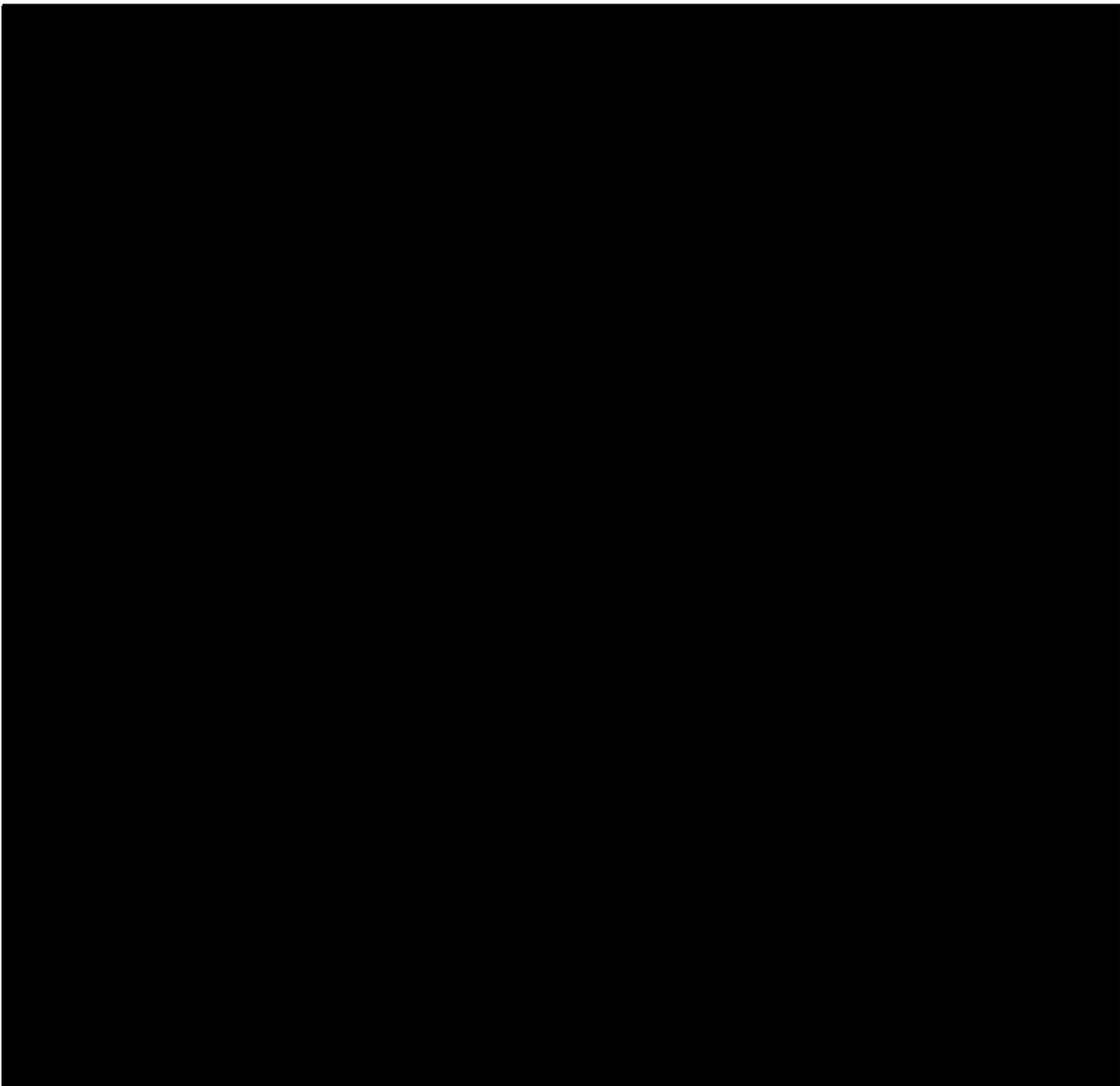
TOP SECRET//COMINT//ORCON,NOFORN



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

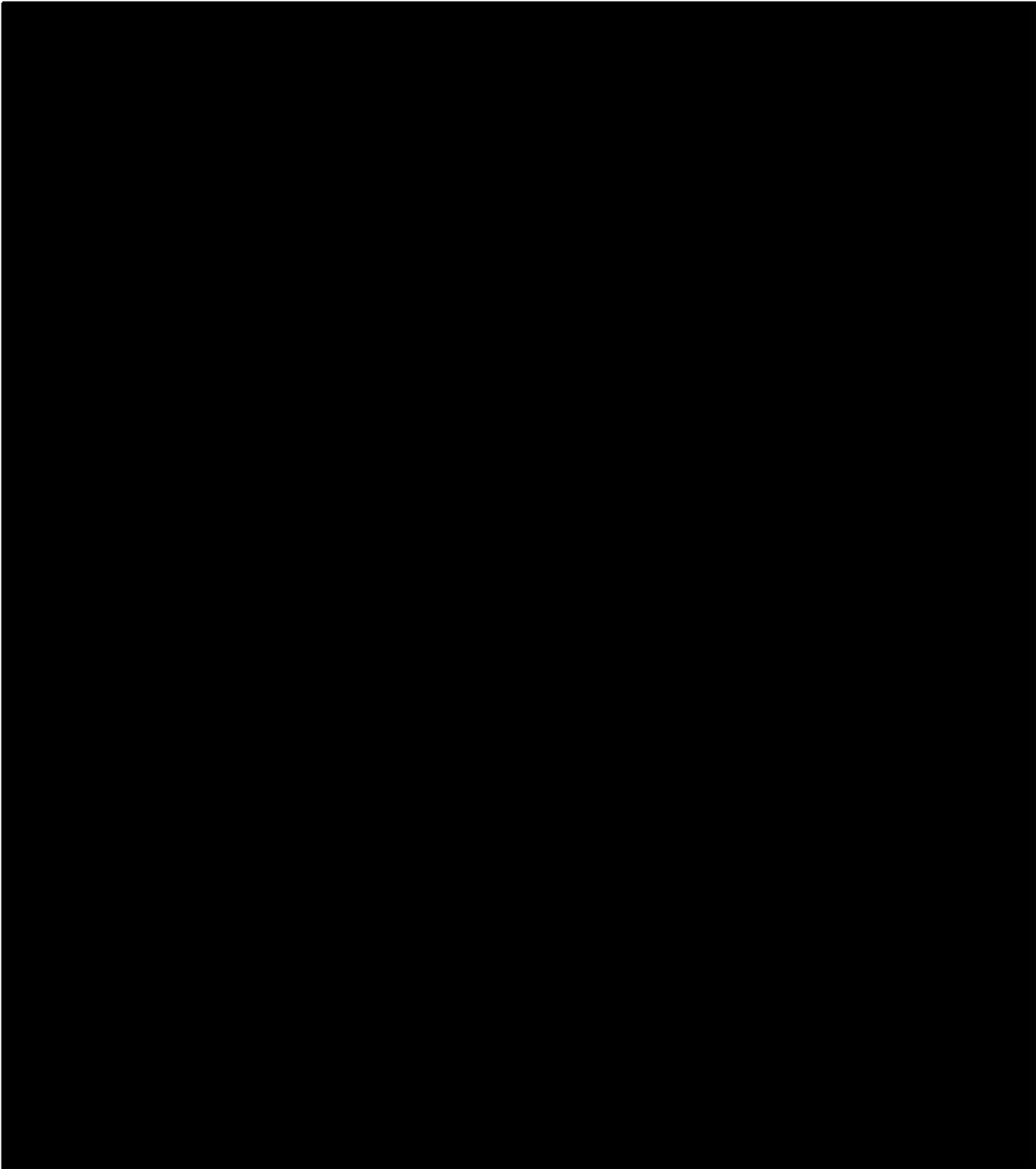






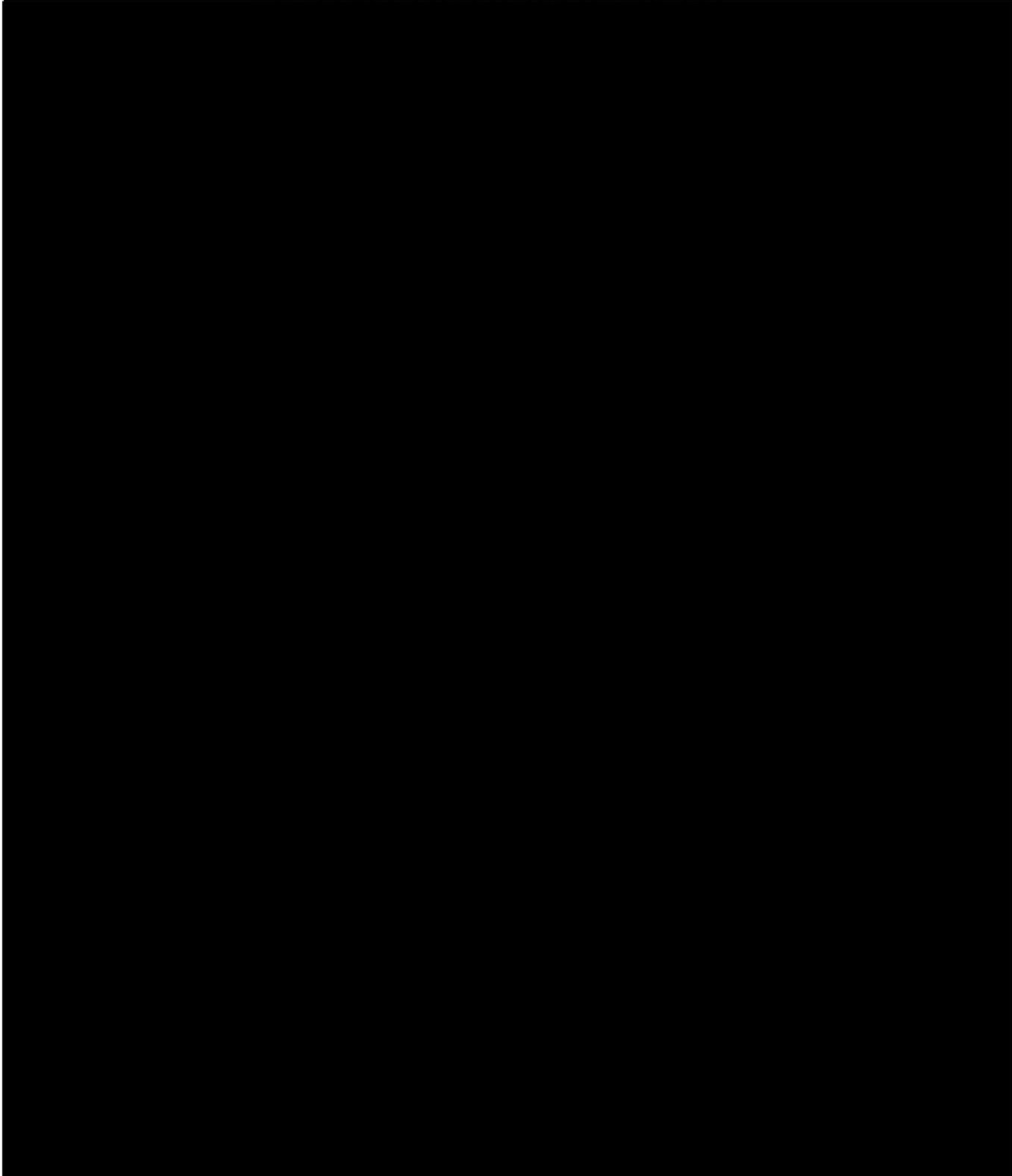
⁵³ See, e.g., TRW Inc. v. Andrews, 534 US. 19, 31 (2001) (“It is our duty to give effect, if possible, to every clause and word of a statute.”) (citation and internal quotations omitted); accord Duncan v. Walker, 533 U.S. 167, 174 (2001).

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

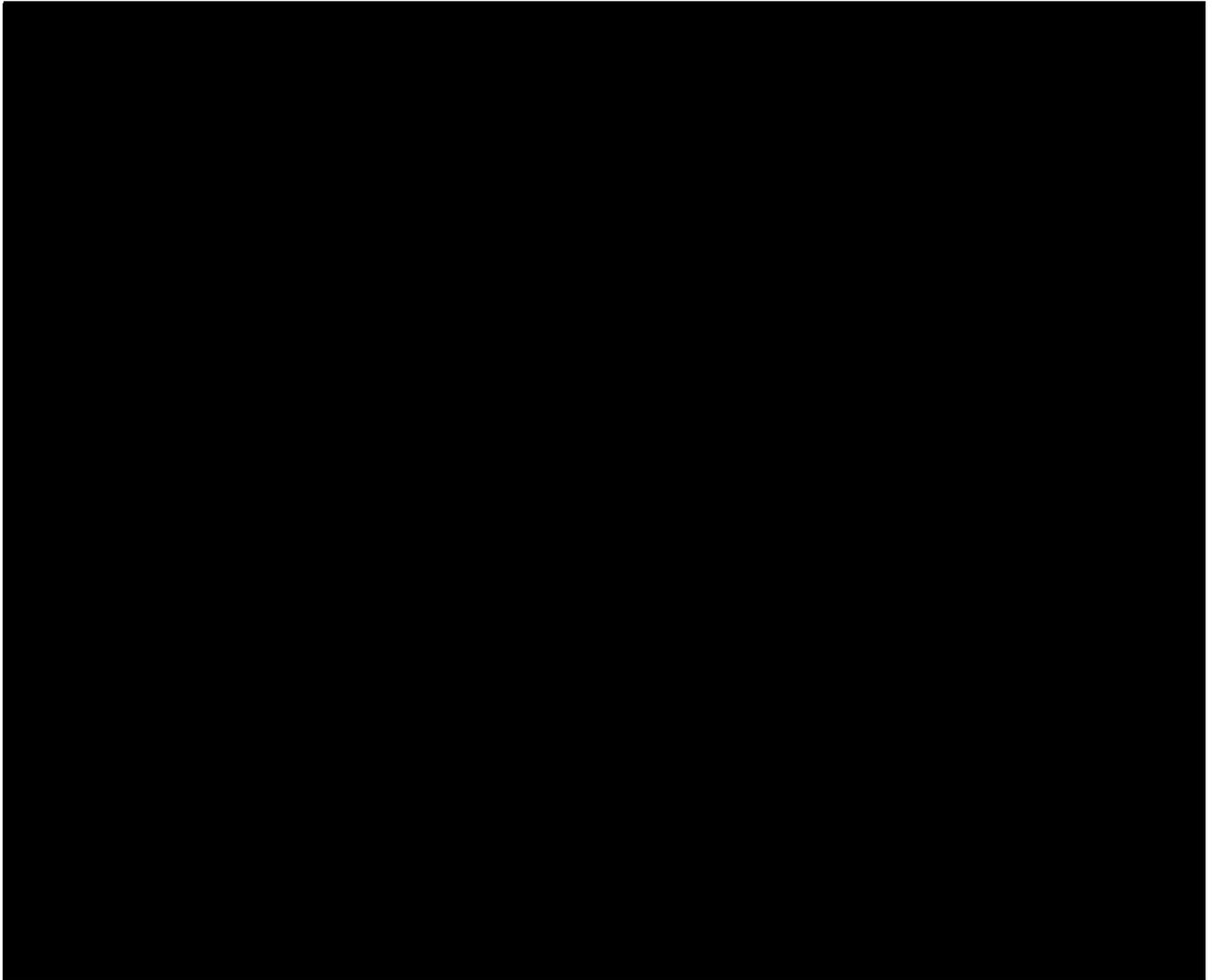


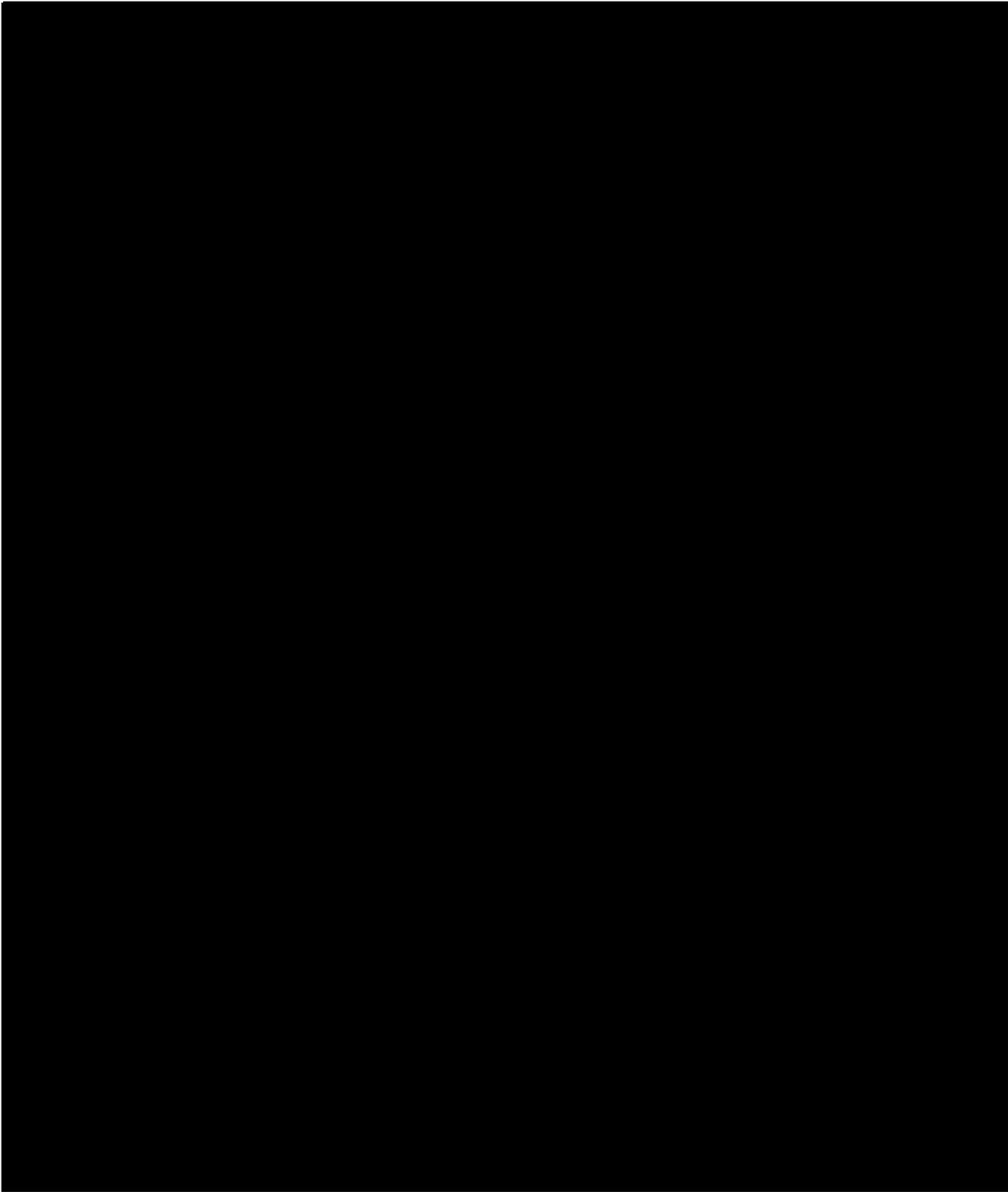
~~TOP SECRET//COMINT//ORCON,NOFORN~~

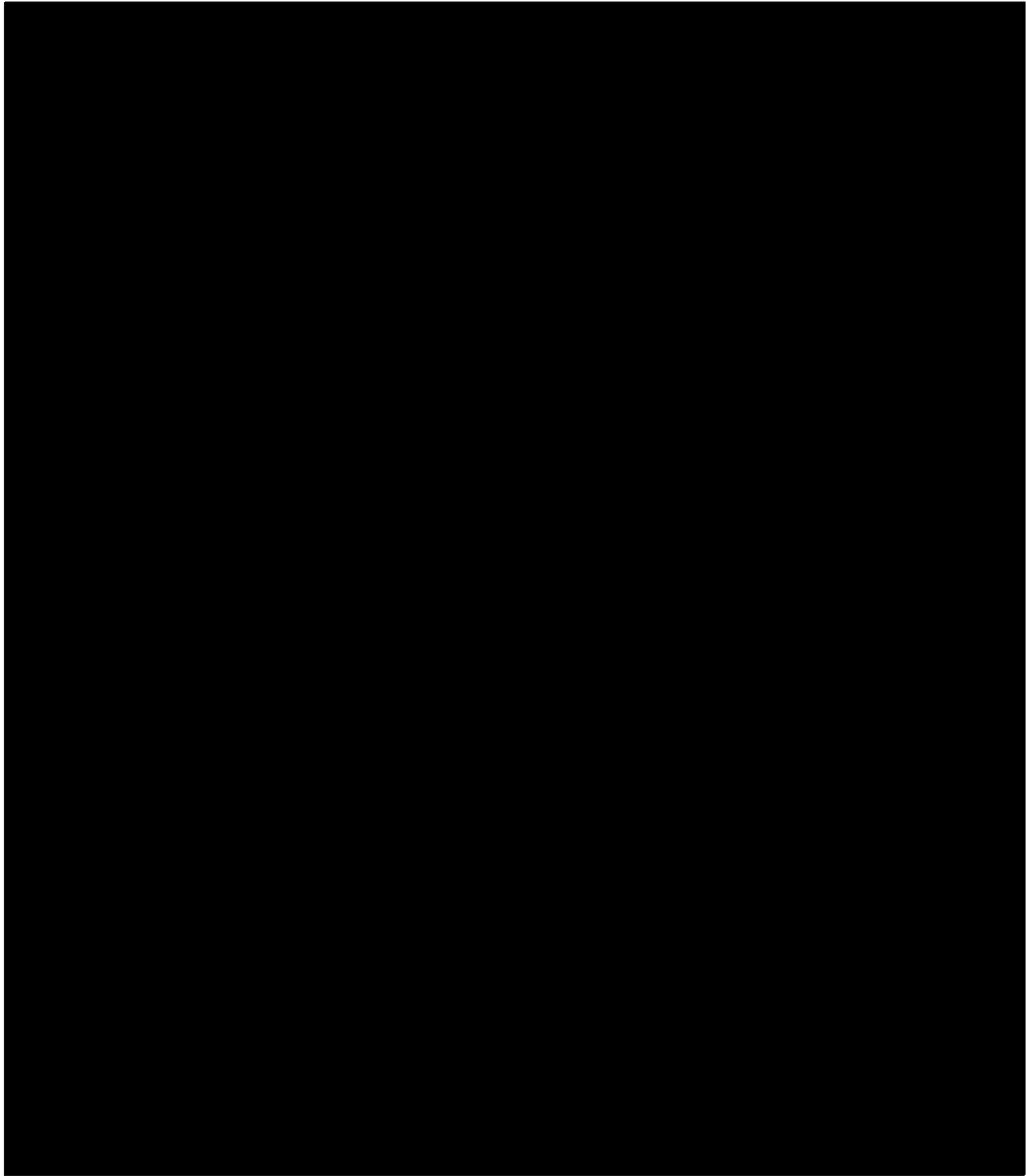
~~TOP SECRET//COMINT//ORCON,NOFORN~~



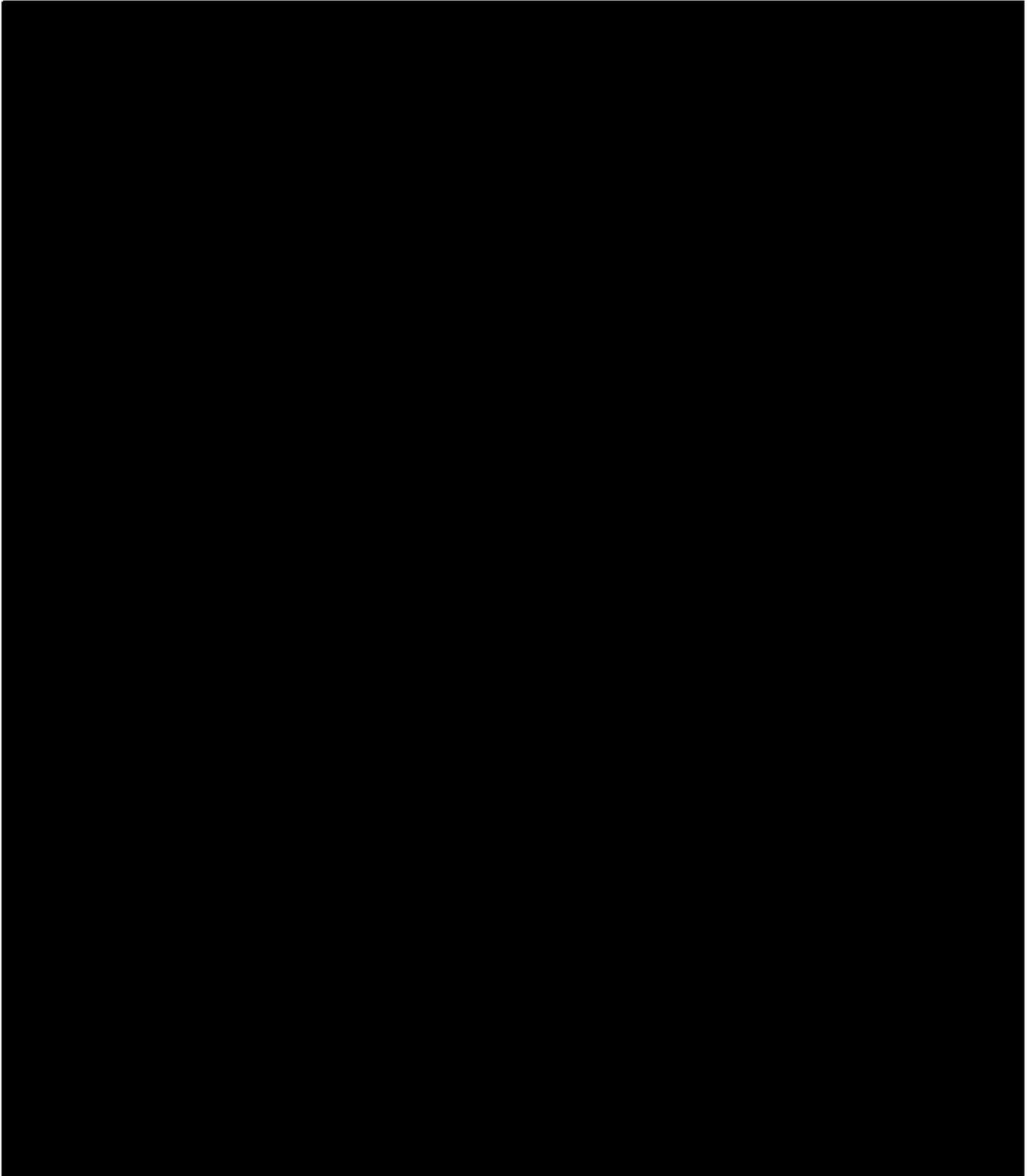
~~TOP SECRET//COMINT//ORCON,NOFORN~~



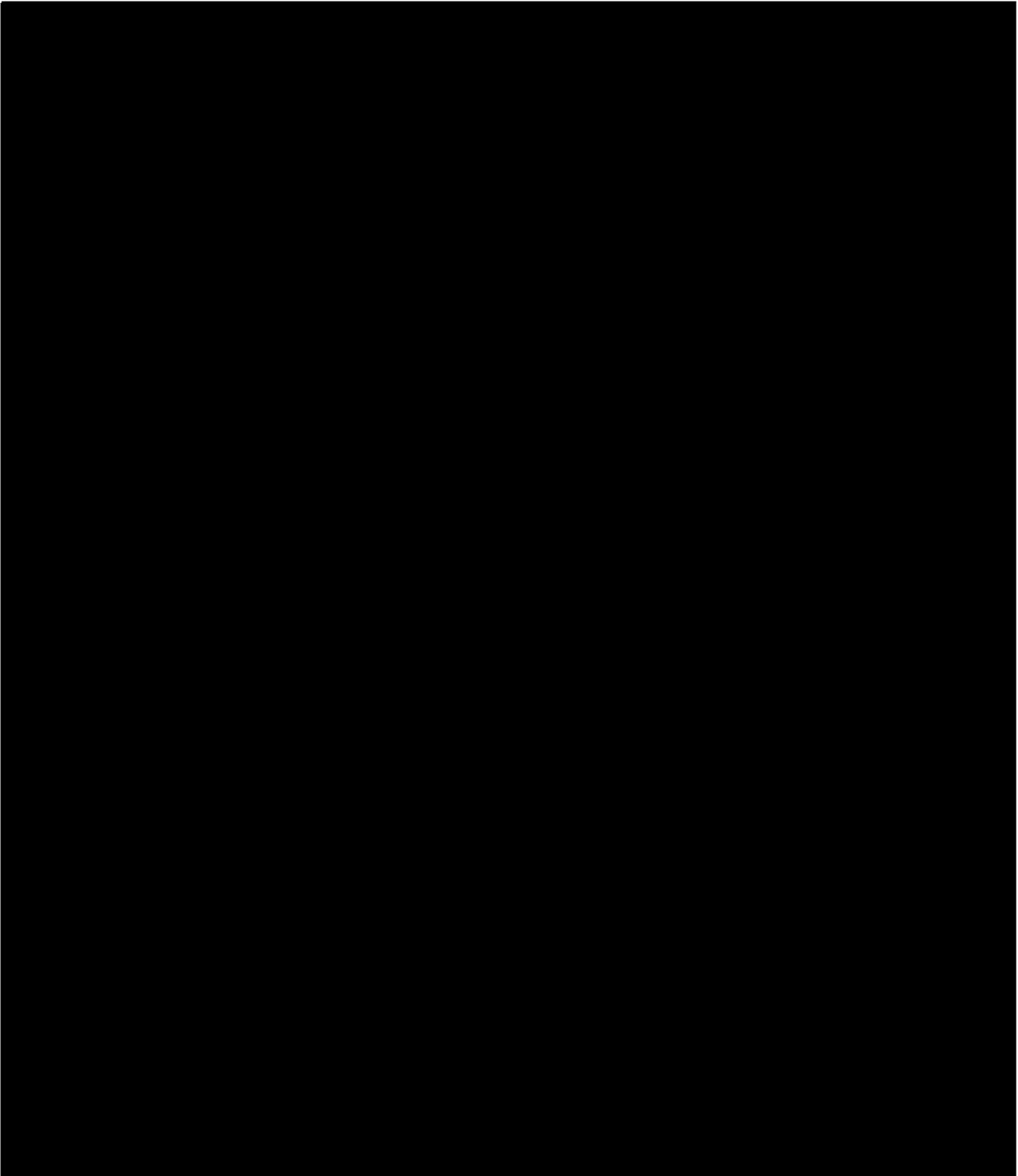




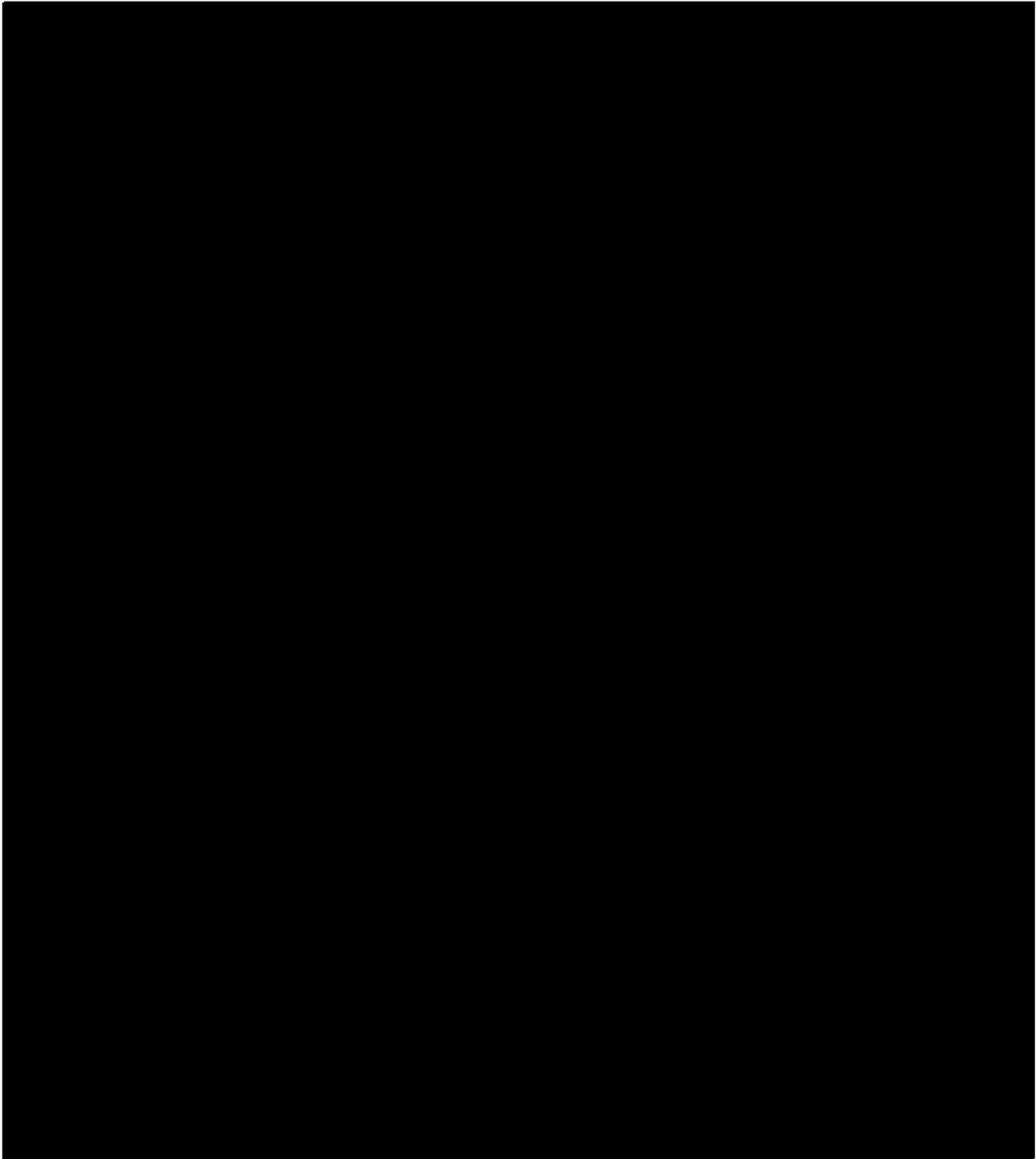
~~TOP SECRET//COMINT//ORCON,NOFORN~~



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



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



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

The foregoing analysis has involved difficult line-drawing. But the end-results correspond well with the evident legislative purpose of permitting the acquisition of DRAS information for e-mail [REDACTED] while avoiding the acquisition of the contents of electronic communications, [REDACTED]

[REDACTED]

[REDACTED] The Court believes that this approach is necessary to ensure that the authority sought by the government [REDACTED] is limited to non-content signaling information properly subject to collection by a PR/TT device. Given the challenges presented by this category of metadata, the Court's authorization will be limited to the [REDACTED] approved above. [REDACTED]

III. The Application Satisfies the Applicable Statutory Requirements

A. Request to Re-Initiate and Expand Collection

The current application, in comparison with prior dockets, seeks authority to acquire a much larger volume of metadata at a greatly expanded range of facilities,⁵⁶ while also modifying

[REDACTED]

– and in some ways relaxing – the rules governing the handling of metadata. In the foreseeable future, NSA does not expect to implement the full scope of the requested authorization because of processing limitations. [REDACTED] Response at 1. Even so, NSA projects the creation of [REDACTED] metadata records per day during the period of the requested order, compared with the norm under prior orders of approximately [REDACTED] records per day. Id. That is roughly an 11- to 24-fold increase in volume.

The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection. The government’s poor track record with bulk PR/TT acquisition, see pages 9-22, supra, presents threshold concerns about whether implementation will conform with, or exceed, what the government represents and the Court may approve. However, after reviewing the government’s submissions and engaging in thorough discussions with knowledgeable representatives, the Court believes that the government has now provided an accurate description of the functioning of the [REDACTED] [REDACTED] and the types of information they obtain. In addition, the Court is approving proposed modifications of the rules for NSA’s handling of acquired information only insofar as they do not detract from effective implementation of protections regarding U.S. person information.

B. Relevance

The current application includes a certification by the Attorney General “that the

[REDACTED]

information likely to be obtained from the pen registers and trap and trace devices requested in this Application . . . is relevant to ongoing investigations to protect against international terrorism that are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” [REDACTED] Application at 19. In its wording, this certification complies with the statute’s requirement of a certification of relevance.⁵⁷ As explained below, the Court also finds that there is an adequate basis for regarding the information to be acquired as relevant to the terrorist-affiliated Foreign Powers that are the subject of the investigations underlying the application. See note 9, supra.⁵⁸

As summarized above, the [REDACTED] Opinion’s finding of relevance most crucially depended on the conclusion that bulk collection is necessary for NSA to employ analytic tools that are likely to generate useful investigative leads to help identify and track terrorist operatives. See page 9, supra. However, in finding relevance, the [REDACTED] Opinion also relied on

⁵⁷ Under FISA, a PR/TT application requires

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 or clandestine intelligence activities, 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.

50 U.S.C. § 1842(c)(2).

⁵⁸ The government again argues that the Court should conduct no substantive review of the certification of relevance. See Memorandum of Law at 29. This opinion follows Judge Kollar-Kotelly’s [REDACTED] Opinion in assuming, without conclusively deciding, that substantive review is warranted. See note 10, supra.

NSA's efforts to acquire metadata that [REDACTED]

[REDACTED] See page 8, supra.⁵⁹ For purposes of assessing relevance, the primary difference between the current application and prior bulk PR/TT authorizations is that the current application encompasses a much larger volume of communications, without limiting the requested authorization to streams of data with a relatively high concentration of Foreign Power communications.⁶⁰

There is precedent, however, for concluding that a wholly non-targeted bulk production of metadata under Section 1861 can be relevant to international terrorism investigations. In those cases, the FISC has found that the ongoing production by major telephone service providers of call detail records for all domestic, United States-to-foreign, and foreign-to-United States calls, in order to facilitate comparable forms of NSA analysis and with similar restrictions on handling and dissemination, is relevant to investigations of the Foreign Powers. See, e.g., Docket No. [REDACTED]

⁵⁹ As part of the relevance analysis, the [REDACTED] Opinion also relied on the presence of "safeguards" governing the handling and dissemination of the bulk metadata and information derived from it. The safeguards proposed in the current application are discussed below, and, as modified, the Court finds them to be adequate. See Part IV, infra.

⁶⁰ The current application also seeks to expand the categories of metadata to be acquired for each communication. The Court is satisfied that the categories of metadata described in the current application constitute directly relevant information, insofar as they relate to communications of a Foreign Power. See, e.g., [REDACTED] Alexander Decl. at 19-22. The metadata for other communications is relevant to the investigations of the Foreign Powers for the reasons discussed herein.

██████████ Primary Order issued on ██████████, at 2-19.⁶¹

The current application similarly supports a finding of relevance for this non-targeted form of bulk acquisition of Internet metadata because it “will substantially increase NSA’s ability to detect and identify the Foreign Powers and those individuals affiliated with them.” ██████████

██████████ Alexander Decl. at 18. There is credible testimony that terrorists affiliated with the Foreign Powers attempt to conceal operational communications by ██████████

██████████ See *id.* at 9, 11. Terrorist efforts to evade surveillance, in combination with the inability to know the full range of ongoing terrorist activity at a given time, make it “impossible to determine in advance what metadata will turn out to be valuable in tracking, identifying, characterizing and exploiting a terrorist.” *Id.* at 17-18. Analysts know that terrorists’ communications are traversing Internet facilities within the United States, but “they cannot know ahead of time . . . exactly where.” *Id.* at 18. And, if not captured at the time of transmission, Internet metadata may be “lost forever.” *Id.* For these reasons, bulk collection of metadata is necessary to enable retrospective analysis, which can uncover new terrorists, as well

⁶¹ The current application further resembles the bulk productions of metadata under Section 1861 in that it proposes to capture metadata for a larger volume of U.S. person communications. See ██████████ Response at 3. The Court is satisfied that the increase in U.S. person communications does not undermine the basis for relevance, particularly in view of the specific safeguards for accessing and disseminating U.S. person information.

as e-mail accounts used by known terrorists that otherwise would be missed. Id. at 21-22.⁶²

As the [REDACTED] Opinion recognizes, the relevance standard does not require “a statistical ‘tight fit’ between the volume of proposed collection and the much smaller proportion of information” that pertains directly to a Foreign Power. [REDACTED] Opinion at 49-50. Nor, in the Court’s view, does the relevance standard necessarily require a PR/TT authorization to limit collection to [REDACTED]

of Foreign Power communications. The circumstances that make bulk metadata relevant include

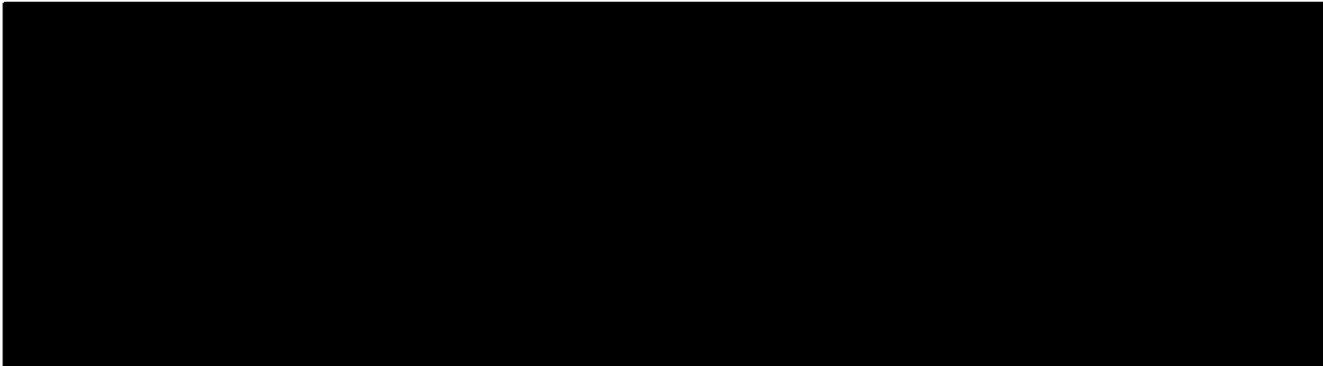
[REDACTED]

[REDACTED] Alexander Decl. at 18. It follows that some Foreign Power communications [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



C. Specifications of the Order

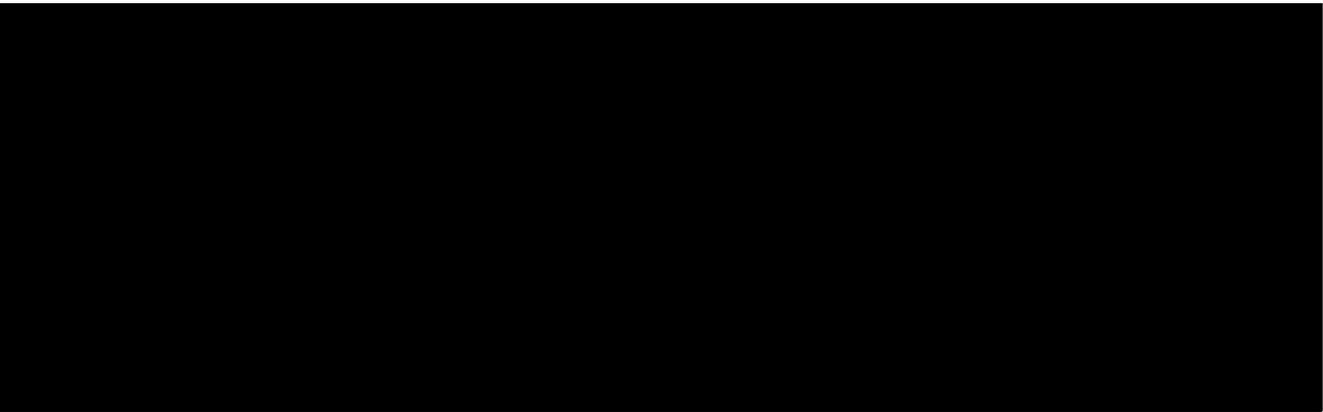
Section 1842(d)(2)(A) requires a PR/TT order to

specify—

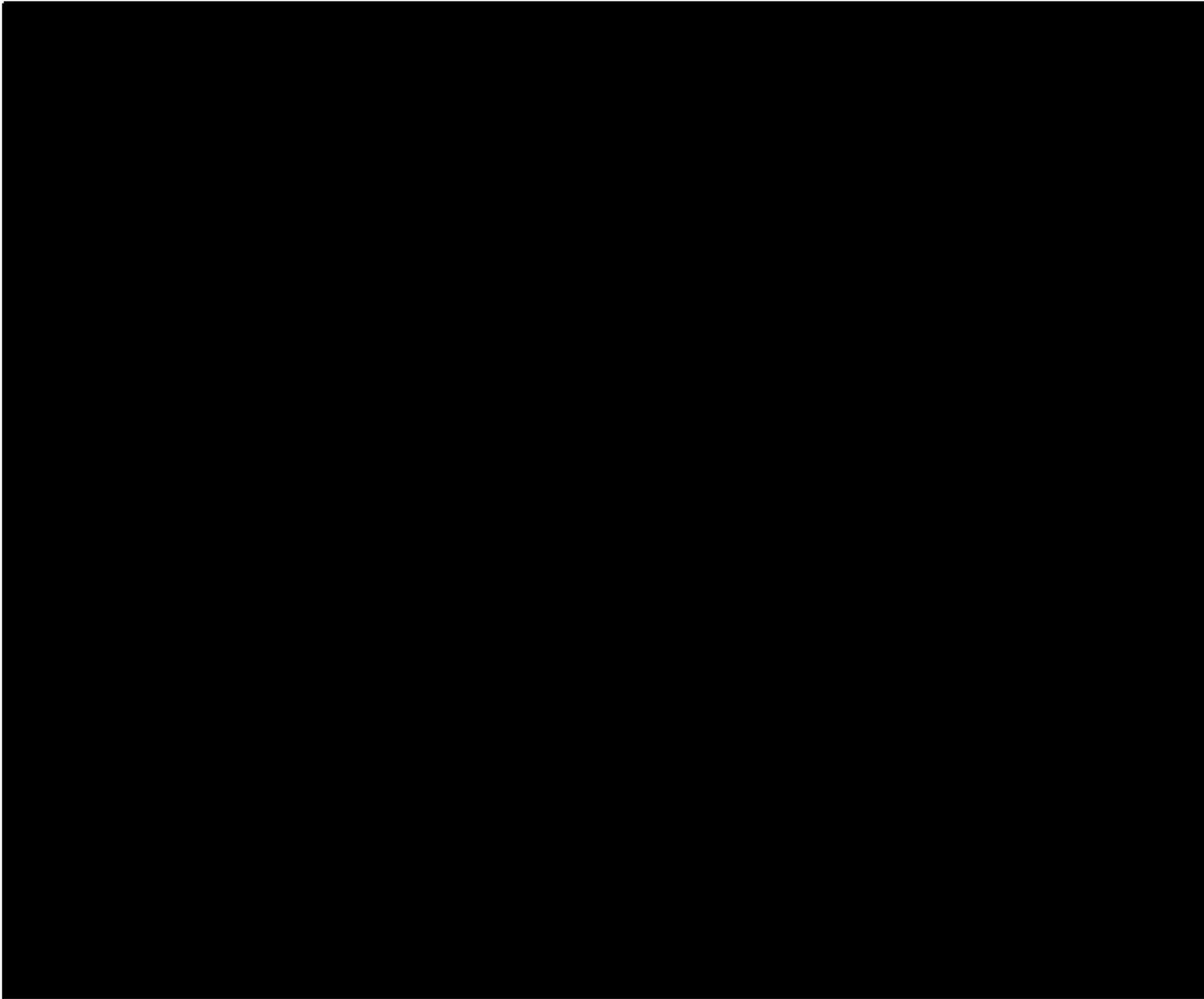
(i) the identity, if known, of the person who is the subject of the investigation;

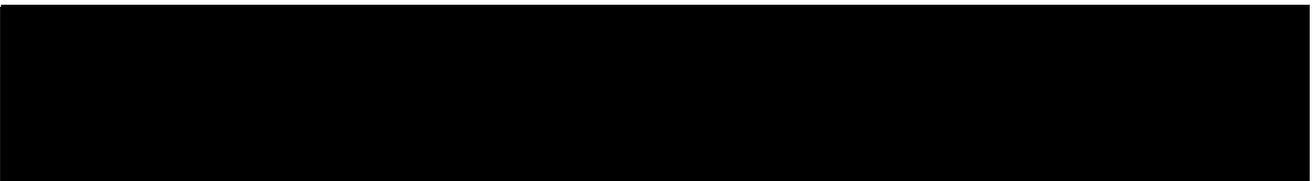
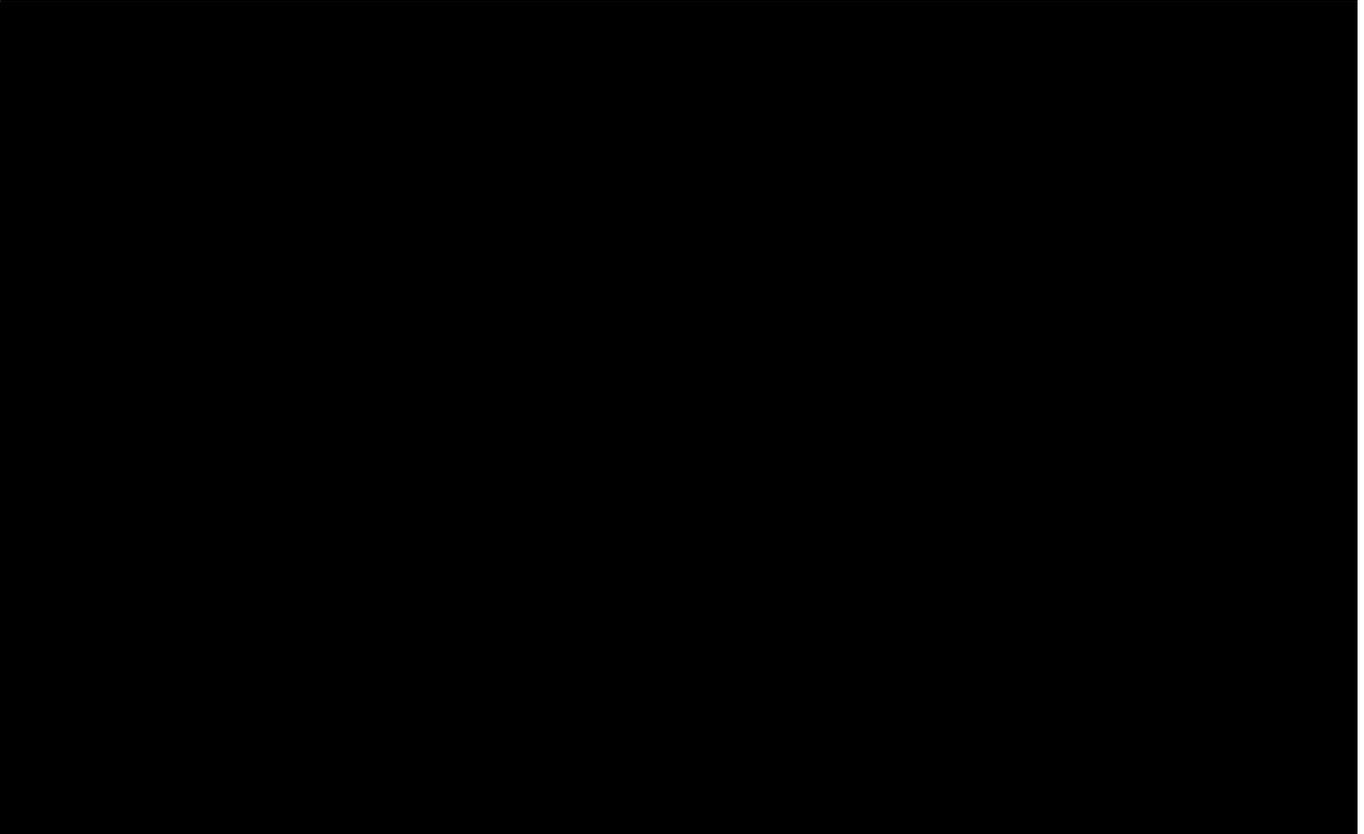
(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and

(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.^[65]

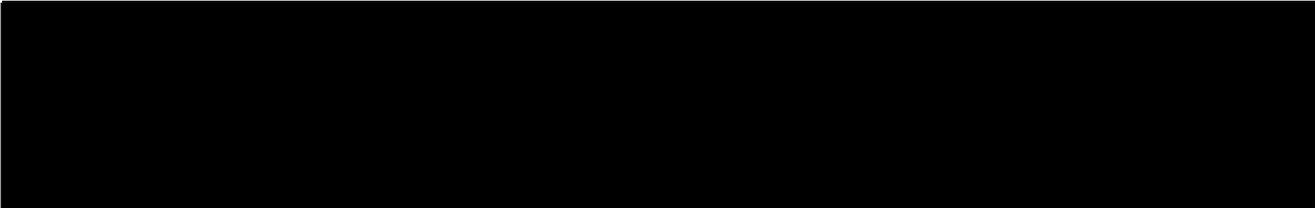
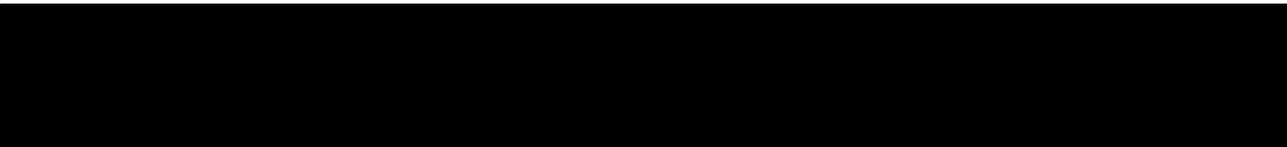


In this case, the subjects of the relevant investigations are sufficiently identified, to the extent known, as the enumerated Foreign Powers “and unknown persons in the United States and abroad affiliated with the Foreign Powers.” [REDACTED] Primary Order at 2-3.





⁶⁷ See, e.g., Docket No. PR/TT [redacted] Application at 26 n.15, Primary Order issued on [redacted] at 3 [redacted]



At this pre-collection stage, it is uncertain to which facilities PR/TT devices will be attached or applied during the pendency of the initial order. See pages 76-77, supra; [REDACTED] [REDACTED] Response at 1-2. For this reason, and because the Court is satisfied that other specifications in the order will adequately demarcate the scope of authorized collection, the Court will issue an order that does not identify persons pursuant to Section 1842(d)(2)(A)(ii). However, once this surveillance is implemented, the government's state of knowledge may well change. Accordingly, the Court expects the government in any future application to identify persons (as described in Section 1842(d)(2)(A)(ii)) who are known to the government for any facility that the government knows will be subjected to PR/TT surveillance during the period covered by the requested order.

Section 1842(d)(2)(A)(iii) requires the order to specify "the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." The order specifies the location of each facility. The Court is also satisfied that "the attributes of the communications to which the order applies" are

appropriately specified. Acquisition of particular forms of metadata (described in Part II, supra) is authorized for all e-mail [REDACTED] communications traversing any of the communications facilities at the specified locations. This form of specification is consistent with the language of Section 1842(d)(2)(A)(iii) and is sufficient to delineate the scope of authorized acquisition from that which is not authorized.⁶⁸

IV. The Court Approves, Subject to Modifications, the Restrictions and Procedures Proposed by the Government For the Retention, Use, and Dissemination of the PR/TTMetadata

Unlike other provisions of FISA, the PR/TT provisions of the statute do not expressly require the adoption and use of minimization procedures. Compare 50 U.S.C. §§ 1805(c)(2)(A) & 1824(c)(2)(A) (providing that orders authorizing electronic surveillance or physical search must direct that minimization procedures be followed). Accordingly, routine FISA PR/TT orders do not require that minimization procedures be followed. The government acknowledges, however, that the application now before the Court is not routine. As discussed above, the government seeks to acquire information concerning [REDACTED] electronic communications, the vast majority of which, viewed individually, are not relevant to the counterterrorism purpose of the collection, and many of which involve United States persons. In light of the sweeping and non-targeted nature of the collection for which authority is sought, the government proposes a

number of restrictions on retention, use, and dissemination, some of which the government refers to as “minimization” procedures. See, e.g., Memorandum of Law at 4, 17. The restrictions now proposed by the government are similar, but not identical, to the rules that were adopted by the Court in its [REDACTED] Order in Docket Number PR/TT [REDACTED] Order”), the most recent order authorizing bulk PR/TT collection by NSA.

Absent any suggestion by the government that a different standard should apply, the Court is guided in assessing the proposed restrictions by the definition of minimization procedures in 50 U.S.C. § 1801(h).⁶⁹ Because procedures satisfying that definition are sufficient

⁶⁹ Section 1801(h) defines “minimization procedures” in pertinent part as follows:

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

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s identity is necessary to understand foreign intelligence information or assess its importance; [and]

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]

. . .

50 U.S.C. § 1801(h).

under FISA to protect the privacy interests of United States persons with respect to the acquisition, use, and dissemination of the contents of communications, restrictions meeting the same standard are also at least adequate in the context of the collection and use of non-content metadata. Guided by the Section 1801(h) standard, the Court concludes, for the reasons stated below, that the procedures proposed by the government, subject to the modifications described below, are reasonably designed in light of the nature and purpose of the bulk PR/TT collection to protect United States person information, and to ensure that the information acquired is used and disseminated in furtherance of the counterterrorism purpose of the collection.

A. Storage and Traceability

NSA will continue to store the PR/TT data that it retains in repositories within secure networks under NSA's control. [REDACTED] Alexander Decl. at 24. As was the case under the [REDACTED] Order, the data collected pursuant to the authority now sought by the government will carry unique markings that render it distinguishable from information collected by NSA pursuant to other authorities. [REDACTED] Response at 15; see also Declaration of [REDACTED] NSA, filed on [REDACTED] in Docket No. PR/TT [REDACTED] ([REDACTED] Decl.") at 14 n.8. The markings, which are applied to the data before it is made available for analytic querying and remain attached to the information as it is stored in metadata repositories, see [REDACTED] Response at 15, are designed to ensure that software and other controls (such as user authentication tools) can restrict access to the PR/TT data solely to authorized personnel who have received appropriate training regarding the special rules for using

and disseminating such information. See [REDACTED] Alexander Decl. at 24-25; [REDACTED] Decl. at 14 n.8. After PR/TT metadata is queried in accordance with the procedures described below, the query results (including analytic output based on query results)⁷⁰ will remain identifiable as bulk PR/TT-derived information. See [REDACTED] Response at 15. Such traceability enables NSA personnel to adhere to the special rules for disseminating PR/TT-derived information that are described below.

B. Access to the Metadata by Technical Personnel for Non-Analytic Purposes

Under the approach proposed by the government, “[t]rained and authorized technical personnel” will be permitted to access the metadata to ensure that it is “usable for intelligence analysis.” *Id.* at 25. For example, such personnel may access the metadata to perform processes designed to prevent the collection, processing, or analysis of metadata associated with [REDACTED] [REDACTED] to create and maintain records necessary to demonstrate compliance with the terms of authority granted; or to develop and test technologies for possible use with the metadata. *Id.*⁷¹ Similar non-analytic

⁷⁰ The government has explained that “[q]query results could include information provided orally or in writing, and could include a tip or a lead (e.g., ‘A query on RAS-approved identifier A revealed a direct contact with identifier Z’), a written or electronic depiction of a chain or pattern, a compilation or summary of direct or indirect contacts of a RAS-approved seed, a draft or finished report, or any other information that would be returned following a properly predicated PR/TT query.” [REDACTED] Response at 15 n.6.

⁷¹ An authorized NSA technician may query the metadata with a non-RAS-approved identifier for the limited purpose of determining whether such identifier is an unwanted [REDACTED] [REDACTED] Alexander Decl. at 25. After recognizing a [REDACTED]

(continued...)

access by appropriately trained and authorized technical personnel was permitted under the

██████████ Order. See ██████████ Order at 10.

C. Access by Analysts

NSA analysts will query the metadata that is collected only with RAS-approved “seed” identifiers, in accordance with the same basic framework that was approved by the Court in the ██████████ Order. See ██████████ Alexander Decl. at 26-27; ██████████ Order at 7-9.

An identifier may be approved for use as a querying seed in one of two ways. First, an identifier may be used as a seed after a designated “approving official” (i.e., the Chief or Deputy Chief of NSA’s Homeland Analysis Center, or one of 20 authorized Homeland Mission Coordinators⁷²) determines that the available facts give rise to a reasonable articulable suspicion that the identifier is associated with one of the targeted Foreign Powers. ██████████ Alexander Decl. at 26-27. Before querying can be performed using an identifier that is reasonably believed to be used by a United States person, NSA’s Office of General Counsel (OGC) must determine that the identifier is not regarded as associated with a Foreign Power solely based on activities that are

⁷¹(...continued)

██████████ through such a query, the NSA technician could share the query results – i.e., the identifier and the fact that it is a ██████████ – with other NSA personnel responsible for the removal of unwanted metadata from NSA’s repositories, but would not be permitted to share any other information from the query. *Id.* at 25-26.

⁷² The ██████████ Order identified one approving official in addition to the 22 officials listed here. See ██████████ Order at 8 (listing the Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate as one of the 23 approving officials).

protected by the First Amendment. Id. at 27. Second, an identifier that is the subject of electronic surveillance or physical search pursuant to 50 U.S.C. § 1805 or § 1824 based on this Court's finding of probable cause that such identifier is used by an agent of a Foreign Power may be deemed RAS-approved without review by an NSA designated approving official. Id.

As was the case under the Court's [REDACTED] Order and prior orders in this matter, RAS-approved queries of the collected data will take the form of "contact chaining." Id. at 18. Such queries yield data for all communications within two "hops" of the RAS-approved seed. Id. The first hop acquires data regarding all identifiers that have been in contact with the seed, and the second hop yields data for all identifiers in contact with identifiers that were revealed by the first hop. Id. at 18 n.12. The government asserts, and the Court has previously accepted, that "[g]oing out to the second 'hop' enhances NSA's ability to find, detect and identify the Foreign Powers and those affiliated with them by greatly increasing the chances that previously unknown Foreign Power-associated identifiers may be uncovered." Id. at 18-19 n.12; [REDACTED] Opinion and Order at 48.⁷³

⁷³ NSA also intends to perform [REDACTED]

[REDACTED] The government has clarified in connection with this application, however, that [REDACTED] is not used as a means for querying the metadata, but instead is applied only to the results of RAS-approved contact-chaining queries. See [REDACTED] [REDACTED] Response at 16.

The government's proposed RAS-approval and querying process differs in two noteworthy respects from the approach previously approved by the Court. First, unlike RAS approvals made pursuant to the ██████████ Order and prior orders in this matter,⁷⁴ RAS approvals made under the approach now proposed by the government will expire after a specified time. A determination by a designated approving official for an identifier reasonably believed to be used by a United States person would be effective for 180 days, while such a determination for any other identifier would last for one year. ██████████ Alexander Decl. at 27. An identifier deemed approved based on FISC-authorized electronic surveillance or physical search will be subject to use as a seed for the duration of the FISC authorization. *Id.* The adoption of fixed durations for RAS approvals will require the government at regular intervals to renew its RAS assessments for identifiers that it wishes to continue to use as querying "seeds." The re-evaluations that will be required under the proposed approach can be expected to increase the likelihood that query results are relevant to the counterterrorism purpose of the bulk metadata collection and to reduce the amount of irrelevant query results (including information regarding

⁷⁴ Previously, approved identifiers remained eligible for querying until they were affirmatively removed from the list of approved "seed" accounts. The government's practice was to remove identifiers from the list only "[w]hen NSA receive[d] information that suggest[ed] that a RAS-approved e-mail address [was] no longer associated with one of the Foreign Powers"; implicitly, the mere passage of time without new information did not obligate the government to revoke a RAS approval. *See* Docket No. PR/TT ██████████ NSA 90-Day Report to the Foreign Intelligence Surveillance Court filed on ██████████ at 6. The government had informed the Court on ██████████ that it was "developing a framework within which to revalidate, and when appropriate, reverse . . . RAS approvals," *id.* at 6, but it does not appear that the new framework had been implemented before the expiration of the Court's ██████████ Order on ██████████.

United States persons) that is yielded.

The second proposed change to the process involves the number of NSA personnel permitted to perform RAS-approved queries. Unlike the ██████████ Order and prior orders in this matter, which limited the number of analysts permitted to run such queries, the re-initiation proposed by the government has no such limitation. See Id. at 26 n.18; ██████████ Order at 7. The government instead proposes the use of “technical controls” to “block any analytic query of the metadata with a non-RAS-approved seed.” ██████████ Alexander Decl. at 26 n.18. The government further notes that all analytic queries will continue to be logged, and that the creation and maintenance of auditable records will “continue to serve as a compliance measure.” Id.; see also ██████████ Order at 7. In light of the safeguards noted by the government, and the additional fact that no identifier will be eligible for use as a querying seed without having first been approved for querying by a designated approving official (or deemed approved by virtue of a FISC order), the Court is satisfied that it is unnecessary to limit the number of NSA analysts eligible to conduct RAS-approved queries.

D. Sharing of Query Results Within NSA

The government’s proposal for sharing query results within NSA is similar to the approach approved by the Court last year. The ██████████ Order provided, subject to a proviso that is discussed below, that the unminimized results of RAS-approved queries could be “shared with other NSA personnel, including those who are not authorized to access the PR/TT metadata.” ██████████ Order at 11. The basis for such widespread sharing of query results

within NSA was the government's assertion that analysts throughout the agency address counterterrorism issues as part of their missions and, therefore, have a need for the information.⁷⁵ Presumably for the same reason, the government proposes in the application now before the Court that the results of RAS-approved queries be available to all NSA analysts for intelligence purposes, and that such analysts be allowed to apply "the full range of SIGINT analytical tradecraft" to the query results. [REDACTED] Alexander Decl. at 28 n.19.⁷⁶ The Court is satisfied

⁷⁵ In a declaration filed in Docket Number PR/TT [REDACTED] late last year, the Director of NSA explained that:

NSA's collective expertise in the [] Foreign Powers resides in more than [REDACTED] intelligence analysts, who sit, not only in the NSA's Counterterrorism Analytic Enterprise, but also in other NSA organizations or product lines. Analysts from other product lines also address counterterrorism issues specific to their analytic missions and expertise. For example, the International Security Issues product line pursues foreign intelligence information on [REDACTED] including [REDACTED]. [REDACTED] The mission of the Combating Proliferation product line includes identifying connections between proliferators of weapons of mass destruction and terrorists, including those associated with the Foreign Powers. The International Crime and Narcotics product line identifies connections between terrorism and human or nuclear smuggling or other forms of international crime. . . . Each of the NSA's ten product lines has some role in protecting the Homeland from terrorists, including the Foreign Powers. Because so many analysts touch upon terrorism information, it is impossible to estimate how many analysts might be served by access to the PR/TT results.

[REDACTED] Report, Exhibit A at 5-6.

⁷⁶ The [REDACTED] Order did not explicitly authorize NSA analysts to apply the "full range of SIGINT tools" to PR/TT query results, but, at the same time it placed no limit on the analytical tools or techniques that could be applied by the trained analysts who were entitled to have access to query results. Accordingly, the Court views the express reference to "the full range of analytic tools" in the government's proposal as a clarification of prior practice that the Court, in any event, approves.

that such internal sharing remains appropriate, subject to the training requirement that is discussed below.

E. Dissemination Outside NSA

The government's proposed rules for disseminating PR/TT-derived information outside of NSA are slightly different from the procedures that were previously in place. Under the [REDACTED] Order, NSA was required to "treat information from queries of the PR/TT metadata in accordance with United States Signals Intelligence Directive 18 (USSID 18)" – NSA's standard procedures for handling Signals Intelligence collection – and to "apply USSID 18 to minimize information concerning U.S. persons obtained from the pen registers and trap and trace devices authorized herein." [REDACTED] Order at 12. In addition,

before NSA disseminate[d] any U.S. person identifying information outside of NSA, the Chief of Information Sharing Services in the Signals Intelligence Directorate, the Senior Operations Officer at NSA's National Security Operations Center, the Signals Intelligence Directorate Director, the Deputy Director of NSA, or the Director of NSA [was required to] determine that the information identifying the U.S. person [was] in fact related to counterterrorism information and that it [was] necessary to understand the counterterrorism information or assess its importance.

Id.

The government's proposal has the same two basic elements, although they are worded slightly differently. First, NSA "will apply the minimization and dissemination procedures of Section 7 of [USSID 18] to any results from queries of the metadata disseminated outside of NSA in any form." [REDACTED] Alexander Decl. at 28. Second,

prior to disseminating any U.S. person information outside NSA, one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of NSA, the Deputy Director of

NSA, the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operation 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.

Id.

The differences are not material. Although the proposal refers specifically to “the minimization and dissemination procedures of Section 7 of [USSID 18]” rather than to USSID 18 generally, the Court does not understand any difference in meaning to be intended; indeed, Section 7 is the portion of USSID 18 that specifically covers disseminations outside NSA. See [REDACTED] Application, Tab C (USSID 18), at 8-10. With regard to the application of the counterterrorism purpose requirement, the proposal adds two high-ranking NSA officials (the Deputy Director of the SID and the Deputy Chief of the ISS office) to the list of five officials who were previously designated to make the required determination. The Court is aware of no reason to think that the two additional officials are less suited than the other five to make the required determination, or that their designation as approving officials will undermine the internal check that is provided by having high-ranking NSA officials approve disseminations that include United States person identifying information.⁷⁷

⁷⁷ Like the [REDACTED] Order, the government’s proposal would also permit NSA to “share results derived from intelligence analysis queries of the metadata, including U.S. person identifying information, with Executive Branch personnel . . . in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings.” [REDACTED] Alexander Decl. 28-29; see also [REDACTED]

(continued...)

The government's proposal contains one additional element that was not part of the framework approved by the Court in the [REDACTED] Order. Specifically, the government proposes that "[i]n the extraordinary event that NSA determines that there is a need to disseminate information identifying a U.S. person that is related to foreign intelligence information, as defined by 50 U.S.C. § 1801(e), other than counterterrorism information and that is necessary to understand the foreign intelligence information or assess its importance, the Government will seek prior approval from the Court." [REDACTED] Alexander Decl. at 28 n.20. Insofar as the government's proposal invites the Court to review and pre-approve individual disseminations of information based upon the Court's own assessments of foreign intelligence value, the Court declines the invitation. The judiciary is ill-equipped to make such assessments, which involve matters on which the courts generally defer to the Executive Branch.⁷⁸ In the

⁷⁷(...continued)

[REDACTED] Order at 12-13. The government's current proposal also permits such sharing with Executive Branch personnel "to facilitate their lawful oversight functions." [REDACTED] Alexander Decl. at 29. Although the [REDACTED] order did not contain an explicit provision to this effect, sharing for such purposes was plainly contemplated. *See, e.g.,* [REDACTED] Order at 16 (providing for NSD review of RAS querying justifications).

⁷⁸ *See, e.g., Holder v. Humanitarian Law Project*, — U.S. —, 2010 WL 2471055, *22 (June 21, 2010) ("[W]hen it comes to collecting evidence and drawing factual inferences in [the national security] area, the lack of competence on the part of the courts is marked.") (citation and internal quotation marks omitted); *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 challenge).

event, however, that NSA encounters circumstances that it believes necessitate alteration of the dissemination procedures that have been approved by the Court, the government may obtain prospectively-applicable modifications to those requirements upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the sweeping and non-targeted nature of the PR/TT collection. Cf. Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search § I.D (on file with the Court in Docket No. 08-1833).

F. Retention

Under the ██████████ Order, the PR/TT metadata was available for querying for four and one-half years, after which it had to be destroyed. ██████████ Order at 13. The four-and-one-half-year retention period was originally set based upon NSA's assessment of how long collected metadata is likely to have operational value. See ██████████ Opinion at 70-71. Pursuant to the government's proposal, the retention period would be extended to five years. ██████████ Application at 13. The government asserts that the purpose of the change is to "develop and maintain consistency" with the retention period for NSA's bulk telephony metadata collection, which is authorized by this Court under the FISA business records provision, 50 U.S.C. § 1861. ██████████ Response at 24. The Court is satisfied that the relatively small extension of the retention period that is sought by the government is justified by the administrative benefits that would result.

G. Oversight

The government proposes to employ an internal oversight regime that closely tracks the oversight provisions adopted by the Court in the ██████████ Order, requiring, among other things, that NSA OGC and NSD take various steps to ensure that the data is collected and handled in accordance with the scope of the authorization. Compare ██████████ Order at 13-16, with ██████████ Alexander Decl. at 29-30. There is, however, one significant difference. The ██████████ Order required NSA OGC to ensure that all NSA personnel permitted to access the metadata or receive query results were first “provided the appropriate and adequate training and guidance regarding the procedures and restrictions for storage, access, and dissemination of the PR/TT metadata and/or PR/TT metadata-derived information, i.e., query results.” ██████████ Order at 13-14. The analogous oversight provision in the government’s current proposal, by contrast, directs NSA OGC and the Office of the Director of Oversight and Compliance (ODOC) to ensure that adequate training and guidance is provided to NSA personnel having access to the metadata, but not to those receiving query results. See ██████████ Alexander Decl. at 29. As discussed above, the government has proposed special rules and restrictions on the handling and dissemination of query results. Most notably, PR/TT query results must remain identifiable as bulk PR/TT-derived information, see ██████████ Response at 15, and may not be disseminated outside NSA without the prior determination by a designated official that any United States person information relates to counterterrorism information and that it is necessary to understand the counterterrorism information or to assess its importance. ██████████

████████ Alexander Decl. at 28. To follow those rules, NSA personnel must know and understand them.

As noted above, NSA's record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained. See pages 18-19, supra. The government has provided no meaningful explanation why these violations occurred, but it seems likely that widespread ignorance of the rules was a contributing factor.

Accordingly, the Court will order NSA OGC and ODOC to ensure that all NSA personnel who receive PR/TT 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.

H. Reporting

The reporting requirements proposed by the government are similar to the reporting requirements adopted by the Court in the ██████████ Order. Compare ██████████ Alexander Decl. at 31, with ██████████ Order at 16-18. As was previously the case, the government will submit reports to the Court approximately every 30 days and upon requesting any renewal of the authority sought. See ██████████ Alexander Dec. at 31. The 30-day reports will include "a discussion of the queries made since the last report and NSA's application of the RAS standard." Id. Because NSA will not apply the requested authority to particular

however, the 30-day reports will no longer include a discussion of “changes in the description of the . . . or in the nature of the communications carried thereon.” See Order at 16. Like the Order, the government’s proposal will also require it, upon seeking renewal of the requested authority, to file a report describing “any new facility proposed to be added” and “any changes proposed in the collection methods.” Alexander Decl. at 31.

The Order also directed the government to submit weekly reports listing each instance in which “NSA has shared, in any form, information obtained or derived from the PR/TT metadata with anyone outside NSA,” including a certification that the requirements for disseminating United States person information (*i.e.*, that a designated official had determined that any such information related to counterterrorism information and was necessary to understand counterterrorism information or to assess its importance) had been followed. See Order at 17. The government’s proposal does not include such a requirement. In light of NSA’s historical problems complying with the requirements for disseminating PR/TT-derived information, the Court is not prepared to eliminate this reporting requirement altogether. At the same time, the Court does not believe that weekly reports are still necessary to ensure compliance. Accordingly, the Court will order that the 30-day reports described in the preceding paragraph include a statement of the number of instances since the preceding report in which NSA has shared, in any form, information obtained or derived from the PR/TT metadata with anyone outside NSA. For each such instance in which United States person information has been

shared, the report must also 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 the counterterrorism information or to assess its importance.

V. The Government's Request for Authority to Access and Use All Previously Collected Data

The government seeks authority to access and use all previously acquired bulk PR/TT data, including information not authorized for collection under the Court's prior orders, subject to the same restrictions and procedures that will apply to newly-acquired PR/TT collection. See [REDACTED] Application at 16. For the following reasons, the Court will grant the government's request in part and deny it in part.

A. The [REDACTED] Order

As discussed above, after the government disclosed the continuous and widespread collection of data exceeding the scope of the Court's prior orders dating back to [REDACTED] it elected not to seek renewal of the authority granted in the [REDACTED] Order. The government was unable, before the expiration of that authority on [REDACTED], to determine the extent to which the previously-acquired information exceeded the scope of the Court's orders or to rule out the possibility that some of the information fell outside the scope of the pen register statute. See [REDACTED] Order at 2-4. Accordingly, as an interim measure, Judge Walton entered an order on [REDACTED] directing the government not to access the information previously

obtained “for any analytic or investigative purpose,” except when such access is “necessary to protect against an imminent threat to human life.” See [REDACTED] Order at 4-5; see also page 23, supra.

The application now before the Court includes a request to lift the [REDACTED] Order. See [REDACTED] Application at 16. Since [REDACTED], both the Court and the government have had the opportunity to make a thorough assessment of the scope and circumstances of the overcollection and to consider the pertinent legal issues. Based on that assessment, the Court believes that it is now appropriate to rescind the [REDACTED] Order, which, as noted, was intended to be an interim measure, and to refine the rules for handling the prior bulk PR/TT collection.

B. The Court Lacks Authority to Grant the Government’s Request in its Entirety

The Court concludes that it has only limited authority to grant the government’s request for permission to resume accessing and using previously-collected information. As discussed in more detail below, the Court concludes that it possesses authority to permit the government to query data collected within the scope of the Court’s prior orders, and that it is appropriate under the circumstances to grant such approval. But for information falling outside the scope of the prior orders, the Court lacks authority to approve any use or disclosure that would be prohibited under 50 U.S.C. § 1809(a)(2). Accordingly, the Court will deny the government’s request with respect to those portions of the unauthorized collection that are covered by Section 1809(a)(2). To the extent that other portions of the unauthorized prior collection may fall outside the reach of

Section 1809(a)(2), the Court concludes that it has authority to grant the government's request and that it is appropriate under the circumstances to do so.

1. Information Authorized for Acquisition Under the Court's Prior Orders

The government argues that the FISA PR/TT statute, 50 U.S.C. § 1842, empowers the Court to authorize NSA to resume querying the prior collection in its entirety. See Memorandum of Law at 72-73. As discussed above, the Court continues to be satisfied that it may, pursuant to Section 1842 and subject to appropriate restrictions, authorize NSA to acquire, in bulk, the metadata associated with Internet communications transiting the United States. Further, although Section 1842 does not explicitly require the application of minimization procedures to PR/TT-acquired information, the Court also agrees that in light of the sweeping and non-targeted nature of this bulk collection, it has authority to impose limitations on access to and use of the metadata that NSA has accumulated.

The Court is satisfied that it may invoke the same authority to permit NSA to resume querying the PR/TT information that was collected in accordance with the Court's prior orders. The Court is further persuaded that, in light of the government's assertion of national security need,⁷⁹ it is appropriate to exercise that authority. Accordingly, the Court hereby orders that the government may access, use, and disseminate bulk PR/TT information that was collected in

⁷⁹ See [REDACTED] Alexander Decl. at 10 n.6 ("The ability of NSA to access the information collected under docket number PR/TT [REDACTED] and previous dockets is vital to NSA's ability to carry out its counterterrorism intelligence mission. If NSA is not able to combine the information it collects prospectively with the information it collected [previously], there will be a substantial gap in the information available to NSA.").

accordance with the terms of the Court's prior orders, subject to the procedures and restrictions discussed herein that will apply to newly-acquired metadata.

2. Information Not Authorized for Acquisition Under the Court's Prior Orders

By contrast, the Court is not persuaded that it has authority to grant the government's request with respect to all information collected outside the scope of its prior orders. FISA itself precludes the Court from granting that request in full.

a. 50 U.S.C. § 1809(a)(2) Precludes the Court from Granting the Government's Request with Respect to Some of the Prior Unauthorized Collection

The crucial provision of FISA, 50 U.S.C. § 1809, provides, in pertinent part, as follows:

(a) Prohibited Activities

A person is guilty of an offense if he intentionally –

...

(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this chapter, chapter 119, 121, or 206 of Title 18 or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title.

50 U.S.C. § 1809(a)(2).

Section 1809(a)(2) has three essential elements: (1) the intentional disclosure or use of information (2) obtained under color of law through electronic surveillance (3) by a person knowing or having reason to know that the information was obtained through electronic surveillance not authorized by one of the enumerated (or similar) statutory provisions. The

government's request to access, use, and disseminate the fruits of the prior unauthorized collection implicates all three elements of Section 1809(a)(2)'s criminal prohibition.

Application of the first two elements is straightforward. Plainly, conducting contact chaining inquiries of stored data and sharing the query results both within and outside NSA would constitute the intentional use and disclosure of information.⁸⁰ It is also clear that the data previously collected by the government – which was acquired through the use of orders issued by this Court pursuant to FISA – was obtained “under color of law.” See West v. Atkins, 487 U.S. 42, 49-50 (1988) (explaining that the misuse of authority possessed by virtue of law is action “under color of law”).⁸¹

The third element requires lengthier discussion, but, in summary, the Court concludes that some of the prior bulk PR/TT collection is information that the responsible government officials know or have reason to know was obtained through electronic surveillance not authorized by one of the statutory provisions referred to in Section 1809(a)(2). To begin with,

⁸⁰ Insofar as the government contends that Section 1809(a)(2) reaches only “intentional violations of the Court’s orders,” or “willful” as opposed to intentional conduct, see Memorandum of Law at 74 n. 37, the Court disagrees. The plain language of the statute requires proof that the person in question “intentionally” disclosed or used information “knowing or with reason to know” the information was obtained in the manner described.

⁸¹ The phrase “a person” in Section 1809 is certainly intended to cover government officials. In addition to requiring conduct “under color of law,” the statute provides an affirmative defense to prosecution for a “law enforcement or investigative officer engaged in the course of his official duties” in connection with electronic surveillance “authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.” See 50 U.S.C. § 1809(b).

the language of Section 1809(a)(2) demonstrates that Congress intended at least some unauthorized PR/TT acquisitions to be covered by the criminal prohibition. The statute expressly reaches, among other things, information obtained through “electronic surveillance not authorized by this chapter, [or] chapter 119, 121, or 206 of Title 18.” Section 1809 is part of Chapter 36 of Title 50 of the U.S. Code. Chapter 36, in turn, encompasses all of FISA, as codified in Title 50, including FISA’s PR/TT provisions found at 50 U.S.C. §§ 1841-1846. Accordingly, “this chapter” in Section 1809(a)(2) refers in part to the FISA PR/TT provisions. Moreover, Chapter 206 of Title 18, which is also referenced in Section 1809(a)(2), consists exclusively of the PR/TT provisions of the criminal code, 18 U.S.C. §§ 3121-3127, key portions of which are incorporated by reference into FISA. See 50 U.S.C. § 1841(2) (incorporating the definitions of “pen register” and “trap and trace device” found at 18 U.S.C. § 3127). Because Chapter 206 of Title 18 authorizes no means of acquiring information other than through the use of PR/TT devices, Section 1809(a)(2)’s reference to “electronic surveillance” must be understood to include at least some information acquired through the use of PR/TT authority.

That conclusion is reinforced by examination of FISA’s definition of “electronic surveillance,” which applies to Section 1809, see 50 U.S.C. § 1801 (“As used in this subchapter: . . .”), and which is broad enough to include some (but not necessarily all) information acquired through the use of PR/TT devices.⁸² “Electronic surveillance” is defined, in

⁸² See also H.R. Rep. 95-1283, pt. 1, at 51 (1978) (“The surveillance covered by [Section 1801(f)(2)] is not limited to the acquisition of the oral or verbal contents of a communication . . . (continued...)”)

pertinent part, as “the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States.” 50 U.S.C. § 1801(f)(2).⁸³

For purposes of this definition of “electronic surveillance,” “contents” is defined in Section 1801(n) to include, among other things, “any information concerning the identity of the parties” to a communication “or the existence . . . of that communication.”⁸⁴ “Wire communication” is defined as “any communication while it is being carried by a wire, cable, or other like connection

⁸²(...continued)

[and] includes any form of ‘pen register’ or ‘touch-tone decoder’ device which is used to acquire, from the contents of a voice communication, the identities or locations of the parties to the communication.”).

⁸³ Section 1801(f) includes three additional definitions of “electronic surveillance,” only one of which appears to have any possible application with regard to the prior bulk PR/TT collection. Subsections (f)(1) (“the acquisition . . . of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person”) and (f)(3) (“the intentional acquisition . . . of any radio communication”) are flatly inapplicable. Subsection (f)(4) could apply to the extent the prior collection included non-wire communications acquired under “circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.” The Court’s analysis of Section 1809(a)(2) would, of course, apply identically to prior unauthorized collection constituting “electronic surveillance” under any of the definitions set forth in Section 1801(f).

⁸⁴ As noted above, the definition of “contents” in Section 1801(n) is different than the definition of “contents” in 18 U.S.C. § 2510(8) – the latter definition does not include information concerning the identity of the parties to or the existence of the communication. See page 27, supra; [REDACTED] Opinion at 6 n.6. Accordingly, information constituting “contents” as used in Section 1801(f) can be acquired through the use of a PR/TT device, provided that it does not also constitute “contents” under Section 2510(8) and that it otherwise satisfies the statutory requirements for acquisition by PR/TT collection.

furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign commerce.” 50 U.S.C. § 1801(I). Reading those definitions together, then, “electronic surveillance” includes, among other things, the acquisition (1) by an electronic, mechanical, or other surveillance device (2) of information concerning the identity of the parties to or the existence of any communication to or from a person in the United States, (3) when such information is acquired in the United States (4) while the communication is being carried on a wire, cable, or other like connection furnished or operated by a common carrier.

The unauthorized portion of the prior PR/TT collection includes some information that meets all four of these criteria. First, there is no question that the prior collection was acquired through the use of “electronic, mechanical, or other surveillance devices.” See, e.g., [REDACTED] Decl. at 9 (describing the use of “NSA-controlled equipment or devices” to “extract metadata for subsequent forwarding to NSA’s repositories”).

Second, the overcollection included information concerning the identity of the parties to and the existence of communications to or from persons in the United States. Persons in the United States were parties to some of the communications for which data was acquired. See, e.g., [REDACTED] Application at 5-6 (stating that the collection will include metadata pertaining to persons within the United States); *id.* at 9 (stating that the “collection activity . . . will collect metadata from electronic communications that are: (1) between the United States and abroad; (2) between overseas locations; and (3) wholly within the United States”). And, as discussed above,

the unauthorized collection included: [REDACTED]

[REDACTED]

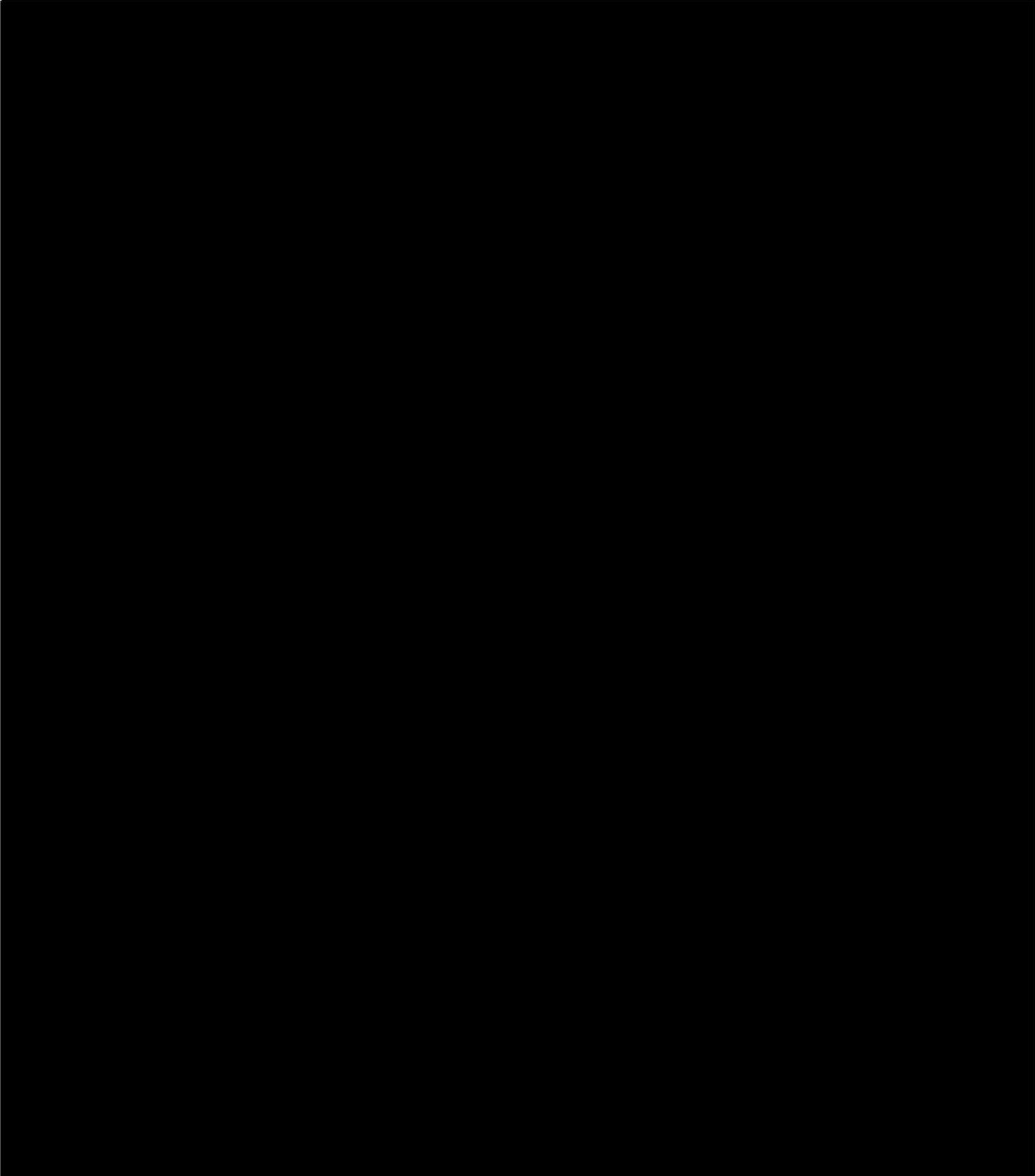
[REDACTED] All of these forms of information concern the existence of an associated communication, and many of them could also concern the identities of the communicants.

Third, the data previously collected, both authorized and unauthorized, was acquired in the United States. See, e.g., [REDACTED] Application at 9 (“All of the collection activity described above will occur in the United States”); [REDACTED] Opinion at 72-80 [REDACTED]

[REDACTED]

Fourth, it appears that much, and perhaps all, of the information previously collected was acquired while the associated communication was “being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign commerce.” See 50 U.S.C. § 1801(d). [REDACTED]

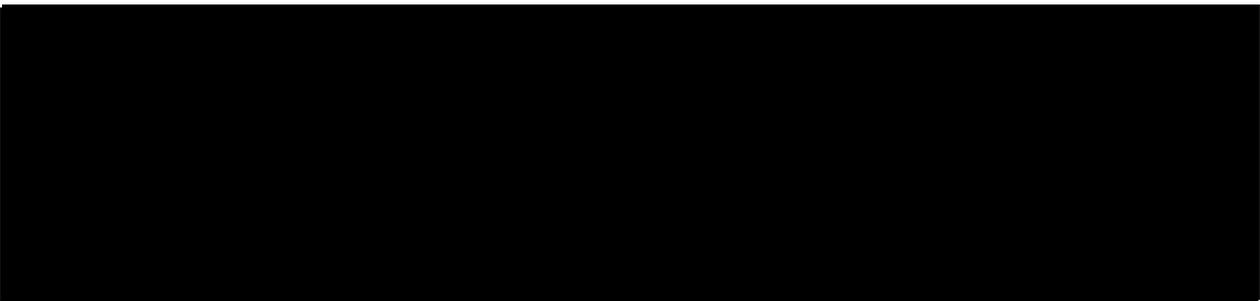
[REDACTED]





For the foregoing reasons, the Court concludes that at least some of the data previously collected, including portions of the data that was not authorized by the Court's prior orders, constitutes unauthorized "electronic surveillance" under Section 1809(a)(2). But that does not complete the analysis. Section 1809 does not prohibit all disclosures or uses of unauthorized electronic surveillance; rather, it reaches disclosure or use only by "a person knowing or having reason to know" that the information was obtained through unauthorized electronic surveillance.

The Court concludes that the knowledge requirement is satisfied for some of the prior unauthorized collection constituting electronic surveillance. The government has acknowledged that particular portions of the prior collection fell outside the scope of the Court's prior



authorizations. See generally [REDACTED] Report. Further, some of that unauthorized collection is identifiable as electronic surveillance – i.e., as information concerning the identity of the parties to or the existence of any communication to or from a person in the United States that was acquired in the United States while the communication was being carried on a wire, cable, or other like connection furnished or operated by a common carrier. As demonstrated above, the government’s filings dating back to [REDACTED] demonstrate that most, if not all, of the information previously collected was acquired in the United States [REDACTED]

[REDACTED] The government’s descriptions of the overcollected information make clear that the information concerns the identity of the parties, the existence of the communication, or both. Finally, the information available to the government – e.g., e-mail identifiers [REDACTED] – is likely to make some of the data collected identifiable as concerning communications to or from a person in the United States. Accordingly, the Court concludes that the government officials responsible for using and making disclosures of bulk PR/TT-derived information know or have reason to know that portions of the prior collection constitute unauthorized electronic surveillance.⁸⁶

⁸⁶ In the law enforcement context, courts have held that there is no statutory prohibition on the use – specifically, the evidentiary use – of the results of unlawful PR/TT surveillance. See, e.g., *Forrester*, *supra*, 512 F.3d at 512-13 (citing cases). Those decisions, however, do not address the potential application of Section 1809(a)(2), and so provide no basis for departing from the clear terms of that statutory prohibition. Indeed, *Forrester* recognized that suppression would be warranted if it were “clearly contemplated by [a] relevant statute” and stressed that the party seeking suppression had failed to “point to any statutory language requiring suppression.”

(continued...)

b. Section 1809(a)(2) Applies to the Prior Collection

The government does not contest that portions of the prior collection contain information that the responsible officials know or have reason to know constitutes “electronic surveillance” that was collected without the necessary authority. Instead, the government offers several reasons why it believes Section 1809(a)(2) presents no bar to Court approval of use of the prior collection. The Court finds the government’s contentions unpersuasive.

The government argues that the opening phrase of 50 U.S.C. § 1842(a) vests the Court with authority to enter an order rendering Section 1809(a)(2) inapplicable. See Memorandum of Law at 74 n. 37. The Court disagrees. Section 1842(a), which is entitled “Application for authorization or approval,” provides in pertinent part as follows:

Notwithstanding any other provision of law, the Attorney General or a designated attorney for the government may make an application for an order or an extension of an order authorizing or approving the installation or use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information

As the context makes clear, the opening phrase “[n]otwithstanding any other provision of law” in Section 1842 relates to the circumstances in which the government may apply for an order permitting it to install and use a PR/TT device for foreign intelligence purposes. It does not speak to the Court’s authority to grant a request for permission to use and disclose information

⁸⁶(...continued)

Id. at 512; see also Nardone v. United States, 302 U.S. 379, 382-84 (1937) (statute prohibiting any person from divulging the substance of interstate wire communications precluded testimony by law enforcement agents about such communications).

obtained in violation of prior orders authorizing the installation of PR/TT devices. Indeed, the Court finds nothing in the text of Section 1842 or the other provisions of FISA that can be read to confer such authority, particularly in the face of the clear prohibition set forth in Section 1809(a)(2).

The government next contends that because the Court has, in its prior orders, regulated access to and use of previously accumulated metadata, it follows that the Court may now authorize NSA to access and use all previously collected information, including information that was acquired outside the scope of prior authorizations, so long as the information “is within the scope of the [PR/TT] statute and the Constitution.” Memorandum of Law at 73. But the government overstates the precedential significance of the Court’s past practice. The fact that the Court has, at the government’s invitation, exercised authority to limit the use of properly-acquired bulk PR/TT data does not support the conclusion that it also has authority to permit the use of improperly-acquired PR/TT information, especially when such use is criminally prohibited by Section 1809(a)(2).

The Court has limited the access to and use of information collected in accordance with prior authorizations, in view of the sweeping and non-targeted nature of that collection. The Court has done so within a statutory framework that generally permits the government to make comparatively liberal use, for foreign intelligence purposes, of information acquired pursuant to PR/TT orders, and in which the Court generally has a relatively small role beyond the acquisition

stage.⁸⁷ Thus, the Court's prior orders in this matter are notable not because they permitted the use of PR/TT-acquired data – again, the statute itself generally allows the use and dissemination of properly-acquired PR/TT information for foreign intelligence purposes – but because they imposed restrictions on such use to account for the bulk and non-targeted nature of the collection.⁸⁸ The Court has never authorized the government to access and use information collected outside the scope of its prior orders in this matter. Indeed, in the prior instances in which the Court learned of overcollections, it has carefully monitored the disposition of the improperly-acquired information to ensure that it was not used or disseminated by the government. See pages 11-12, 14, supra.

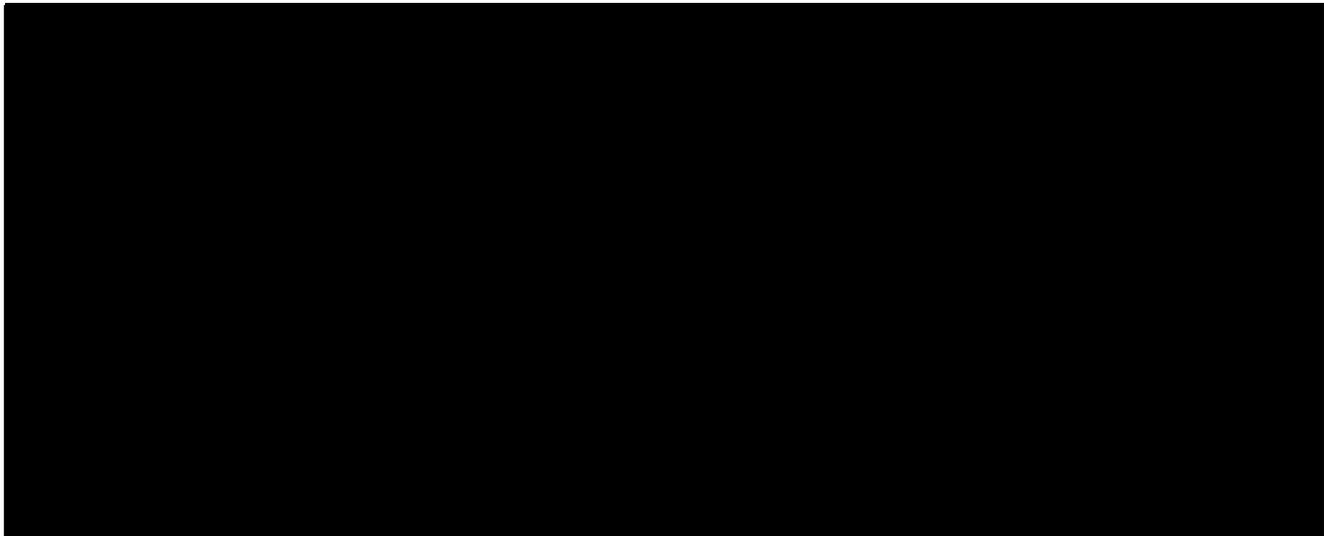
The government further contends that Rule 10(c) of the Rules of this Court gives the Court discretion to authorize access to and use of the overcollected information. Memorandum of Law at 73. The Court disagrees. Rule 10(c) requires the government, upon discovering that

⁸⁷ As discussed above, unlike the provisions for electronic surveillance and physical search, see 50 U.S.C. §§ 1801-1812, 1821-1829, the FISA PR/TT provisions do not require the application of Court-approved minimization procedures. In the context of Court-authorized electronic surveillance and physical searches, such procedures govern not only the acquisition of information, but also its retention and dissemination. See 50 U.S.C. §§ 1801(h), 1821(4). Like the electronic surveillance and physical search provisions, the FISA PR/TT provisions limit the use and disclosure of information acquired for law enforcement and other non-foreign intelligence-related purposes. Compare 50 U.S.C. § 1845 with 50 U.S.C. § 1806.

⁸⁸ Contrary to the government's assertion, the imposition of restrictions on the use and dissemination of the data collected is not "unique" to the bulk PR/TT. Indeed, the Court restricts the government's use of [REDACTED] See, e.g., Docket No. PR/TT [REDACTED] Primary Order at 4.

“any authority granted by the Court has been implemented in a manner that did not comply with the Court’s authorization,” to notify the Court of the incident and to explain, among other things, “how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.” FISC Rule 10(c). Rule 10 does not explicitly give the Court the authority to do anything. To be sure, the rule implicitly recognizes the Court’s authority, subject to FISA and other applicable law, to ensure compliance with its orders and with applicable Court-approved procedures. It does not, however, state or suggest that the Court is free in the event of an overcollection to dictate any disposition of the overcollected material that it wishes, without regard to other provisions of law, such as Section 1809(a)(2).⁸⁹

Finally, insofar as the government suggests that the Court has inherent authority to permit the use and disclosure of all unauthorized collection without regard to Section 1809, see Memorandum of Law at 73-74 & n.37, the Court again must disagree. To be sure, this Court, like all other Article III courts, was vested upon its creation with certain inherent powers. See In



re Motion for Release of Court Records, 526 F. Supp. 2d 484, 486 (FISA Ct. 2007); see also Chambers v. NASCO, Inc., 501 U.S. 32, 43 (1991) (“It has long been understood that [c]ertain implied powers must necessarily result to our Courts of justice from the nature of their institution . . .”). It is well settled, however, that the exercise of such authority “is invalid if it conflicts with constitutional or statutory provisions.” Thomas v. Arn, 474 U.S. 140, 148 (1985). And defining crimes is not among the inherent powers of the federal courts; rather, federal crimes are defined by Congress and are solely creatures of statute. Bousley v. United States, 523 U.S. 614, 620-21 (1998); United States v. Hudson, 11 U.S. (7 Cranch) 32, 34 (1812). Accordingly, when Congress has spoken clearly, a court assessing the reach of a criminal statute must heed Congress’s intent as reflected in the statutory text. See, e.g., Huddleston v. United States, 415 U.S. 814, 831 (1974). The plain language of Section 1809(a)(2) makes it a crime for any person, acting under color of law, intentionally to use or disclose information with knowledge or reason to know that the information was obtained through unauthorized electronic surveillance. The Court simply lacks the power, inherent or otherwise, to authorize the government to engage in conduct that Congress has unambiguously prohibited.⁹⁰

⁹⁰ In its [REDACTED] Response at page 4 n.1, the government added an alternative request for the Court to amend all prior bulk PR/TT orders nunc pro tunc to permit acquisition of the overcollected information. The Court denies that request. Nunc pro tunc relief is appropriate to conform the record to a court’s original intent but is not a means to alter what was originally intended or what actually transpired. See, e.g., U.S. Philips Corp. v. KBC Bank N.V., 590 F.3d 1091, 1094 (9th Cir. 2010) (citing cases). Here, the prior bulk PR/TT orders make clear that the Court intended to authorize the government to acquire only information [REDACTED]

(continued...)

For the foregoing reasons, the Court will deny the government's request for authority to access and use portions of the accumulated prior PR/TT collection constituting information that the government knows or has reason to know was obtained through electronic surveillance not authorized by the Court's prior orders.

c. Portions of the Unauthorized Collection Falling Outside the Scope of Section 1809(a)(2)

There is one additional category of information to consider – overcollected information that is not subject to Section 1809(a)(2). The Court is not well positioned to attempt a comprehensive description of the particular types of information that are subject (or not) to Section 1809(a)(2)'s prohibition, but it appears that some of the overcollected data is likely to fall outside its reach. For example, NSA may have no way to determine based on the available information whether a particular piece of data relates to a communication obtained from the

[REDACTED]

[REDACTED]

Similarly, it may not be apparent from available information whether the communication to which a piece of data relates is to or from a person in the United States, such that acquisition constituted electronic surveillance as defined at Section 1801(f)(2).

⁹⁰(...continued)

[REDACTED] categories. Nunc pro tunc relief would thus be inappropriate here. See page 14, supra (discussing an instance in which the Court declined to grant a comparable request for nunc pro tunc relief).

When it is not known, and there is no reason to know, that a piece of information was acquired through electronic surveillance that was not authorized by the Court's prior orders, the information is not subject to the criminal prohibition in Section 1809(a)(2). Of course, government officials may not avoid the strictures of Section 1809(a)(2) by cultivating a state of deliberate ignorance when reasonable inquiry would likely establish that information was indeed obtained through unauthorized electronic surveillance. See, e.g., United States v. Whitehill, 532 F.3d 746, 751 (8th Cir.) (where "failure to investigate is equivalent to 'burying one's head in the sand,'" willful blindness may constitute knowledge), cert. denied, 129 S. Ct. 610 (2008). However, when it is not known, and there is genuinely no reason to know, that a piece of information was acquired through electronic surveillance that was not authorized by the Court's prior orders, the information is not subject to the criminal prohibition in Section 1809(a)(2).

The Court is satisfied that neither Section 1809(a)(2) nor any other provision of law precludes it from authorizing the government to access and use this category of information. The bigger question here is whether the Court should grant such authority. Given NSA's longstanding and pervasive violations of the prior orders in this matter, the Court believes that it would be acting well within its discretion in precluding the government from accessing or using such information. Barring any use of the information would provide a strong incentive for the exercise of greater care in this massive collection by the executive branch officials responsible for ensuring compliance with the Court's orders and other applicable requirements. On the other hand, the government has asserted that it has a strong national security interest in accessing and

using the overcollected information. The Court has no basis to question that assertion.

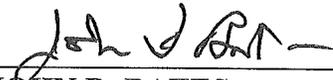
Furthermore, high-level officials at the Department of Justice and NSA have personally assured the Court that they will closely monitor the acquisition and use of the bulk PR/TT collection to ensure that the law, as reflected in the Court's orders, is carefully followed by all responsible officials and employees. In light of the government's assertions of need, and in heavy reliance on the assurances of the responsible officials, the Court is prepared – albeit reluctantly – to grant the government's request with respect to information that is not subject to Section 1809(a)(2)'s prohibition. Hence, the government may access, use, and disseminate such information subject to the restrictions and procedures described above that will apply to future collection.

The Court expects the responsible executive branch officials to act with care and in good faith in determining which portions of the prior collection are subject to Section 1809(a)(2)'s prohibition. The authorization to use overcollected information falling outside the scope of the criminal prohibition should not be understood as an invitation to disregard information that, if pursued, would create a reason to know that data was obtained by unauthorized electronic surveillance within the meaning of Section 1809(a)(2). The Court also expects the government to keep it reasonably apprised with regard to efforts to segregate those portions of the prior collection that it intends to use from the portions it is prohibited from using. Accordingly, the Court will order that each of the 30-day reports described above include a description of those efforts.

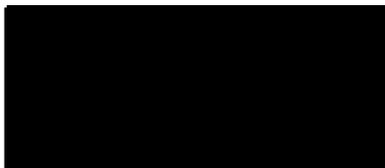
VI. Conclusion

For all the reasons set forth herein, the government's application will be granted in part and denied in part. Accompanying Primary and Secondary Orders are being issued contemporaneously with this Memorandum Opinion.

Signed _____ P02:37
Date _____ Time _____ E.T.



JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court



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.

██████████ 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 ██████████ ██████████ 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; ██████████ 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

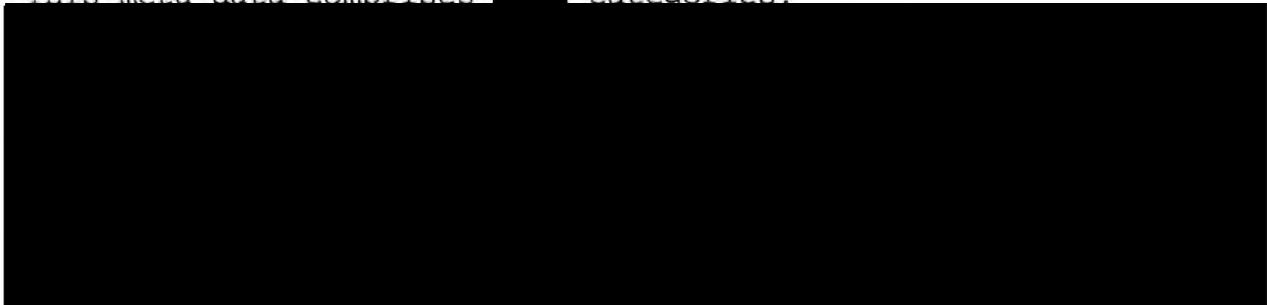
⁵ The other exclusions to this definition at § 2510(12)(B)-(D) are not relevant to this case.

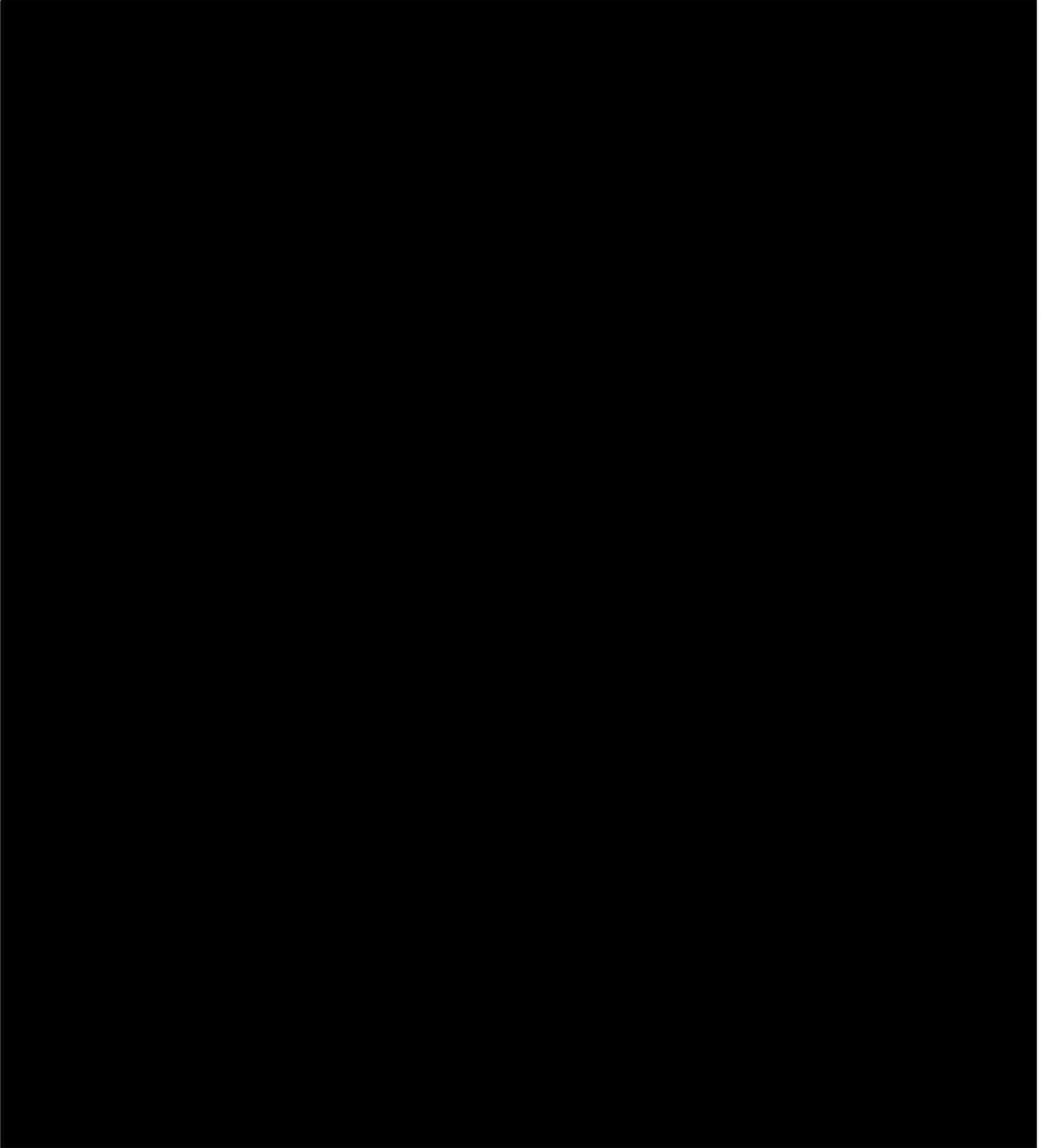
⁶ Different definitions of "wire communication" and "contents" are provided at 50 U.S.C. § 1801(l), (n). However, the definitions set forth in § 1801 apply to terms "[a]s used in this subchapter," i.e., in 50 U.S.C. §§ 1801-1811 (FISA subchapter on electronic surveillance), and thus have no bearing on 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).

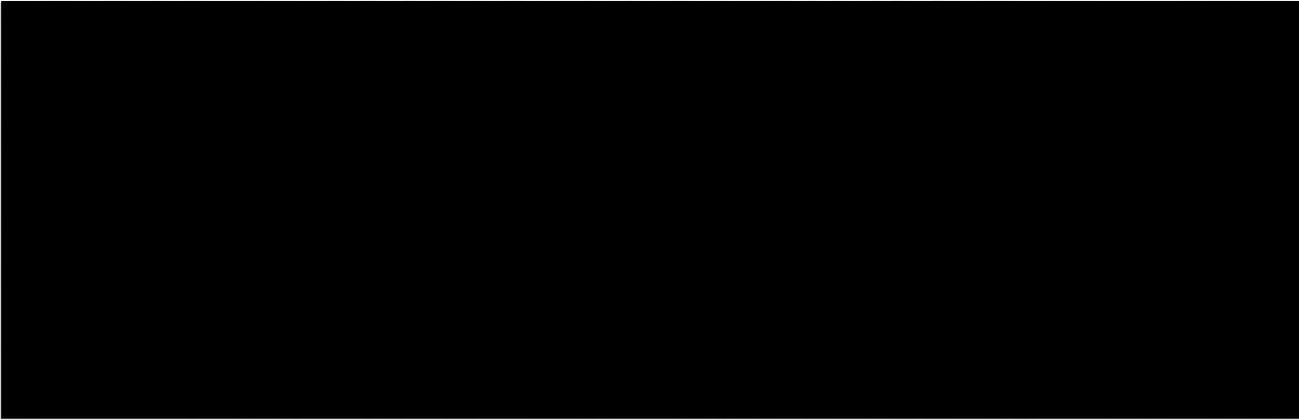
definitions to the devices described in the application presents two primary questions: (1) Does the information to be obtained constitute "dialing, routing, addressing, or signaling information" that does not include the "contents" of any communication? (2) Does the means by which such information would 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] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

Also, the address from which an e-mail was sent and [REDACTED] [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.

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]

[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] [REDACTED] [REDACTED]

[REDACTED], these groups of information are discussed separately below.

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

The above-described means of collecting information in Categories [REDACTED] [REDACTED] [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).

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).

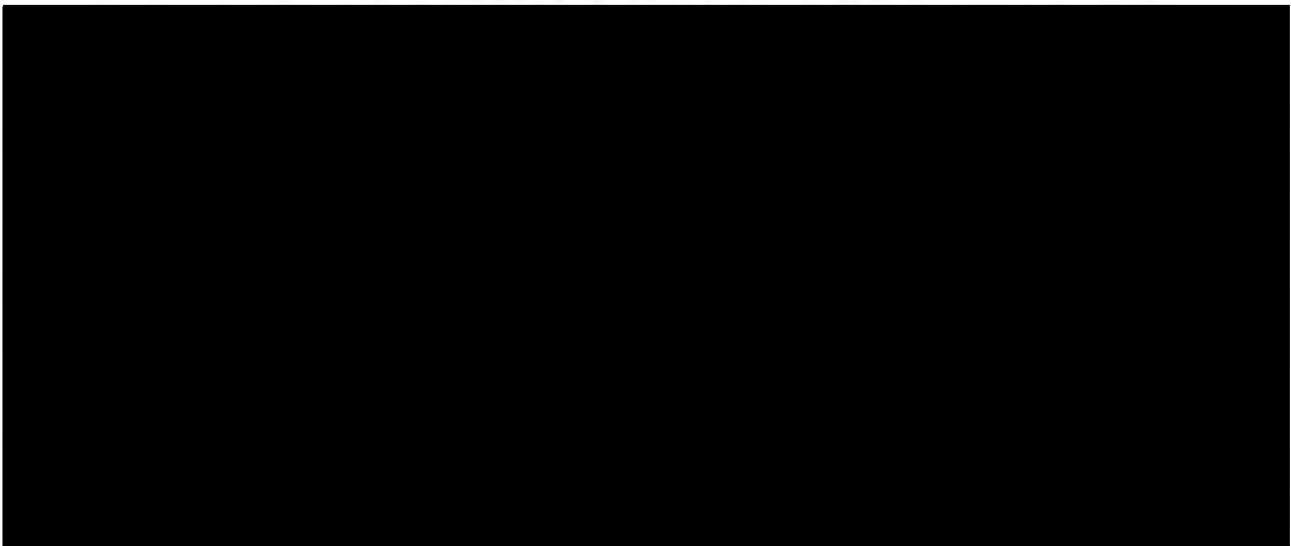
meta data in Categories [REDACTED] [REDACTED] [REDACTED] above falls under the definition of "pen register" at section 3127(3).

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] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[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]

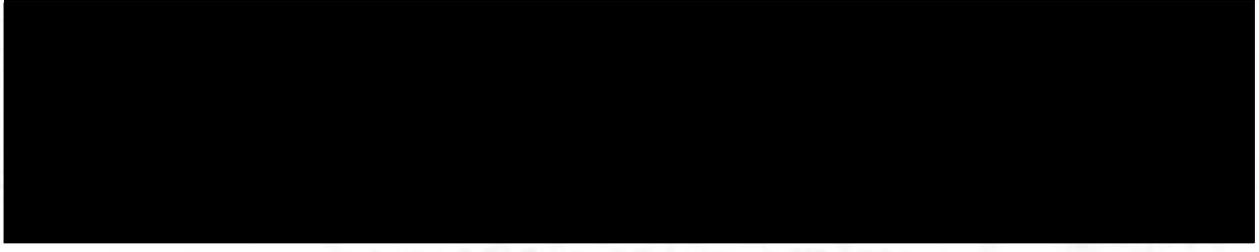


Thus, based on the plain meaning of

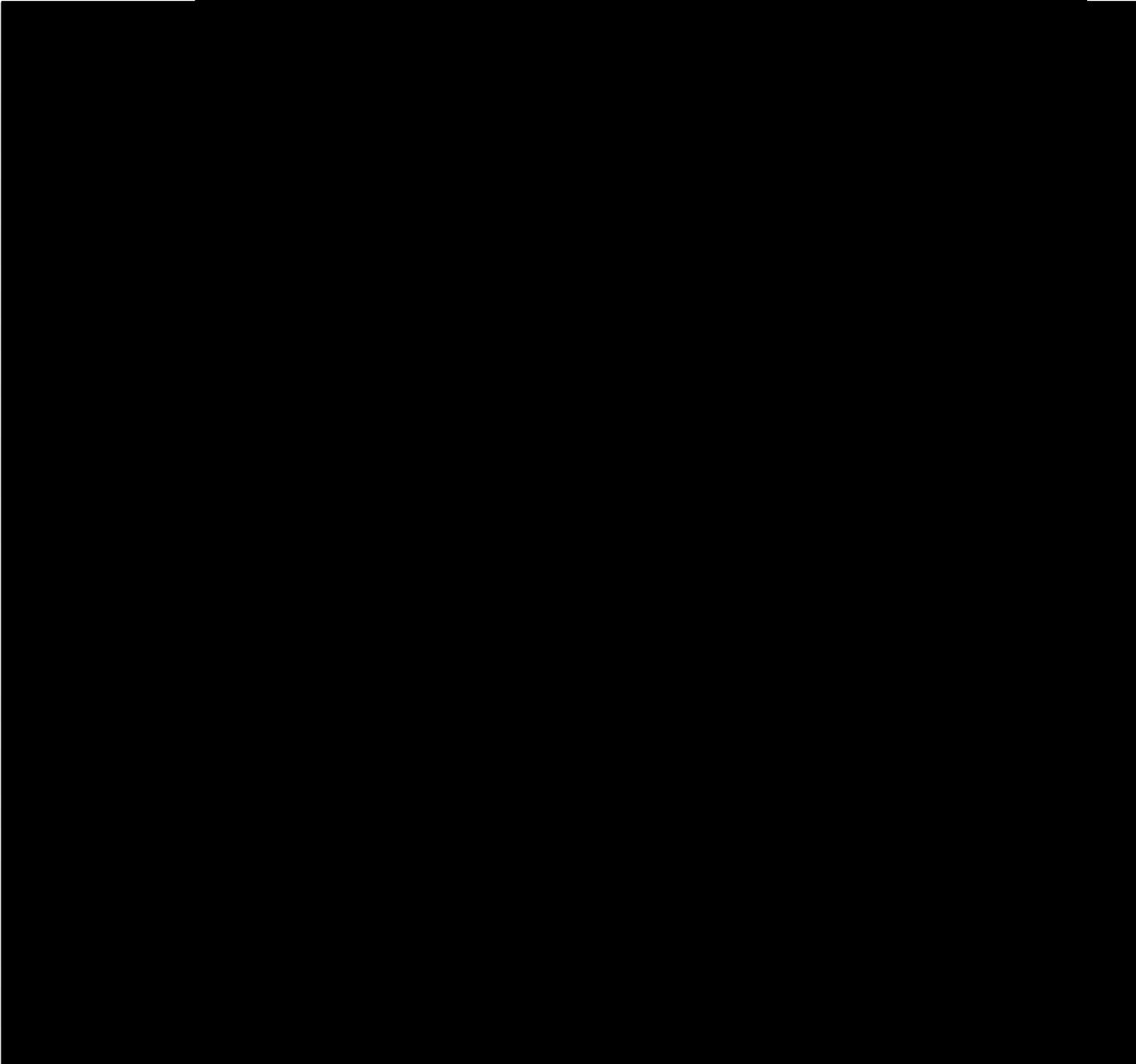
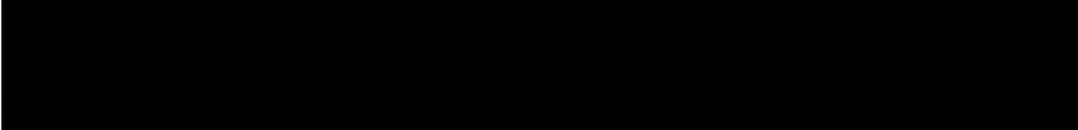
¹³ "Capture" is defined as, inter alia, " . . . 3. To succeed in preserving in a permanent form." Webster's II New College Dictionary 166 (2001).

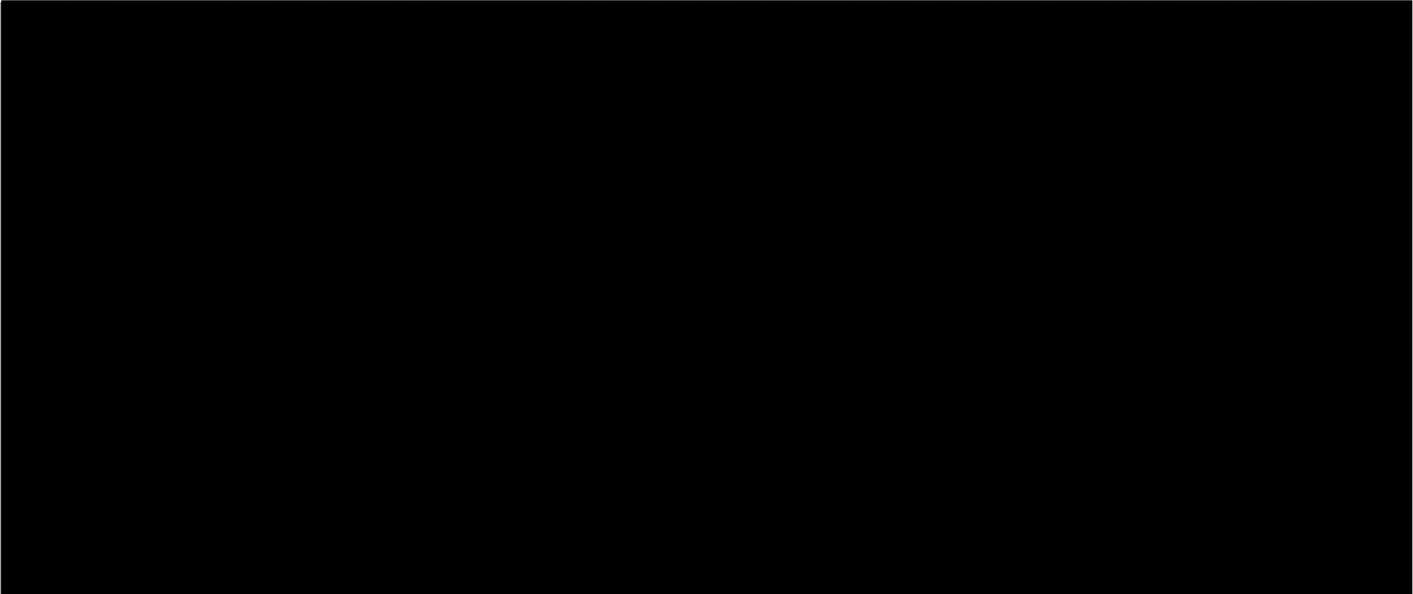


Such a result could be argued to violate the "cardinal principle of statutory construction that we must give effect, if possible, to every clause and word of a statute." Williams v. Taylor, 529 U.S. 362, 404 (2000) (internal quotations and citation omitted).



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





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.

 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  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] [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

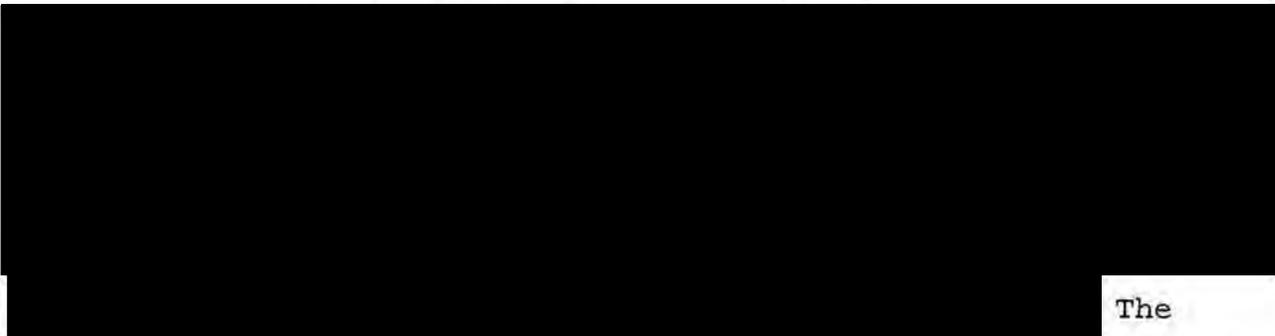
from the wording of § 1842(d)(2)(A)(ii) would make the applicability of the statute depend on the commercial or administrative practices of particular communications service providers - a result that here would serve no apparent purpose of Congress. Cf. Smith v. Maryland, 442 U.S. 735, 745 (1979) (finding 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]

[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.



The

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

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

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

(continued...)

statutory text," not "predecessor statutes," Lamie, 124 S. Ct. at 1030, and analysis of that text shows that collecting information in Categories [REDACTED] [REDACTED] [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] [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 threats²³ 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.

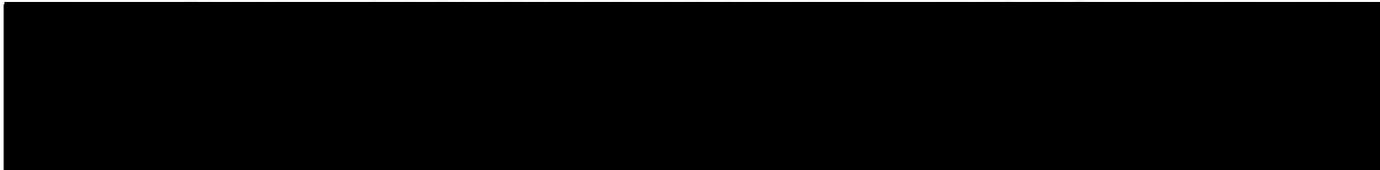
In support of the certification of relevance, the Government relies on the following facts and circumstances:

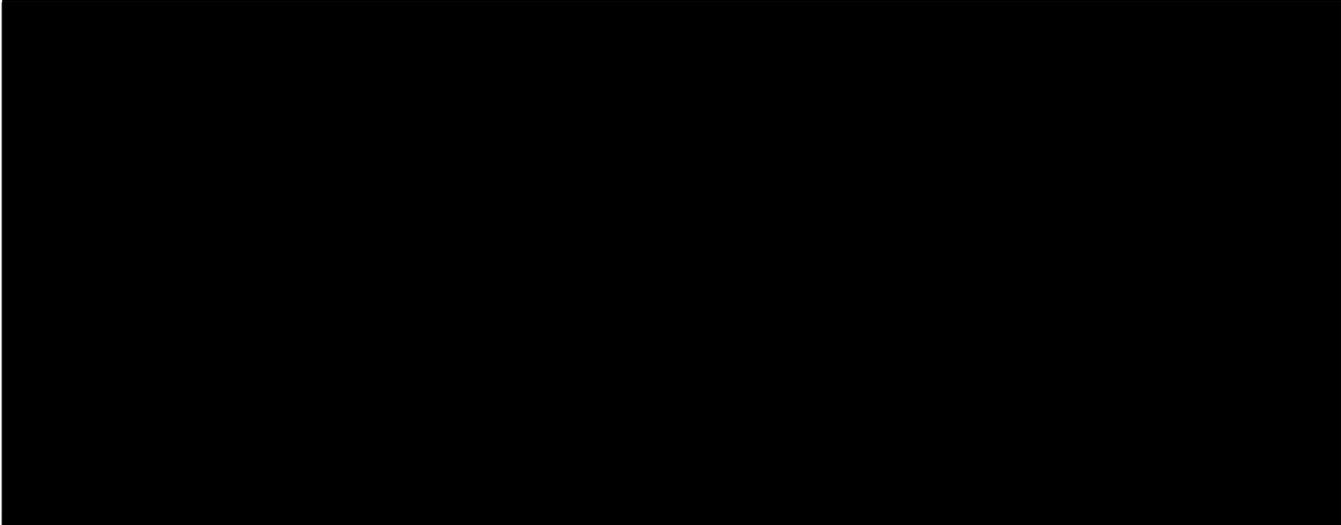
1. The Threat Currently Posed



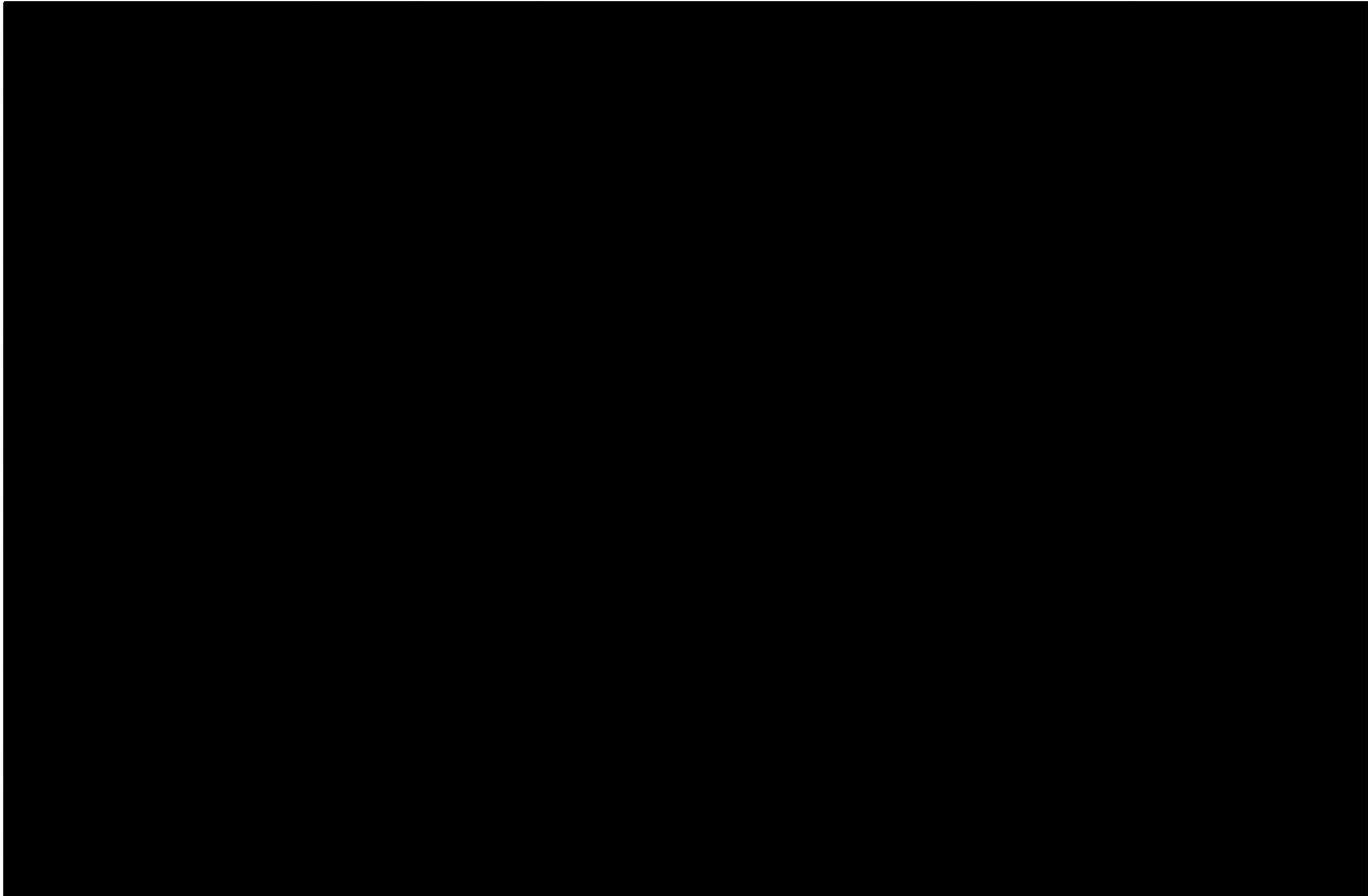
²⁴ (...continued)
risks at stake." Id. at 179.

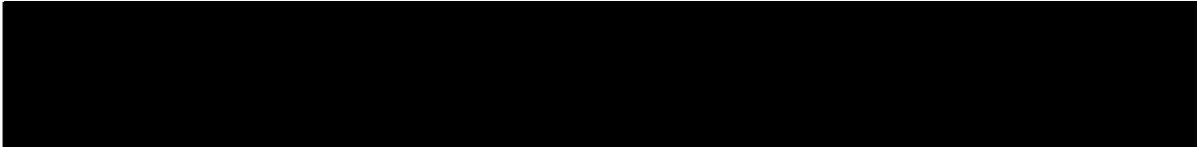
²⁵ For simplicity, this opinion standardizes the variant spellings of foreign names appearing in different documents submitted in support of the application.





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





3. The Use of the Internet by 





4. The Scope of the Proposed Collection of Meta Data

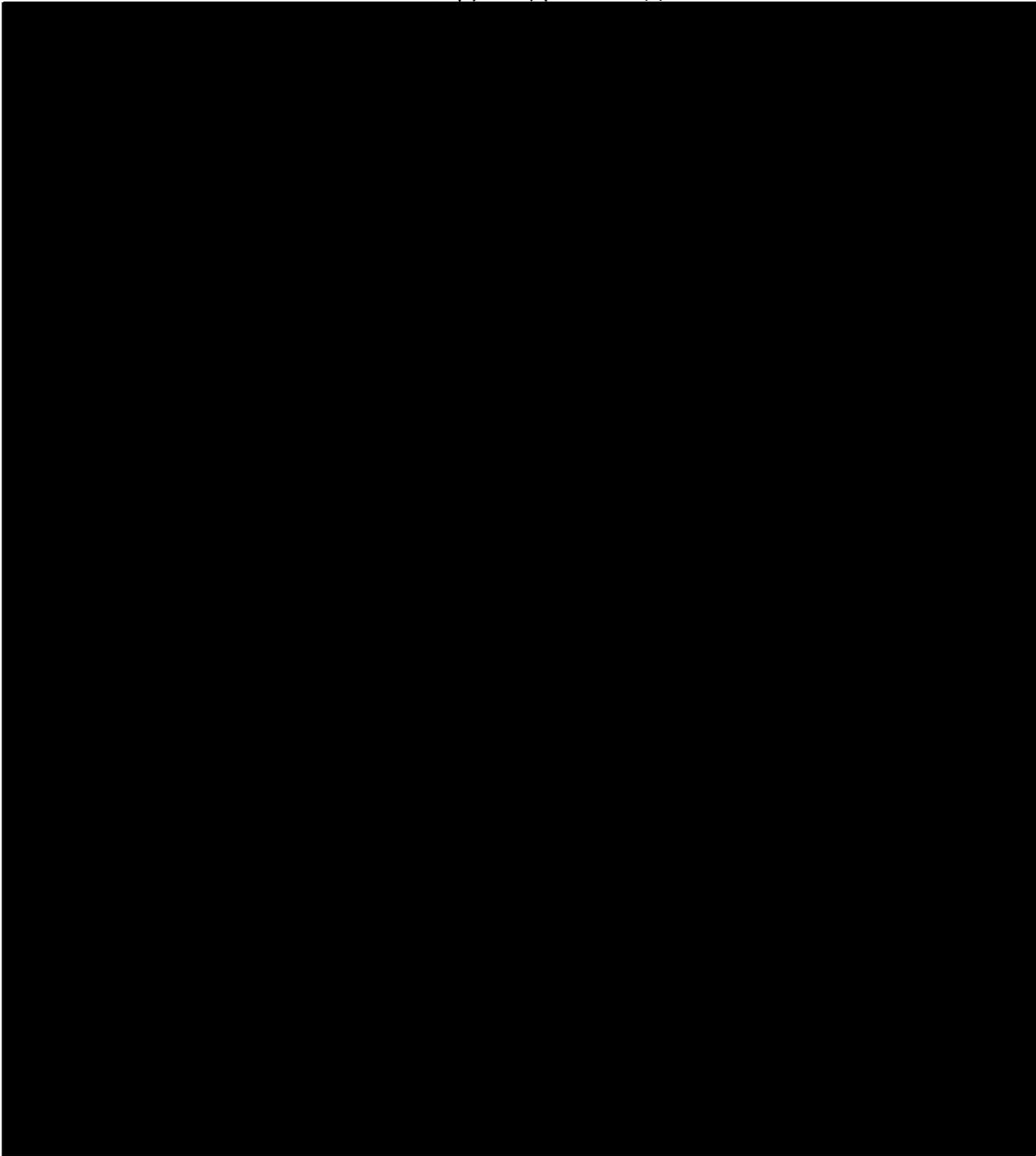
In an effort both to identify unknown and to track known operatives [redacted] through their Internet communications, NSA seeks to acquire meta data, as described above, from all e-mail [redacted]



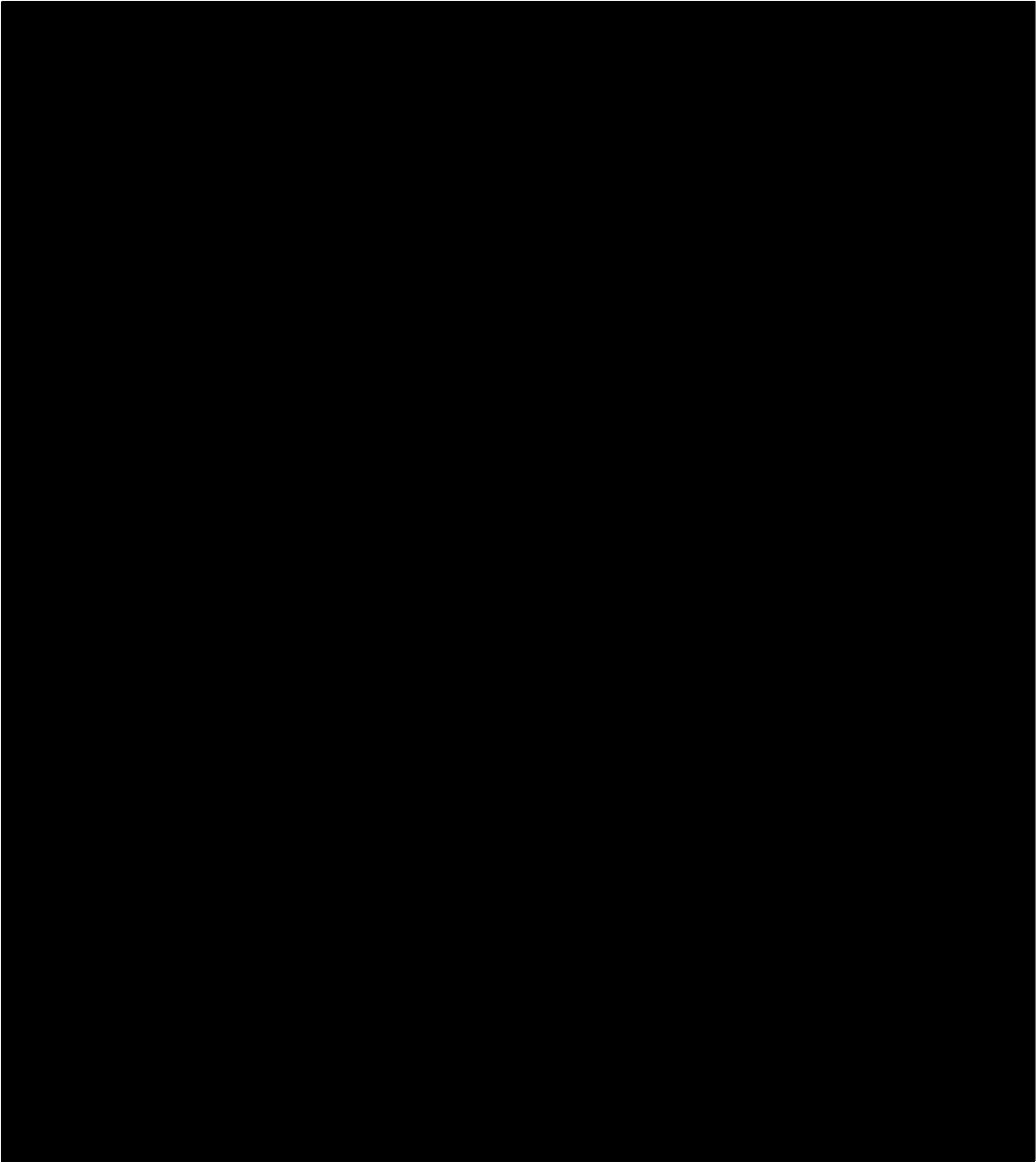
[redacted] are described in detail in the application and the DIRNSA Declaration. In brief, they are:

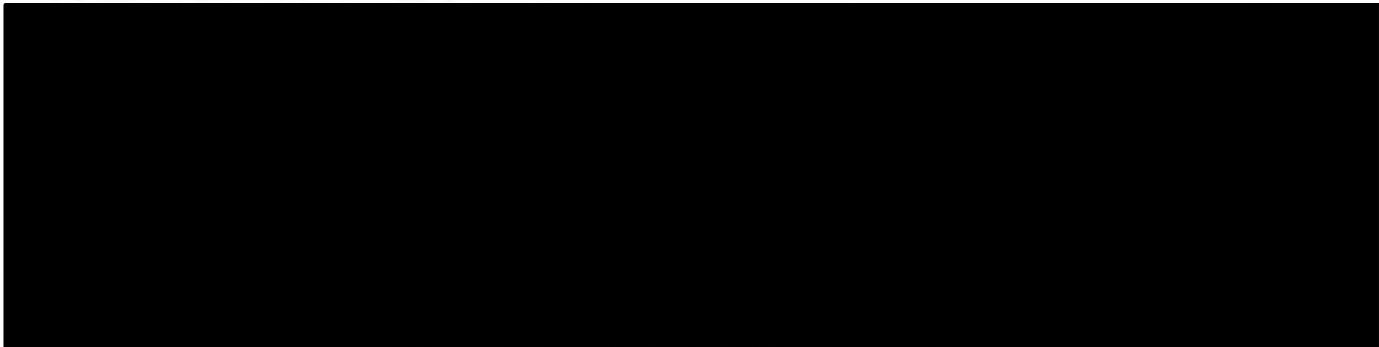
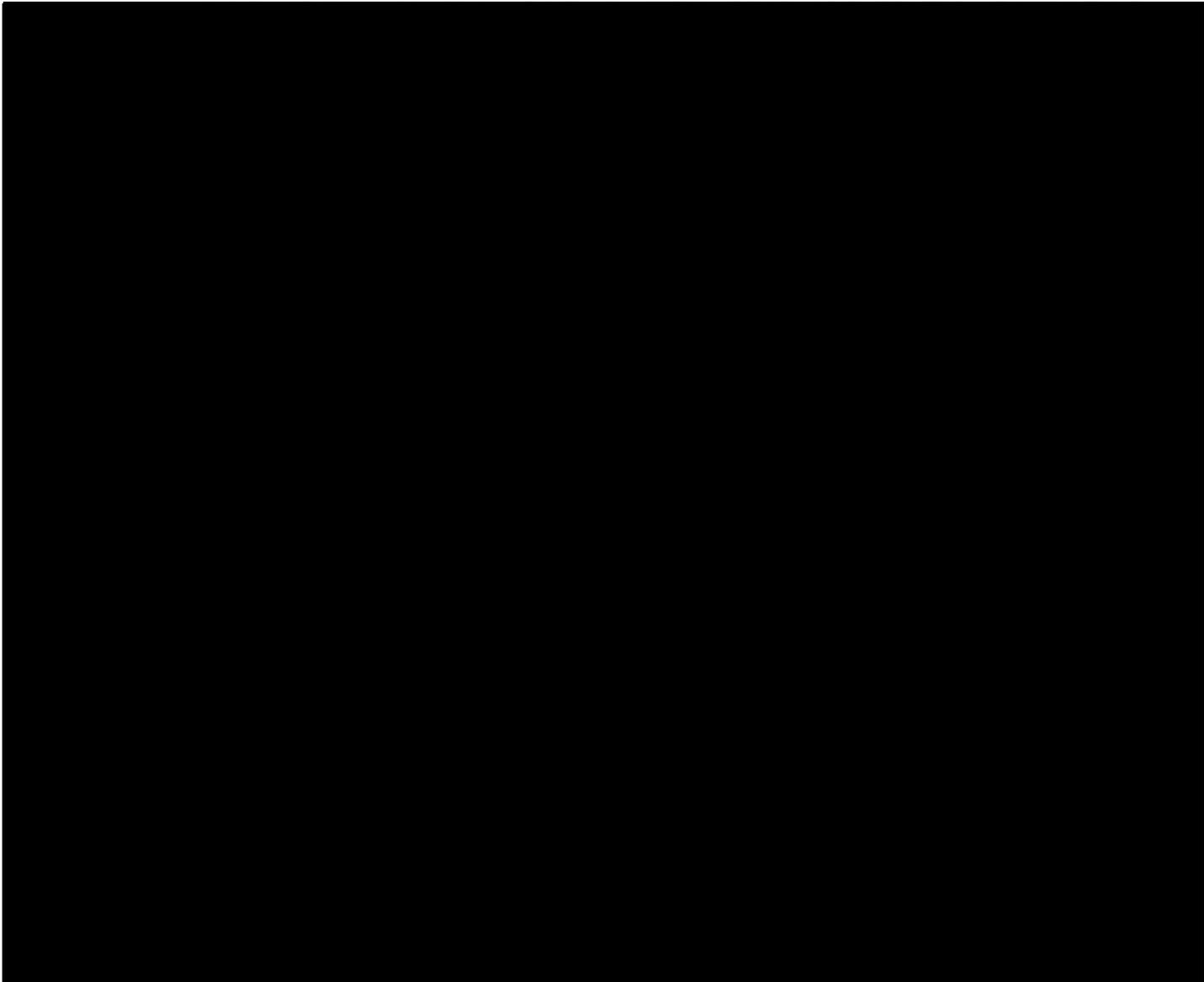


²⁷ For ease of reference, the term [redacted] is used to mean [redacted]



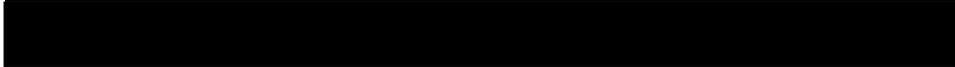
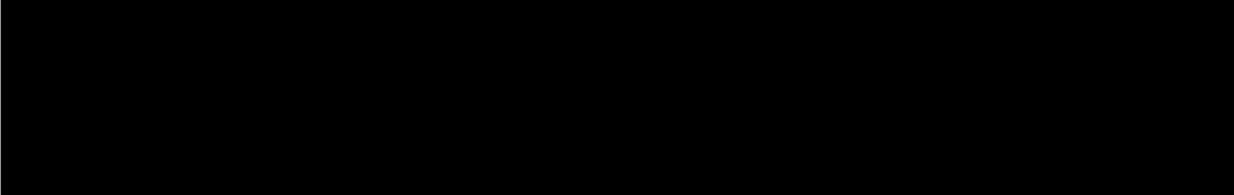
~~TOP SECRET//HCS//COMINT//NOFORN~~







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] [REDACTED] who bear no relation to [REDACTED]
[REDACTED]

[REDACTED]

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

[REDACTED]

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

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

[REDACTED]

states that even identified operatives [REDACTED]

[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]

[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]

[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]

[REDACTED] DIRNSA Declaration

at 15-16.

[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]

[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]

[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 CIA³³ 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]

[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] [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]

[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] [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]

[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 enforcement³⁶ 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] [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]

[REDACTED] These officials have also explained why they seek to collect meta data [REDACTED]

[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]

[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]

[REDACTED] is associated with [REDACTED] [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] [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."



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]

[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]otwithstanding any other provision of law," 50 U.S.C. § 1842(a)(1), and states that the Court "shall enter an ex parte order . . . approving the installation and use of a pen register or trap and trace device" upon a finding "that the application satisfies the requirements of [section 1842]," id. § 1842(d)(1), the Court has no need to consider how other statutes, such as the Privacy Act, 5 U.S.C. § 552a, might apply to the proposed activities of the Government.

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

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

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

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

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

B. First Amendment Issues

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

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

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

Conversely,

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

Reporters Comm., 593 F.2d at 1064.⁴⁸

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

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

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

content addressing information does not violate the First Amendment.⁴⁹

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

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

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

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

will help ensure that this information is used for the stated purpose of its collection - the identification and tracking of [REDACTED] [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

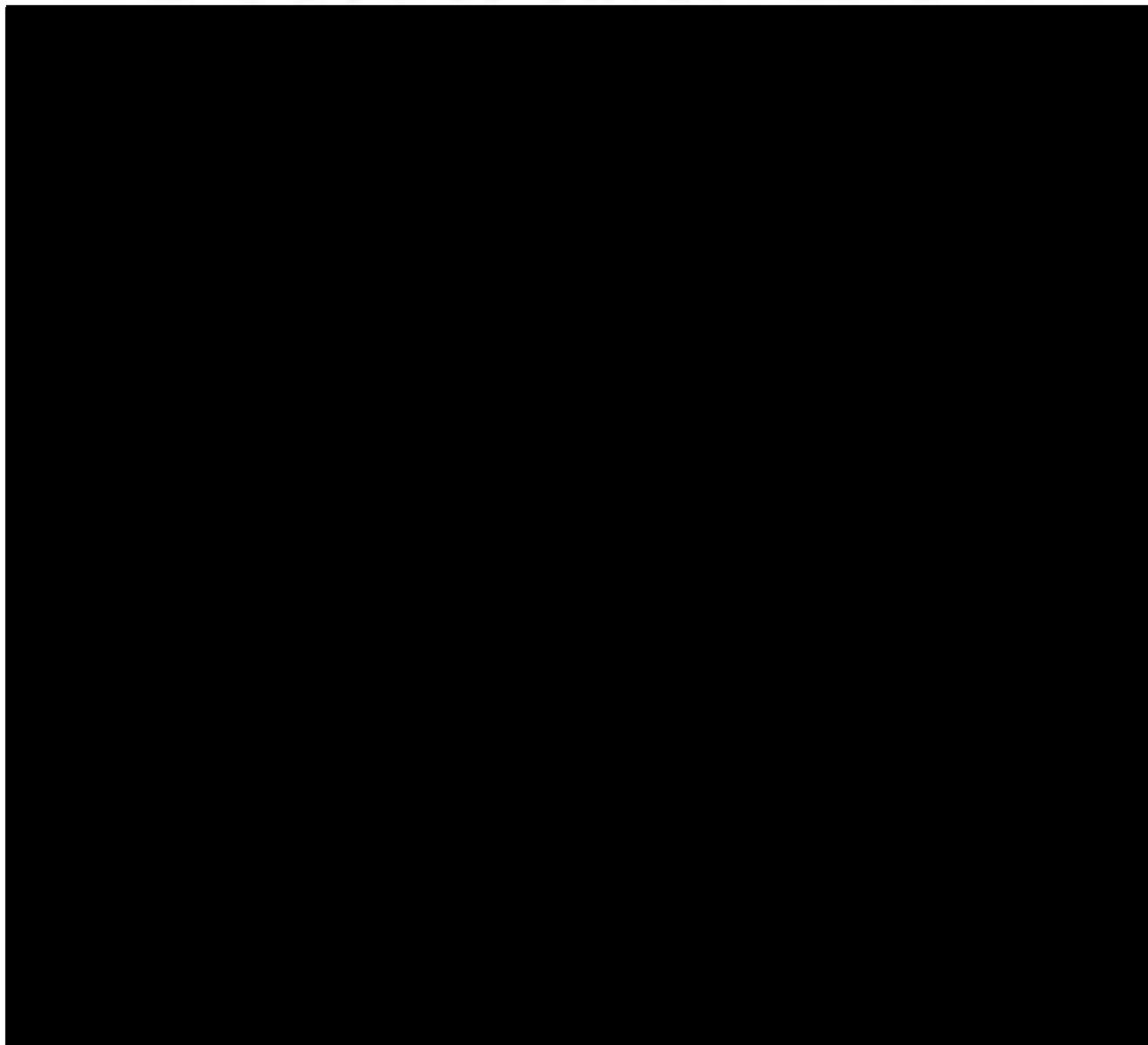
to the matters set forth therein, the Court finds, on the grounds explained above, that:

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.

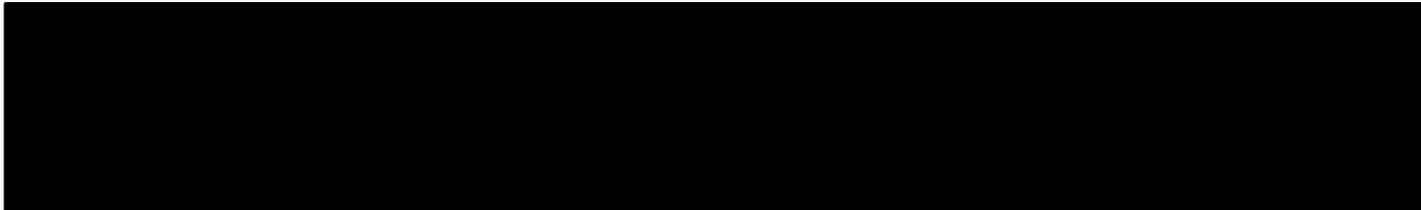
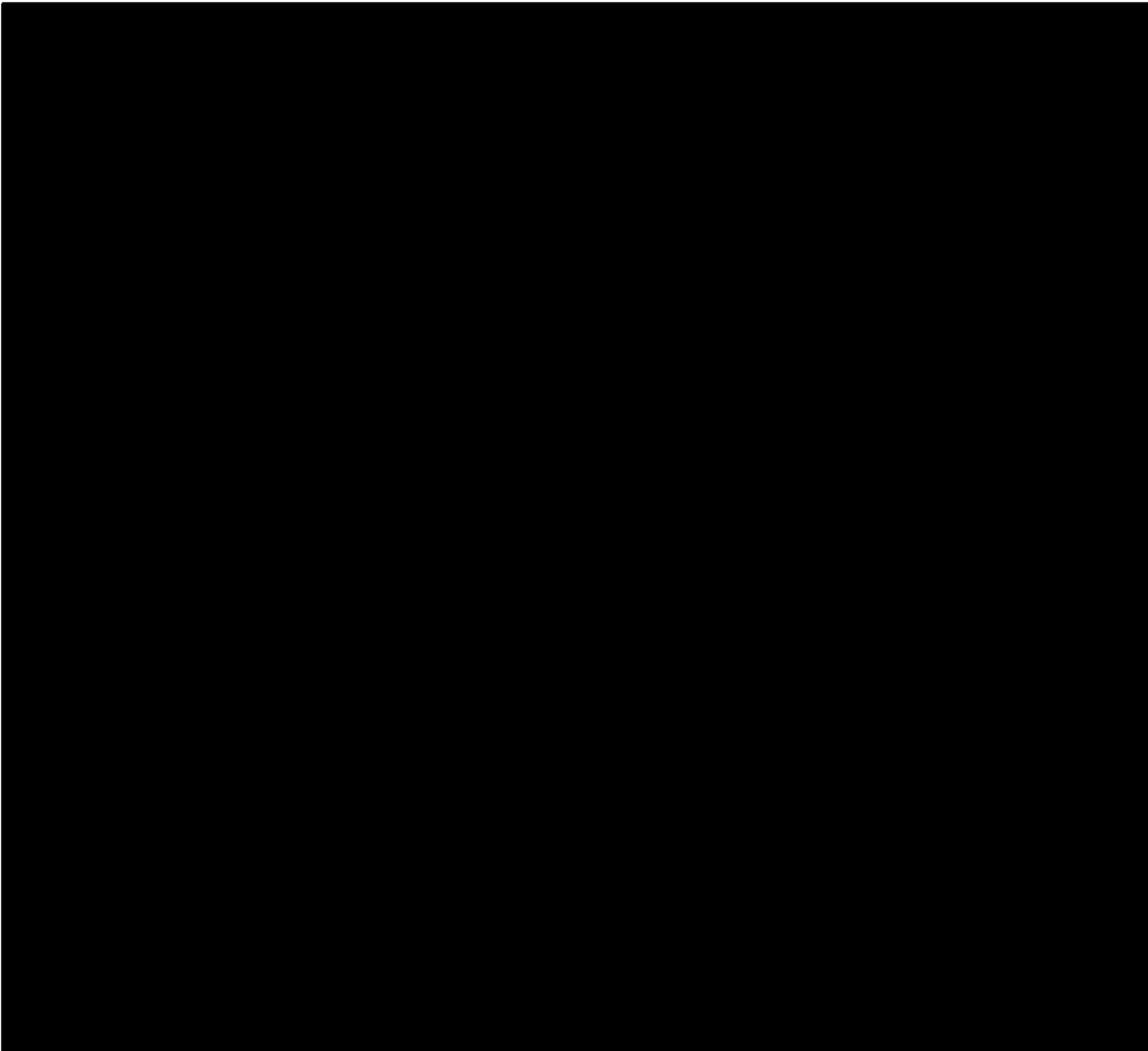
3. [REDACTED] in the United States and abroad are the subjects of National Security investigations conducted by the Federal Bureau of Investigation (FBI) under guidelines approved by the Attorney General pursuant to Executive Order No. 12333.

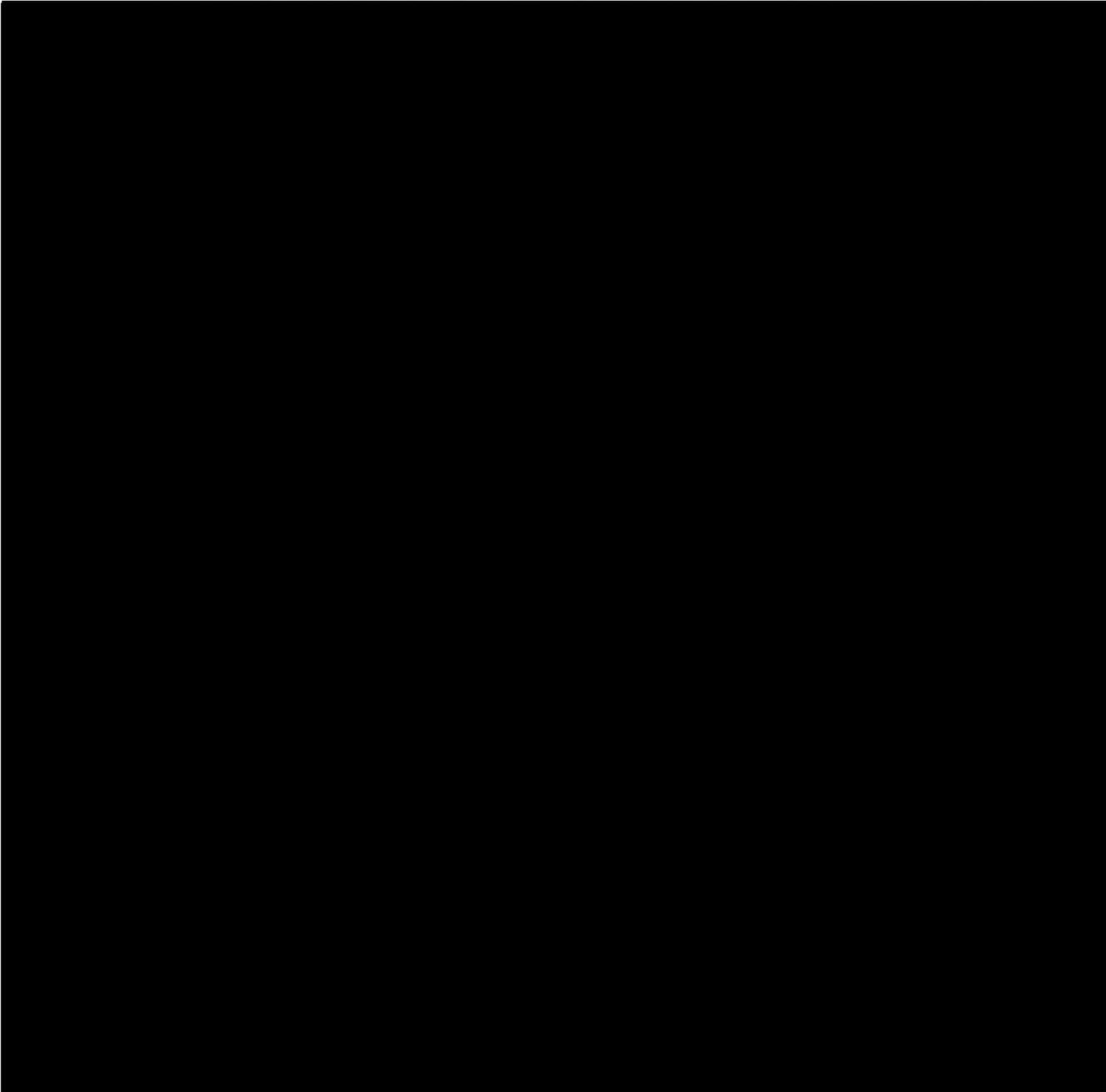
4. The pen registers and trap and trace devices [REDACTED]
[REDACTED]
[REDACTED]



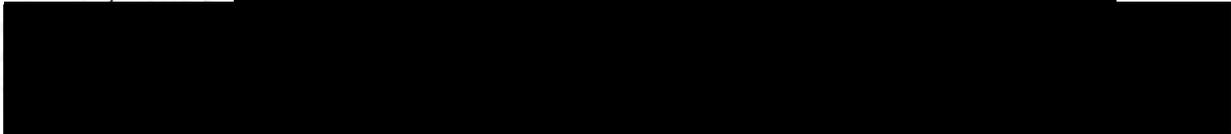
⁵¹ The Government has represented that it is overwhelmingly likely that at [REDACTED]

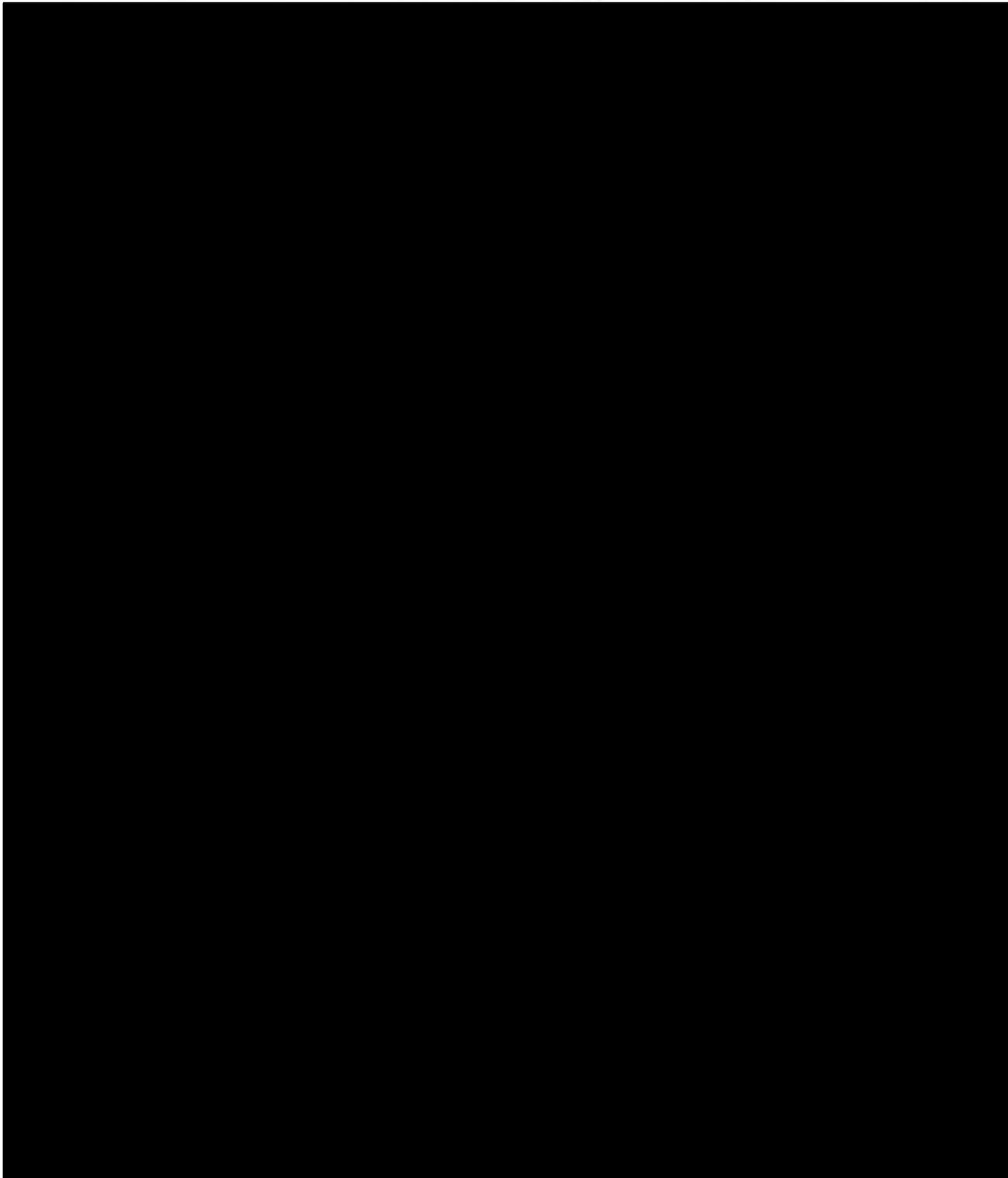
⁵² The Government has represented that it is overwhelmingly likely that [REDACTED]

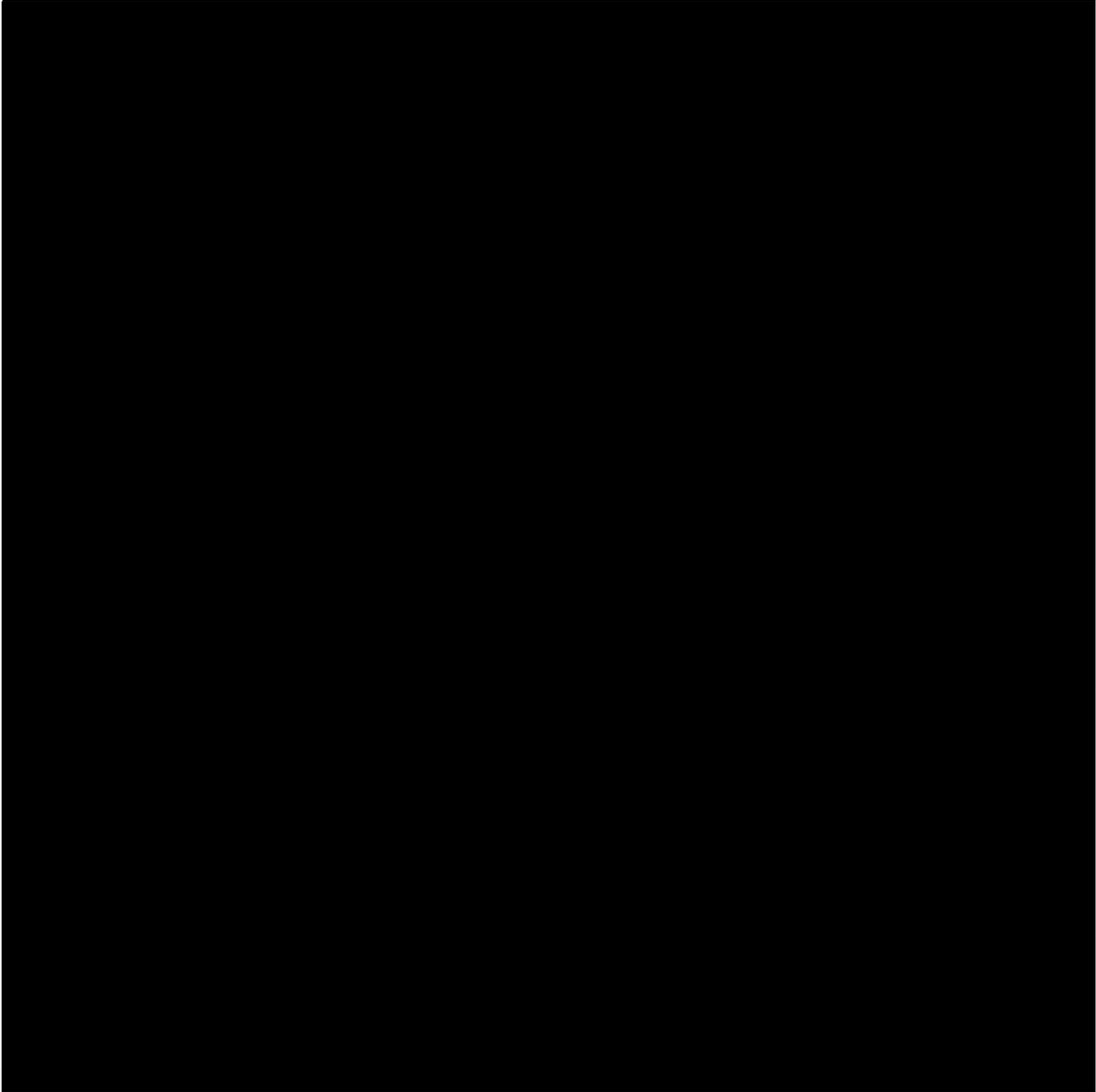




⁵³ The Government has represented that it is overwhelmingly likely that 

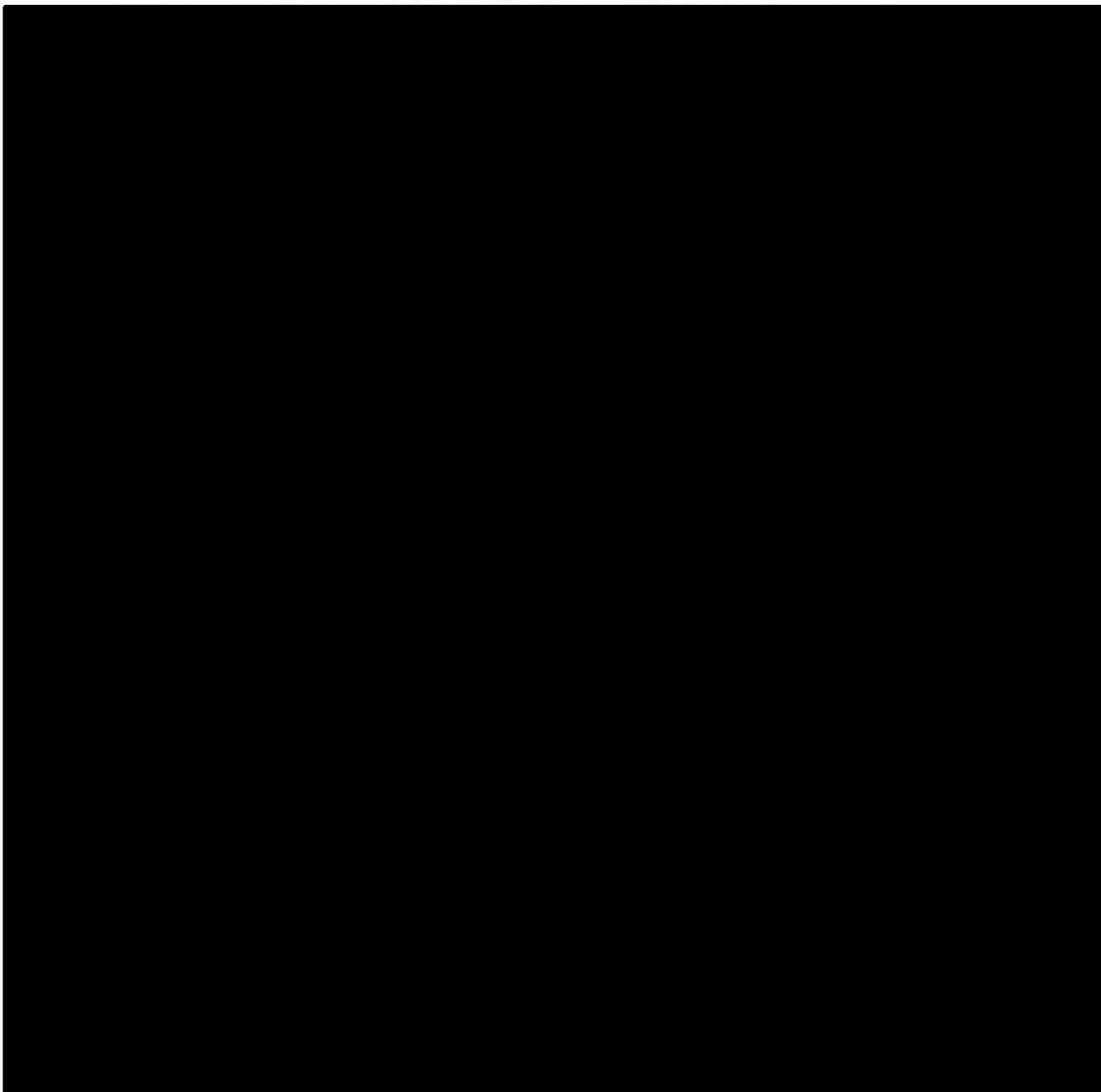




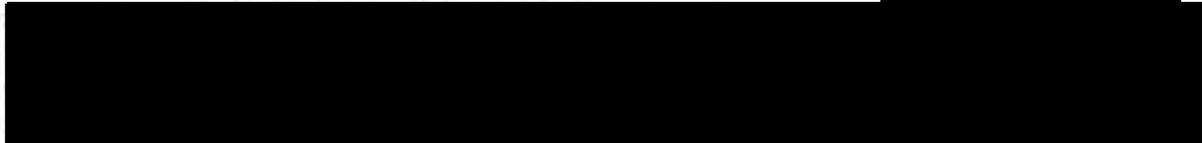


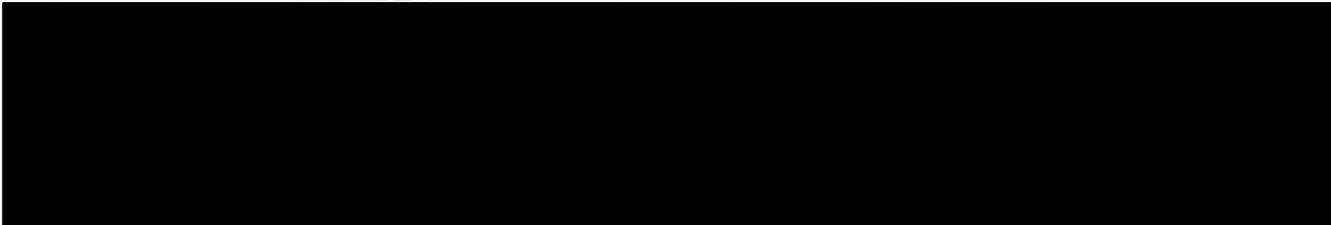
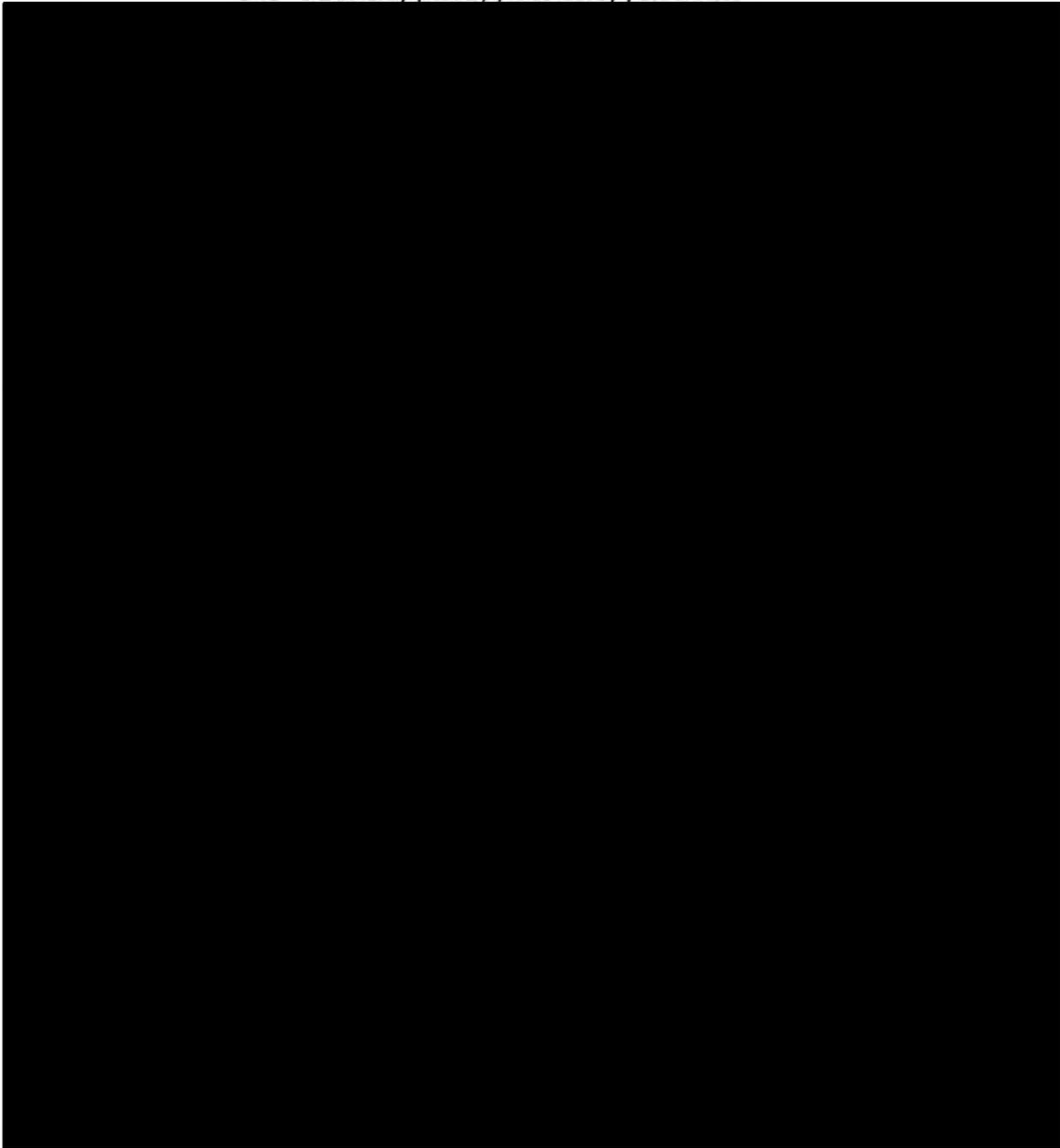
⁵⁴ The Government has represented that the majority of the communications [redacted]





⁵⁵ Because electronic communications will 







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]

[REDACTED]

[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]

[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] [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] [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] [REDACTED] provided, however, that [REDACTED] [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. 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]

[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]
[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]
[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]
[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

~~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]

[REDACTED]

Docket Number: BR 13-158

MEMORANDUM

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

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

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

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

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

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

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

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

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

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

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

Page 4

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

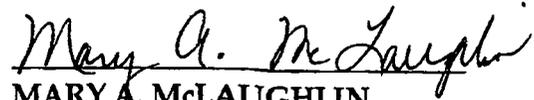
Justice Sotomayor stated in her concurring opinion in Jones that it "may be necessary" for the Supreme Court to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," which she described as "ill suited to the digital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

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

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

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

ENTERED this 11th day of October, 2013.


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

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

Page 6

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

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

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

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

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

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

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

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

FURTHER ORDERED, as follows:

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

B. The Custodian of Records of [REDACTED]

[REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

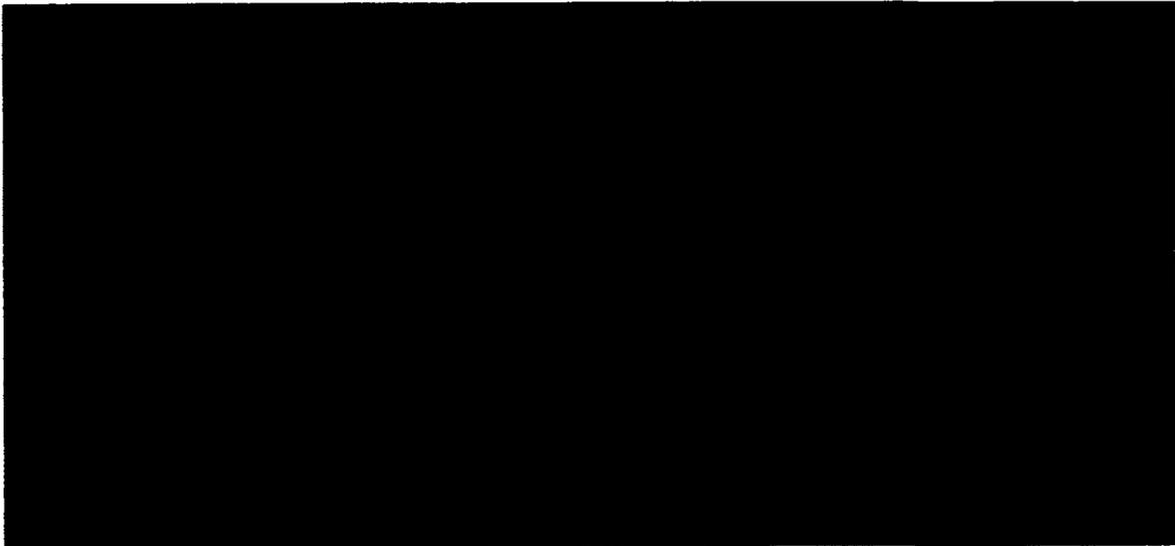
¹ For purposes of this Order "telephony metadata" includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station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

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.³

Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms⁴ that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

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

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



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

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

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

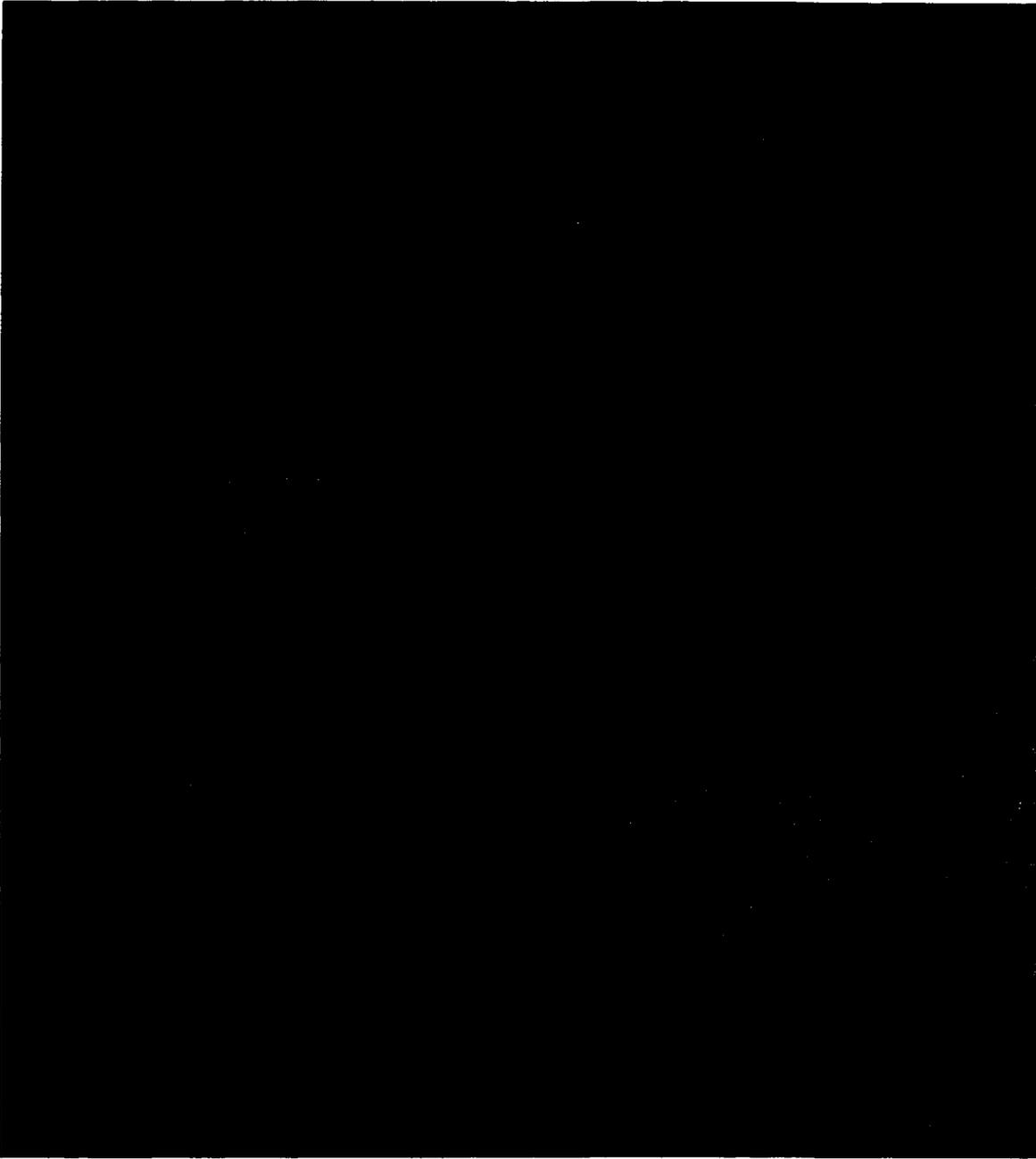
through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign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

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

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

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

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



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

shall first determine that any selection term reasonably believed to be used by a

United States (U.S.) person is not regarded as associated with [REDACTED]

[REDACTED]

[REDACTED] solely on the basis of activities that are protected by the

First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [REDACTED]

[REDACTED]

[REDACTED] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official.

The preceding sentence shall not apply to selection terms under surveillance

[REDACTED]

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

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

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

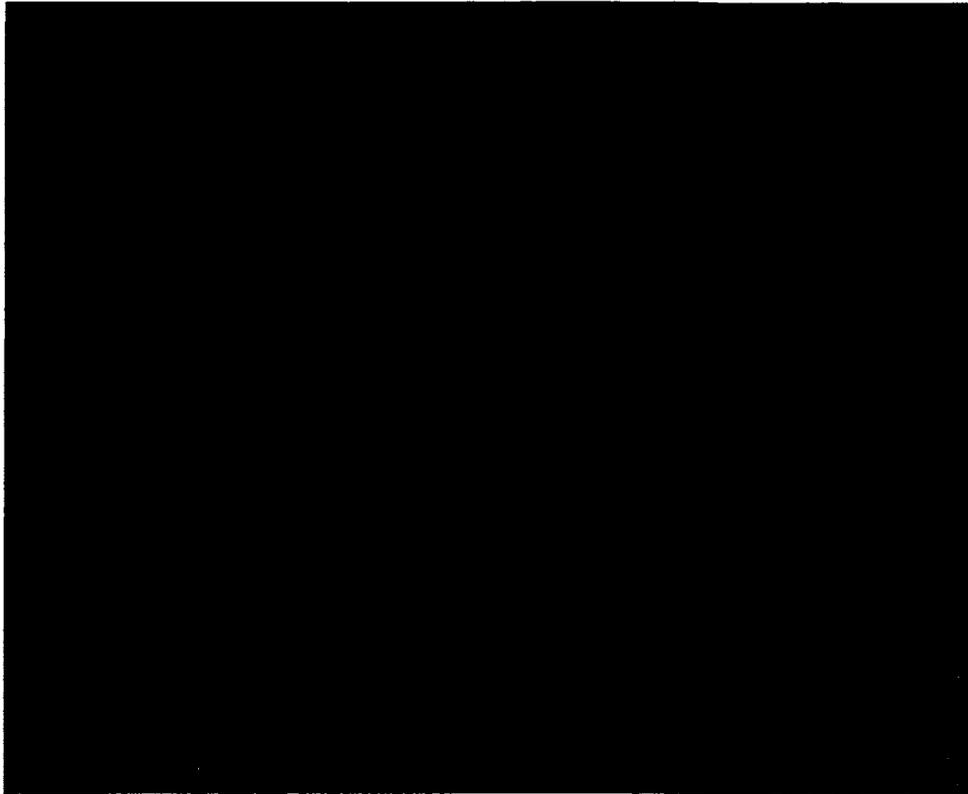
¹⁰ The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to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

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



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

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



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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This authorization regarding 

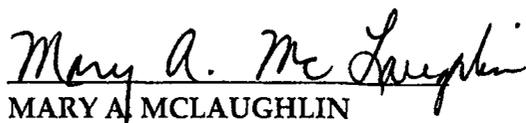


expires on the 3RD day

of January, 2014, at 5:00 p.m., Eastern Time.

Signed _____ Eastern Time
Date Time

10-11-2013 P12:05


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

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



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

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

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

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

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

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

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

Specifically, the government requested Orders from this Court to obtain certain business records of specified telephone service providers. Those telephone company business records consist of a very large volume of each company's call detail records or telephony metadata, but expressly exclude the contents of any communication; the name, address, or financial information of any subscriber or customer; or any cell site location information (CSLI). Primary Ord. at 3 n.1.⁵ The government requested production of this data on a daily basis for a period of 90 days. The sole purpose of this production is to obtain foreign intelligence information in support of [REDACTED] individual authorized investigations to protect against international terrorism and concerning various international terrorist organizations. See Primary Ord. at 2, 6; App. at 8; and, Ex. A. at 2-3. In granting the government's request, the Court has prohibited the government from accessing the data for any other intelligence or investigative purpose.⁶ Primary Ord. at 4.

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

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

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

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

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

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

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

II. Fourth Amendment.⁹

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

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

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

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

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

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

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

government. See id. at 744. Thus, the Supreme Court concluded that a person does not have a legitimate expectation of privacy in telephone numbers dialed and, therefore, when the government obtained that dialing information, it “was not a ‘search,’ and no warrant was required” under the Fourth Amendment. Id. at 746.¹³

In Smith, the government was obtaining the telephone company’s metadata of one person suspected of a crime. See id. at 737. Here, the government is requesting daily production of certain telephony metadata in bulk belonging to companies without specifying the particular number of an individual. This Court had reason to analyze this distinction in a similar context in [REDACTED]

[REDACTED] In that case, this Court found that “regarding the breadth of the proposed surveillance, it is noteworthy that the application of the Fourth Amendment depends on the government’s intruding into some individual’s reasonable expectation of privacy.” Id. at 62. The Court noted that Fourth Amendment rights are personal and individual, see id. (citing Steagald v. United States, 451 U.S. 204, 219 (1981); accord, e.g., Rakas v. Illinois, 439 U.S. 128, 133 (1978) (“Fourth Amendment rights are personal rights which ... may not be vicariously asserted.”) (quoting Alderman v. United States, 394 U.S. 165, 174 (1969))), and that “[s]o long as no individual has a reasonable expectation of privacy

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

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

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

III. Section 215.

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

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

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

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

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

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

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

It is instructive to compare Section 215, which is used for foreign intelligence purposes and is codified as part of FISA, with 18 U.S.C. § 2703 (“Required disclosure of customer communications or records”), which is used in criminal investigations and is part of the Stored Communications Act (SCA). See In Re Production of Tangible Things From [REDACTED]

[REDACTED], Docket No. BR 08-13, Supp. Op. (Dec. 12, 2008) (discussing Section 215 and Section 2703). Section 2703 establishes a process by which the government can obtain information from electronic communications service providers, such as telephone companies. As with FISA, this section of the SCA provides the mechanism for obtaining either the contents of communications, or non-content records of communications. See 18 U.S.C. §§ 2703(a)-(c).

For non-content records production requests, such as the type sought here, Section 2703(c) provides a variety of mechanisms, including acquisition through a court order under Section 2703(d). Under this section, which is comparable to Section 215, the government must offer to the court "*specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation.*" *Id.* § 2703(d) (emphasis added). Section 215, the comparable provision for foreign intelligence purposes, requires neither "specific and articulable facts" nor does it require that the information be "material." Rather, it merely requires a statement of facts showing that there are reasonable grounds to believe that the records sought are relevant to the investigation. *See* 50 U.S.C. §1861(b)(2)(A). That these two provisions apply to the production of the same type of records from the same type of providers is an indication that Congress intended this Court to apply a different, and in specific respects lower, standard to the government's Application under Section 215 than a court reviewing a request under Section 2703(d). Indeed, the pre-PATRIOT Act version of FISA's business records provision required "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." 50 U.S.C. §1862(b)(2)(B) as it read on October 25, 2001.¹⁶ In enacting Section 215,

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

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

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

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

provided a specific and complex statutory scheme for judicial review of an Order from this Court to ensure that providers could challenge both the legality of the required production and the nondisclosure provisions of that Order. 50 U.S.C. § 1861(f). This adversarial process includes the selection of a judge from a pool of FISC judges to review the challenge to determine if it is frivolous and to rule on the merits, *id.* § 1861(f)(2)(A)(ii), provides standards that the judge is to apply during such review, *id.* §§ 1861(f)(2)(B)-(C), and provides for appeal to the Foreign Intelligence Surveillance Court of Review and, ultimately, the U.S. Supreme Court, *id.* § 1861(f)(3).¹⁷ This procedure, as opposed to the motion process available under Section 2703(d) to challenge a production as unduly voluminous or burdensome, contemplates a substantial and engaging adversarial process to test the legality of this Court's Orders under Section 215.¹⁸ This enhanced process appears designed to ensure that there are additional safeguards in light of the lower threshold that the government is required to meet for production under Section 215 as opposed to Section 2703(d). To date, no holder of

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

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

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

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

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

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

b. Relevance.

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

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

Things for Investigations to Protect Against International Terrorism, Docket No. BR 06-05 (filed May 23, 2006), at 13-14 (quoting dictionary definitions, Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351 (1978), and Fed. R. Evid. 401²⁰). This Court recognizes that the concept of relevance here is in fact broad and amounts to a relatively low standard.²¹ Where there is no requirement for specific and articulable facts or materiality, the government may meet the standard under Section 215 if it can demonstrate reasonable grounds to believe that the information sought to be produced has some bearing on its investigations of the identified international terrorist organizations.

This Court has previously examined the issue of relevance for bulk collections.

See [REDACTED]

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

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

[REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED]

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

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

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

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

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

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

c. Legislative Re-enactment or Ratification.

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

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

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

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

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

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

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

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

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

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

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

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

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

IV. Conclusion.

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

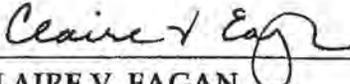
As discussed above, because there is no cognizable Fourth Amendment interest in a telephone company's metadata that it holds in the course of its business, the Court finds that there is no Constitutional impediment to the requested production. Finding no Constitutional issue, the Court directs its attention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

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

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

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

ENTERED this 29th day of August, 2013.



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

~~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]

[REDACTED]

Docket Number: BR 13-109

PRIMARY ORDER

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

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

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

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

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

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

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

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

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

FURTHER ORDERED, as follows:

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

B. The Custodian of Records of [REDACTED]

[REDACTED]
[REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

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

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

[REDACTED]

[REDACTED]

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

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

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

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

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

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.³

Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms⁴ that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

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

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

⁴ [REDACTED]

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

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

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

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

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

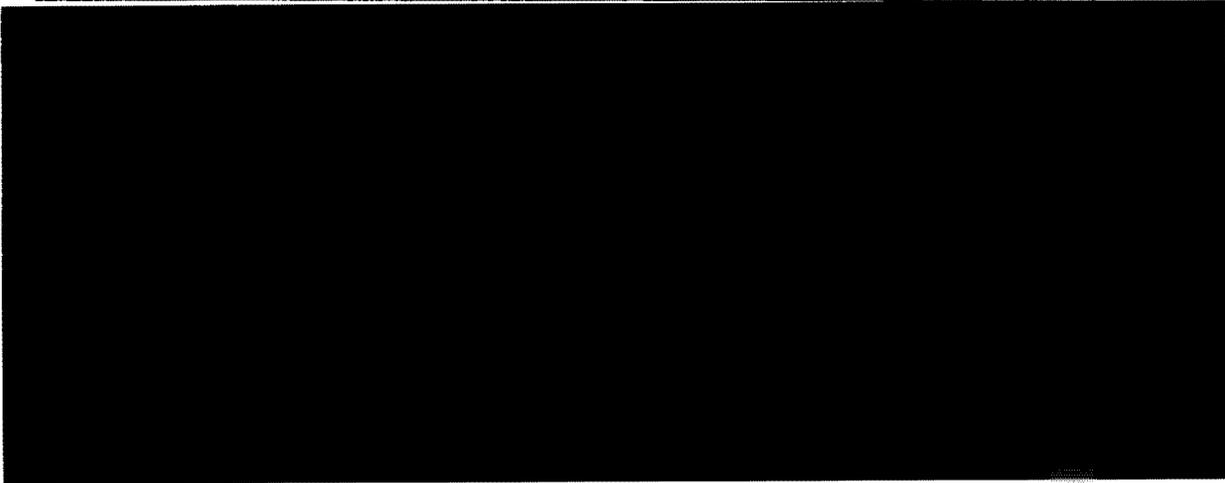
⁶ This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

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

[REDACTED]

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

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



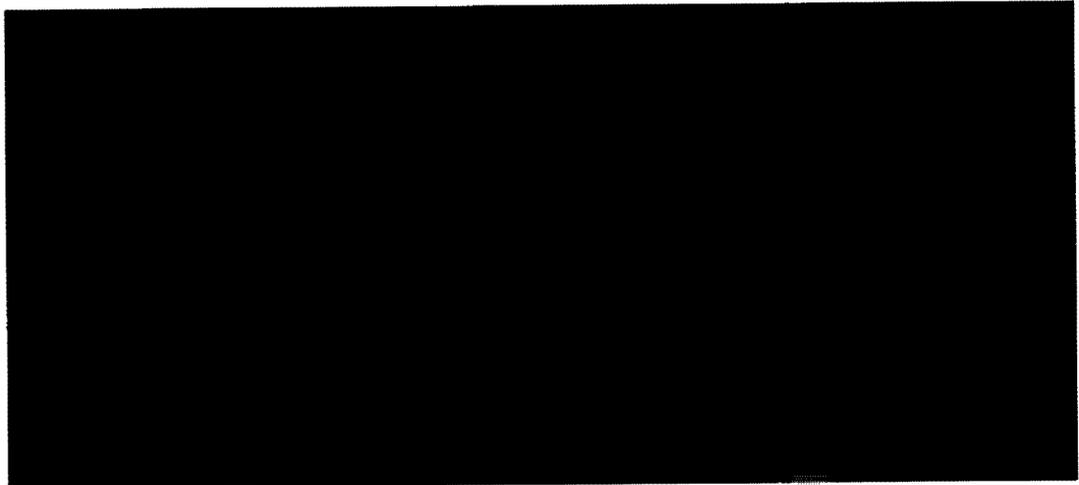
pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

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

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

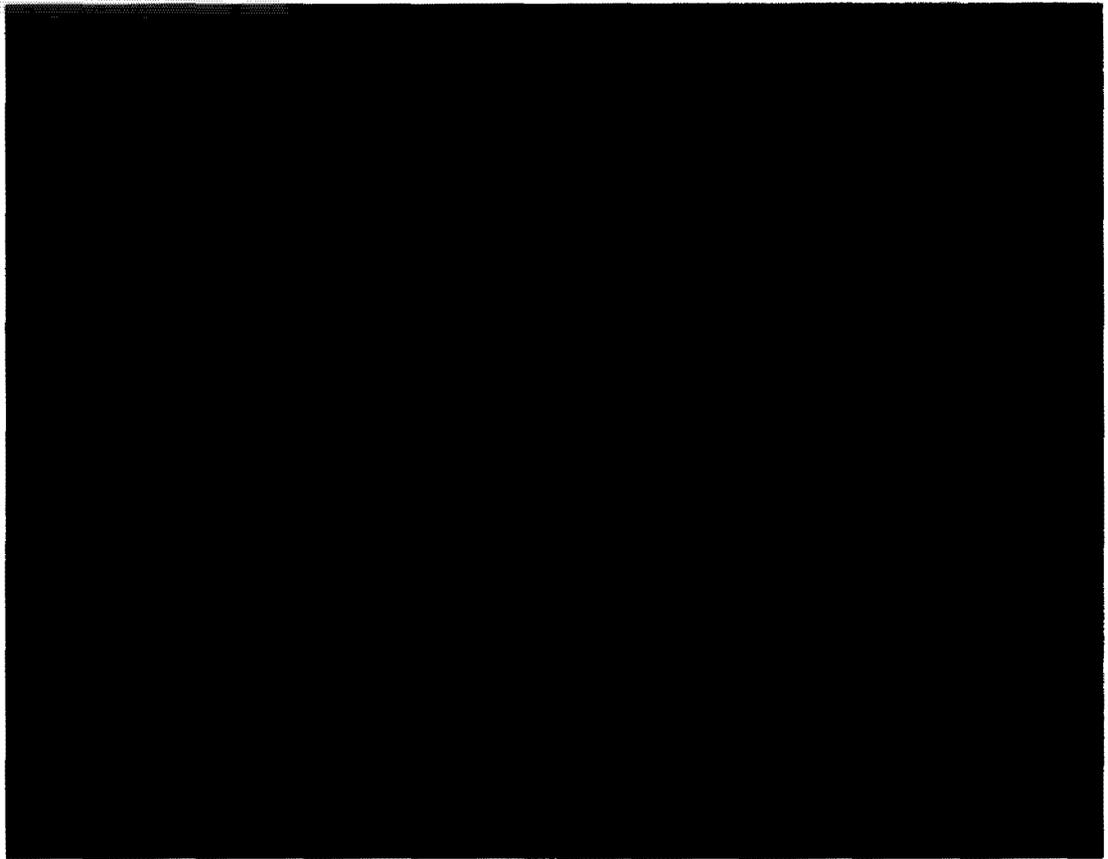
¹⁰ The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to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

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



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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This authorization regarding [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] expires on the 11th day

of October, 2013, at 5:00 p.m., Eastern Time.

Signed _____ Eastern Time
Date Time
10-19-13 10:45

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



CSU
DATE: 4.25.08~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

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

IN RE DIRECTIVES TO YAHOO!, INC.

Docket Number 105B(g): 07-01

PURSUANT TO SECTION 105B OF THE
FOREIGN INTELLIGENCE SURVEILLANCE
ACT

MEMORANDUM OPINION

Background

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

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

Page 1

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

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

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

¹ [redacted]

² Each directive states that

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

(continued...)

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

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

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

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

²(...continued)

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

Feb. 2008 Classified Appendix at [REDACTED]

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

(continued...)

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

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

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

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

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

³(...continued)

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

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

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

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

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

Analysis

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

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

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

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

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

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

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

Section 6 of the PAA, as amended, states in relevant part:

(c) SUNSET.—Except as provided in subsection (d), sections 2, 3, 4, and 5 of this Act, and the amendments made by this Act, shall cease to have effect 195 days after the date of the enactment of this Act.

(d) AUTHORIZATIONS IN EFFECT.—Authorizations for the acquisition of foreign intelligence information pursuant to the amendments made by this Act, and directives issued pursuant to such authorizations, shall remain in effect until their expiration. Such acquisitions shall be governed by the applicable provisions of such amendments and shall not be deemed to constitute electronic surveillance as that term is defined in [50 U.S.C.A. § 1801(f)].

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

prior judicial decisions, whether a surveillance¹⁰ comports with the Fourth Amendment. Id. at 21-23.

As authority for its separation of powers objection, Yahoo cites Doe v. Gonzales, 500 F. Supp. 2d 379 (S.D.N.Y. 2007), which involved First Amendment challenges to non-disclosure obligations imposed on the recipient of a national security letter (NSL) under 18 U.S.C.A. § 2709 (West 2000 & Supp. 2007). In Doe, the separation of powers concerns derived from 18 U.S.C.A. § 3511(b) (West Supp. 2007), which governs the scope and standard of review to be applied by a district court when the recipient of an NSL petitions for relief from the non-disclosure obligations. 500 F. Supp. 2d at 409, 411-13.¹¹ Employing one of the quintessential tenets of separation of powers jurisprudence – that “Congress cannot legislate a constitutional standard of review that contradicts or supercedes what the courts have determined to be the standard applicable under the First Amendment for that purpose,” Doe, 500 F. Supp. 2d at 411 (citing Dickerson v. United States, 530 U.S. 428, 437 (2000); Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803)) – the Doe court invalidated certain aspects of § 3511(b).¹²

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

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

(continued...)

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

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

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

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

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

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

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

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

this Court.” Yahoo’s Mem. in Opp’n at 23.¹³ Another judge of the FISC acknowledged this ambiguity when reviewing the government’s procedures under § 1805c(b). See In re DNI/AG Certifications [REDACTED] Memorandum Opinion and Order entered January 15, 2008 (In re DNI/AG Certifications) at 6-8. However, that judge, after applying ordinary principles of statutory construction, concluded that for the types of acquisition pertinent to this case, the statute should be understood to require that the procedures be “reasonably designed to ensure that the users of tasked facilities^[14] are reasonably believed to be outside of the United States.” Id. at 15. This understanding of the statutory requirement is also adopted here, for the reasons stated in In re DNI/AG Certifications.¹⁵ Because this ambiguity can be resolved by such

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

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

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

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

(continued...)

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

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

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

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

¹⁵(...continued)

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

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

Despite these interpretative difficulties, it seems clear that procedures will satisfy the relevant statutory requirements if they are reasonably designed to ensure both

(1) that such acquisitions do not constitute "electronic surveillance," because they are surveillance directed at persons reasonably believed to be outside of the United States, and

(2) that the acquisitions of foreign intelligence information concern persons reasonably believed to be located outside of the United States.

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

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

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

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

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

With this background, the Court returns to Yahoo's second argument.

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

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

¹⁸ See Feb. 2008 Classified Appendix at [REDACTED]

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

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

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

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

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

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

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

Third, Yahoo challenges the directives, arguing that, under section 6(c)-(d) of the PAA, it remains obligated to comply with the directives for up to one year, even though the protection of immunity provided to it by the legislation may not apply by virtue of the lapse of 50 U.S.C.A. § 1805b(1). Yahoo's Mem. in Opp'n at 24. In response, the government asserts that the immunity provision remains in effect throughout the life of the directives. Memorandum in Support of Government's Motion to Compel (Mem. in Support of Gov't Motion) at 24 n.22. For essentially the same reasons that support the Court's holding that § 1805b(g) remains in effect with regard to the directives at issue by operation of § 6(d) of the PAA, see supra Part I, the Court finds that § 6(d) also preserves the operability of the immunity provision of § 1805b(1). Not only does § 1805b(1) fit comfortably within the preserving language of § 6(d), but it would be wholly illogical for Congress to have initially afforded civil immunity to the recipients of directives, only to have it subsequently extinguished even though the obligation to comply with the directives remains in effect.²⁰

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

²⁰ Moreover, in Yahoo's case, any assistance rendered will be pursuant to this Court's (continued...)

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

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

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

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

²⁰(...continued)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

²²



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(continued...)

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

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

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

The government correctly observes that the FISC has granted motions by the government to amend a previously issued primary order – for example, to approve modified minimization procedures. Govt.'s Resp. to Feb. 29 Order at 9-11 (discussing, e.g.,

[REDACTED]

In such cases, the

FISC has sometimes amended primary orders without amending secondary orders, see, e.g.,

[REDACTED]

based on the implicit understanding that the efficacy of previously issued secondary orders was not undermined by the amendment. As a general rule, the FISC has issued new or amended secondary orders to a third party who is already subject to an extant secondary order in the same docket only when the primary order has been amended in a way that changes the nature or scope of the assistance to be provided – for example, when the amendment authorizes surveillance of a new facility that was beyond the scope of the original orders. See,

e.g., [REDACTED]

²⁸(...continued)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Secondly, Yahoo notes that the recipient of a directive does not have access to the underlying certification and procedures. Yahoo's Supp. Brief. on Stat. Issues at 10.³³ Yahoo

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

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

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

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

³³(...continued)
Classified Appendix at 

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

³⁸ Compare [REDACTED]

[REDACTED] Each directive states that it encompasses information [REDACTED]

[REDACTED] The directives provide a more detailed description of the information sought from Yahoo than the certifications do, but the information described by the directives does not extend beyond the authorization in each certification to obtain “foreign intelligence information from or with the assistance of communications service providers . . . who have access to communications, [REDACTED]

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

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

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

As described above, see supra notes 17-18 and accompanying text, the government also amended all [REDACTED] certifications to adopt additional procedures under § 1801b(a)(1) for the acquisition of [REDACTED] by the FBI. See Feb. 2008 Classified Appendix at [REDACTED]

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

³⁹ The minimization procedures for [REDACTED]

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

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

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

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

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

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

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

⁴⁰(...continued)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

was issued in accordance with subsection (e) and is otherwise lawful.” *Id.* (emphasis added),⁴⁴

The plain reading of this language leads the Court to the conclusion that a government directive to Yahoo that violates the Fourth Amendment is not “otherwise lawful,” regardless of whose Fourth Amendment rights are being violated.⁴⁵

Moreover, in the context of a statute that authorizes the government to acquire the contents of communications to and from United States persons⁴⁶ without their knowledge or consent, the protections provided by the Fourth Amendment are critically important. *See, e.g., United States v. United States District Court*, 407 U.S. 297 (1972); *Katz v. United States*, 389 U.S. 347 (1967). In this context especially, the expansive language that Congress used to

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

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

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

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

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

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

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

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

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

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

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

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

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

⁴⁸(...continued)

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

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

- Page 47

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(continued...)

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

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

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

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

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

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

⁵²(...continued)

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

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

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

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

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

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

Yahoo contends⁵³ (and the government has not argued to the contrary) that “the people” protected by the Fourth Amendment include not only United States citizens located within the country’s boundaries, but also United States citizens abroad as well, see United States v. Bin Laden, 126 F. Supp. 2d 264, 270-71 (S.D.N.Y. 2000) (Fourth Amendment protects American citizen in Kenya), and that the directives may sweep up communications to which a United States citizen is a party.⁵⁴ The Court assumes that United States citizens (and other United States persons, as well) will have a reasonable expectation of privacy in at least some of these communications, even though the scope of Fourth Amendment protection for email communications is not a settled

⁵³See Yahoo’s Mem. in Opp’n at 6-8.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

As noted above, the government subsequently filed amended certifications, which the Court has concluded encompass the directives issued to Yahoo. The amended certifications provide that "[a]ny time the acquisition of foreign intelligence information against a U.S. person abroad is sought pursuant to the above-referenced certification, Attorney General authorization, pursuant to the procedures under Executive Order 12333, section 2.5, must first be obtained." Feb. 2008 Classified Appendix at [REDACTED] Although the language in both the original and amended certifications is similar, the original certifications specify that it is "NSA" that must obtain the authorization from the Attorney General. The amendment was made presumably because the original certifications envisioned that the acquisitions would be accomplished by the NSA, while under the amended certifications the FBI also plays a role in securing some acquisitions. In any event, it seems reasonably clear that, under both the original and amended certifications, Attorney General authorization is required for all acquisitions targeting U.S. persons abroad, pursuant to "the procedures" under section 2.5 of E.O. 12333.⁶³

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

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

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

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

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

Section 2.5 of E.O. 12333 is a delegation to the Attorney General from the President to approve the use of certain techniques for intelligence collection purposes, "provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power." E.O. 12333, § 2.5.⁶⁴ As for "the procedures" under section 2.5 referenced in the certifications, the government's memorandum in support of its motion to compel identifies the Department of Defense Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, DoD 5240.1-R (1982) (DoD Procedures), as the applicable procedures.

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

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

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

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

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

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

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

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

surveillance⁶⁶ against a United States person who is physically outside of the United States for foreign intelligence or counterintelligence purposes unless the surveillance is approved by the Attorney General. Although it does not specifically use the term "agent of a foreign power," Procedure 5, Part 2.C provides what is tantamount to such a definition. Specifically, it requires that a request for Attorney General approval contain a statement of facts supporting a finding of probable cause that the target of the electronic surveillance is one of the following:

- (1) A person who, for or on behalf of a foreign power is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, or activities in preparation for international terrorist activities; or who conspires with, or knowingly aids and abets a person engaging in such activities;
- (2) A person who is an officer or employee of a foreign power;
- (3) A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;
- (4) A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
- (5) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to

⁶⁶ "Electronic surveillance" is defined under the DoD Procedures (Appendix A) as the

[a]cquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication, or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter. (Electronic surveillance within the United States is subject to the definitions in the Foreign Intelligence Surveillance Act of 1978 (reference (b)).)

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

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

information or material classified by the United States to which such person has access.^[67]

In the context of the certifications at issue, the question becomes whether a finding of probable cause by the Attorney General that comports with Procedure 5, Part 2.C, is sufficient to invoke the foreign intelligence exception to the Warrant Clause. The Court finds that the answer is yes for the following reasons.

First, the Attorney General is an appropriate official to make the probable cause finding. See United States v. Bin Laden, 126 F. Supp. 2d at 279 & n.18. Second, the descriptions in Procedure 5, Part 2.C, regarding what makes a United States person an acceptable target (i.e., an agent of a foreign power), themselves pass muster. Certainly in common sense terms, a United States person who falls into any of the five categories can reasonably be believed to be an "agent" of a foreign power.⁶⁸ Moreover, it also seems clear that categories 1, 3, and 5 suffer from no constitutional or other legal infirmities. See In re Sealed Case, 310 F.3d at 719 (U.S. citizen target was an agent of a foreign power because there was probable cause that he or she was

⁶⁷ Procedure 7.C, which is applicable to physical searches, contains materially identical language as to a showing of probable cause concerning the target.

⁶⁸ The Procedures independently define a "foreign power" as "[a]ny foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities." DoD Procedures, Appendix A. However, the particular foreign powers at issue here are further constrained by the certifications, which by their terms are directed at


cf. 50 U.S.C.A. § 1801(a)(1) & (a)(4) (defining "foreign power" under FISA as including foreign governments, as well as groups engaged in international terrorism or activities in preparation for international terrorism).

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

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

aiding, abetting, or conspiring with others in international terrorism); Bin Laden, 126 F. Supp. 2d at 278 (agent of al Qaeda). Similarly, to the extent the certifications contemplate targeting entities abroad as agents, the Court finds it unlikely that category four has any constitutional impediments either, at least not in the context of the foreign powers at issue (see supra note 68). Cf. 50 U.S.C.A. § 1801(a)(6) (even for purposes of a FISA order within the United States, the term "foreign power" includes an entity directed and controlled by a foreign government or governments). Finally, the second category admittedly does go beyond what FISA permits the government to do in the United States, cf. 50 U.S.C.A. § 1801(b)(1)(A) (limiting definition of "agent of foreign power" to a non-U.S. person acting in the U.S. as an officer or employee of a foreign power). Nonetheless, the Court concludes that it is constitutionally appropriate for the government to acquire for foreign intelligence purposes the communications of a United States person abroad who is acting as an officer or employee of a foreign government or terrorist group. Indeed, were it otherwise, then the United States government would be routinely prevented from obtaining necessary foreign intelligence [REDACTED]

[REDACTED] Such a result would be untenable.

Based on the above analysis, the Court holds that the foreign intelligence exception to the warrant requirement is applicable to the directives issued to Yahoo. The Court must therefore address whether the directives are reasonable under the Fourth Amendment.

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

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

2. The Directives are Reasonable Under the Fourth Amendment

The Fourth Amendment analysis merely begins with the finding that the government need not obtain a warrant to acquire the communications it seeks to obtain from Yahoo through the issuance of directives. In order for those directives to comport with the Fourth Amendment, they must also be reasonable. United States v. Knights, 534 U.S. 112, 118-19 (2001) (“The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined ‘by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.’” (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))). And, to assess the reasonableness of the directives issued to Yahoo pursuant to the PAA, this Court must examine the totality of the facts and circumstances. Samson v. California, 547 U.S. 843, 848 (2006); Ohio v. Robinette, 519 U.S. 33, 39 (1996).

The acquisitions at issue in this case present this Court with the challenge of balancing the government’s interest in acquiring foreign intelligence information against the privacy interests of those United States persons whose communications will be acquired.⁶⁹ There is little doubt about the weightiness of the government’s interest, as this Court accepts the government’s assertion that the information it seeks to acquire from Yahoo would “advance the government’s compelling interest in obtaining foreign intelligence information to protect national security. . . .”

⁶⁹The foreign intelligence that the government seeks to obtain from Yahoo is not limited to the communications of United States persons. Indeed, there is every reason to assume that most of the accounts that will be targeted will be ones used by non-United States persons overseas who do not enjoy the protections of the Fourth Amendment. See *supra* note 60.

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

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

Mem. in Support of Gov't Motion at 14; see also Gov't.'s Supp. Brief on the Fourth Amend. at 6 ("... It is obvious and unarguable that no government interest is more compelling than the security of the Nation." (citing Haig v. Agee, 453 U.S. 280, 307 (1981))).

In furtherance of this objective, the government seeks to obtain from Yahoo communications that include communications to or from United States persons. See supra note 54. The directives at issue require Yahoo to provide to the government a [REDACTED] information relating to targeted accounts, [REDACTED]

Declaration of [REDACTED] January 16, 2008; Declaration of [REDACTED] January 23, 2008 at 2 (noting, however, Yahoo's understanding that, at least initially, the government would only expect Yahoo to produce [REDACTED])

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

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

[REDACTED] Declaration of [REDACTED] January 23, 2008.⁷⁰ As noted above, the government concedes that at least some of this information is protected by the Fourth Amendment, and there is no question that extremely sensitive, personal information could be acquired through the directives, akin to electronic eavesdropping of telephone conversations.

Thus, unlike those circumstances involving a disparity between the importance of the government's interest and the degree of intrusiveness required to serve that interest, *see, e.g., United States v. Martinez-Fuerte*, 428 U.S. 543, 557-58 (1976) (analyzing traffic stops in which the government need is great but the intrusion is minimal), here there are weighty concerns on both sides of the equation. This Court, however, is not the first to assess the reasonableness of [REDACTED] surveillance.⁷¹ Since the enactment of the Foreign Intelligence Surveillance Act, two particularly significant opinions have examined the Fourth Amendment reasonableness of the acquisition by the government of foreign intelligence information through the interception of communications of United States persons: the FISC in *In re Sealed Case*, 310 F.3d 717 and the United States District Court for the Southern District of New York in *United States v. Bin Laden*, 126 F. Supp. 2d 264.

⁷⁰As may be obvious by the enumeration, this acquisition also will obtain [REDACTED] [REDACTED] communications of those persons who send communications to or receive communications from targeted accounts, regardless of whether these communicants are located outside the United States and without regard to whether such individuals are agents of foreign powers. *See infra* Part III.B.2.e for a further discussion of these communications.

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

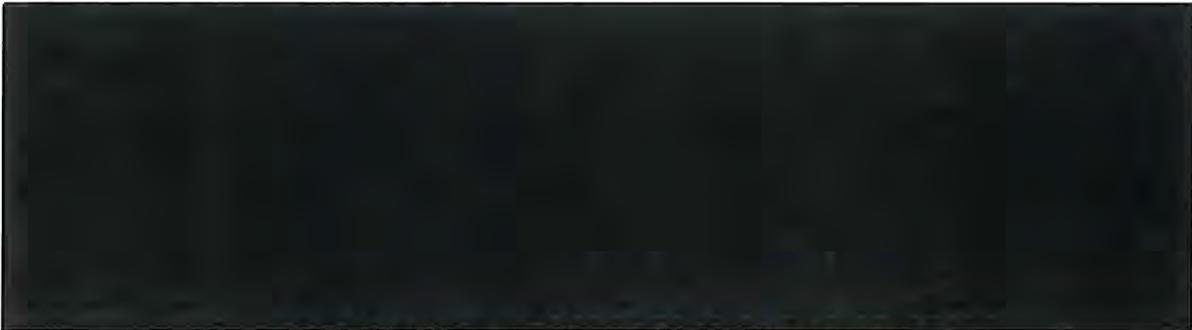
~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

In determining the reasonableness of the acquisition at issue here, this Court will look to the factors considered by both courts, even though the facts of this case more closely resemble those presented in Bin Laden. However, because this Court is bound by the holding in In re Sealed Case, it must accord special consideration to that case in determining the extent to which the FISCRC findings are applicable to a case such as this one, involving surveillance of United States persons abroad rather than within the boundaries of the United States.

a. In re Sealed Case

In re Sealed Case involved electronic surveillance conducted in the United States of the  communications of a United States person located in the United States.⁷² As noted above, the FISCRC implicitly found that the FISA orders fell within the parameters of the foreign intelligence exception to the warrant requirement. But, as this Court is also required to do, the FISCRC closely examined various facts and circumstances to determine whether the issuance of those orders was reasonable under the Fourth Amendment. In re Sealed Case, 310 F.3d at 736-42.

The FISCRC began its reasonableness analysis by looking to the requirements for the issuance of a warrant: issuance by a neutral detached magistrate, demonstration of probable



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

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

cause, and particularity. *Id.* at 738. The FISCRC compared the procedural framework of the surveillance at issue in that case with the procedures required by the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C.A. § 2510 *et seq.* (West 2000 & Supp. 2007) (Title III)⁷³ and noted that to the extent a FISA order differed from a Title III order, “few of those differences have any constitutional relevance.” *Id.* at 737. While it appears that the FISCRC determined that the three factors recited above were the essential factors to consider in assessing the constitutionality (and hence, the reasonableness) of a FISA order, the FISCRC also analyzed several other factors noting, “[t]here are other elements of Title III that at least some circuits have determined are constitutionally significant - that is, necessity, duration of surveillance, and minimization.” *Id.* at 740 (citation omitted). The following factors all appear to have been considered by the FISCRC in determining that the FISA orders were reasonable under the Fourth Amendment.

i. Prior Judicial Review

The FISCRC assessed that Title III and FISA were virtually identical so far as the requirement for prior judicial approval. As such, the FISCRC devoted little attention to analyzing this factor. However, given that the FISCRC highlighted prior judicial review as one of the three essential requirements of the Fourth Amendment Warrant Clause, it seems apparent that the FISCRC considered this to be a critical element in its reasonableness assessment.

⁷³ “[I]n asking whether FISA procedures can be regarded as reasonable under the Fourth Amendment, we think it is instructive to compare those procedures and requirements with their Title III counterparts. Obviously, the closer those FISA procedures are to Title III procedures, the lesser are our constitutional concerns.” *In re Sealed Case*, 310 F.3d at 737.

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

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

ii. Probable Cause

The FISCER noted that orders issued pursuant to FISA and Title III required different probable cause findings. Under FISA, the FISC need only find probable cause to believe "that the target is a foreign power or an agent of a foreign power," *id.* at 738 (citing 50 U.S.C.A. § 1805(a)(3)), while Title III requires "'probable cause for belief that an individual is committing, has committed, or is about to commit' a specified predicate offense," *id.* (quoting 18 U.S.C.A. § 2518(3)(a)). The FISCER acknowledged that while the FISA probable cause showing was not as great as that required under Title III, FISA incorporated "another safeguard not present in Title III," *id.* at 739 - a probable cause requirement, if the target is an agent, that "the target is acting 'for or on behalf of a foreign power'," *id.* The FISCER concluded that the import of this additional showing is that it would ensure that FISA surveillance was only authorized to address, "certain carefully delineated, and particularly serious, foreign threats to national security." *Id.*

iii. Particularity

In addressing particularity, the FISCER focused on two components: one concerning the nature of the communications to be obtained through the surveillance and the second concerning the relationship between the facilities to be targeted and the activity or person being investigated. *Id.* at 739-40. With regard to the former, FISA mandates that a senior executive branch official⁷⁴ certify the purpose of the surveillance, including the type of foreign intelligence information

⁷⁴FISA identifies the officials authorized to make certifications as "the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate." 50 U.S.C.A. § 1804(a)(7).

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

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

sought. 50 U.S.C.A. § 1804(a)(7). The FISC judge considering the application is obliged to grant such certification great deference. *Id.* at 739. Only when the target is a United States person does the FISC even make a substantive finding concerning that certification and even then, the standard of review is merely clear error. 50 U.S.C.A. § 1805(a)(5).⁷⁵

The findings made with regard to the facilities to be targeted are significantly different between the two statutes. Under FISA, the FISC must find probable cause to believe that the target is using or about to use the targeted facility, without regard to the purpose for which the facility will be used by the target. 50 U.S.C.A. § 1805(a)(3)(B); compare 18 U.S.C.A. § 2518(3)(d). As the FISCR noted, “[s]imply put, FISA requires less of a nexus between the facility and the pertinent communications than Title III, but more of a nexus between the target and the pertinent communications.” *Id.* at 740.

iv. Necessity

The FISCR noted that while both statutes impose a necessity requirement, under FISA the assessment of necessity is made by the above-mentioned certifying official (a requirement not mandated by Title III), albeit subject to the above-described deferential standard of judicial review. *Id.* at 740.

v. Duration

Both statutes also address the length of time orders may remain in effect. FISA permits a longer duration than does Title III, but the FISCR found the difference between 30 days and 90

⁷⁵Title III, on the other hand, requires that a judge make a probable cause finding that particular communications concerning the offense will be obtained. 310 F.3d at 739 (citing 18 U.S.C.A. § 2518(3)(b)).

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

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

days to be reasonable in light of the "nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information.'" Id. (citations omitted). The FISCR took further comfort in the fact that "the longer surveillance period is balanced by continuing FISC oversight of minimization procedures during that period." Id.

vi. Minimization

Finally, in addressing the requirement for minimization that is embodied in both statutes, the FISCR acknowledged that Title III focuses on minimization at the time of acquisition (thus, more effectively protecting the privacy interests of non-target communications), while FISA permits minimization at both the acquisition and retention stages. Id. at 740. This discrepancy, according to the FISCR, "may well be justified[.] . . . Given the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots." Id. at 741.⁷⁶

In summary, the FISCR relied upon a variety of factors in finding the FISA statute constitutional, and thus, that orders issued pursuant to it were reasonable under the Fourth Amendment. While the FISCR appears to have placed great stock in the fact that FISA applications must be subjected to prior judicial scrutiny, the Court did not find it constitutionally problematic that a senior government official, rather than a detached magistrate, made findings

⁷⁶The FISCR also addressed the amici filers' concerns that FISA does not parallel Title III's notice requirements or its requirement that a defendant may obtain the Title III application and order when challenging the legality of the surveillance. Id. at 741. The FISCR distinguished FISA from Title III in these two contexts and refused to find that the absence of these requirements undermined the reasonableness of the FISA orders under consideration. Id.

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

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

comparable to those that Title III requires a judge to make. *Id.* at 739-41. The FISCR was also satisfied with the probable cause findings made under FISA, *id.* at 738-39, as well as with the extended duration of orders issued under it. *Id.* at 740. Both particularity requirements in FISA weighed into the FISCR's analysis and the FISCR did not negatively opine on the fact that one of those findings was made by a senior executive branch official rather than a judge.

So, from the FISCR's opinion in *In re Sealed Case*, it is logical to assume that electronic surveillance targeted against United States persons within the United States is reasonable under the Fourth Amendment under the following circumstances: (1) there is some degree of prior judicial scrutiny, (2) there is probable cause to believe that the target is an agent of a foreign power (or a foreign power itself), (3) there is probable cause to believe that the facility to be targeted is being used or is about to be used by the target, (4) at least some constitutionally required determinations are made by the senior executive branch officials designated in the statute, subject to a highly deferential degree of judicial review, (5) the duration may extend to 90 days, particularly when there is Court oversight over minimization procedures, and (6) such minimization procedures are in place and being applied.

It is not clear from the FISCR opinion how much importance the Court attached to each of the above-described factors. For that reason, it is difficult to discern what effect the modification or removal of one of the factors would have on the overall determination of reasonableness. Nor is there clear guidance on how the requirements of reasonableness might vary for targets who are United States persons located outside of the United States.

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

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

b. United States v. Bin Laden

A case that far more closely resembles the case now before this Court is United States v. Bin Laden, which involved search and surveillance targeted at a United States person located overseas. The facts there were the following.

In its investigation of al Qaeda in Kenya, in August 1996, the intelligence community began monitoring telephone lines used by certain persons associated with al Qaeda, including Wadih El-Hage, an American citizen. Bin Laden, 126 F. Supp. 2d at 269. Although the government was aware that El-Hage was a United States person, it was not until eight months later, on April 4, 1997, that the Attorney General specifically authorized search and surveillance of El-Hage pursuant to E.O. 12333, § 2.5. Id. at 269 & n.23.

At his criminal trial, El-Hage filed a motion to suppress evidence seized during the search of his home and the surveillance of his telephone and cellular telephone in Kenya, arguing that the search and surveillance violated his Fourth Amendment rights. Id. at 268, 270. The District Court found that the searches and surveillance conducted subsequent to the Attorney General's E.O. 12333 authorization fell under the foreign intelligence exception to the Fourth Amendment's warrant requirement and were reasonable; therefore, the evidence was lawfully acquired and not subject to suppression. Id. at 279, 288. However, the District Court found that surveillance conducted prior to April 4, 1997, was not incidental, as the government argued, and because the government had not obtained the Attorney General's authorization, was "not embraced by the foreign intelligence exception to the warrant requirement." Id. at 279. Further, because no warrant had issued, the Court found that the surveillance violated El-Hage's Fourth

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

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

Amendment rights. *Id.* at 281-82. However, for reasons not relevant to this matter, the Court declined to apply the exclusionary rule to the evidence that had been seized and intercepted. *Id.* at 282-84.

As the District Court in Bin Laden noted, in order to find that the surveillance did not offend the Fourth Amendment, the Court needed to find not only that the government met the requirements of the foreign intelligence exception to the warrant requirement, but also that the conduct of the surveillance was reasonable. *Id.* at 284. There, the Court identified three factors as being essential in order to find that electronic surveillance targeted against a United States person abroad fit within the foreign intelligence exception to the warrant requirement: (1) the target must be an agent of a foreign power, (2) the primary purpose of the surveillance must be to acquire foreign intelligence, and (3) the President or the Attorney General must authorize the surveillance. *Id.* at 277.⁷⁷ The Bin Laden Court found that all three criteria were satisfied by virtue of the Attorney General's E.O. 12333 authorization.

The District Court in Bin Laden then analyzed the reasonableness of the surveillance. *Id.* at 284-86. In response to El-Hage's concerns, the District Court acknowledged that the duration

⁷⁷These criteria appear to derive directly from the holding in United States v. Truong, 629 F.2d 908 at 915. See Bin Laden, 126 F. Supp. 2d at 275, 277-79. As already noted, the FISCRC took exception with Truong's articulation of the primary purpose requirement in its opinion in In re Sealed Case, 310 F.3d at 744. See *supra* pp. 61-62. Following the lead of the FISCRC, as discussed above, this Court holds that the foreign intelligence exception to the warrant requirement requires only that a significant purpose of the acquisition is to obtain foreign intelligence information, there is probable cause to believe the individual who is targeted is an agent of a foreign power and that such probable cause finding is made by a sufficiently authoritative official, such as the Attorney General.

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

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

of a surveillance may be a factor to consider in analyzing reasonableness. *Id.* at 286. However, the District Court accepted the government's argument that "more extensive monitoring and 'greater leeway' in minimization efforts are permitted in a case like this given the 'world-wide, covert and diffuse nature of the international terrorist group(s) targeted.'" *Id.* (citations omitted). As this quote suggests, the Court appears to have found that the existence of minimization procedures bears upon reasonableness, although the Court did not address the necessary parameters of such procedures. *Id.* Finally, as part of its reasonableness analysis, the District Court, citing *United States v. Scott*, 516 F.2d 751, 759 (D.C. Cir. 1975), found it significant that the telephones were used communally by al Qaeda agents, thereby making it more reasonable for the government to monitor them than it would be if the phones were primarily used for legitimate, non-foreign intelligence-related purposes. *Id.*

Thus, the factors the *Bin Laden* Court appears to have relied upon to assess the reasonableness of the surveillance were: (1) the existence of minimization procedures, (2) the duration of the monitoring as balanced against both the minimization procedures and the nature of the threat being investigated, and (3) the extent to which the targeted facilities are used in support of the activity being investigated.

c. Reasonableness Factors

i. Common Factors Utilized in Both *In re Sealed Case* and *Bin Laden*

Comparing the factors relied upon by the FISCR in *In re Sealed Case* and by the District Court in *Bin Laden*, some factors are common in both cases. These factors can provide the starting point for this Court's reasonableness analysis of the directives issued to Yahoo. Both

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

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

courts favorably noted that probable cause findings were made with regard to the target being an agent of a foreign power, In re Sealed Case, 310 F.3d at 738; Bin Laden, 126 F. Supp. 2d at 277-78, with the District Court expressly finding this factor to be an essential criterion for meeting the requirements of the foreign intelligence exception to the warrant requirement, id. at 277. Both Courts also relied upon the existence of minimization procedures in finding the surveillance at issue reasonable. In re Sealed Case, 310 F.3d at 740-41; Bin Laden, 126 F. Supp. 2d at 286. In addition, both Courts examined the duration of the authorized surveillance and both intimated that a longer duration must be balanced by more rigorous minimization procedures than might be reasonable for a shorter period of surveillance. In re Sealed Case, 310 F.3d at 740; Bin Laden, 126 F. Supp. 2d at 285-86. On this point, the FISCR found a 90-day duration reasonable and the District Court seemed to find a several month duration to be reasonable (although it is not clear whether the District Court predicated its assessment on the 90-day re-authorization by the Attorney General in July 1997). Id.⁷⁰ Both Courts found it reasonable that at least some findings were made by high level executive branch officials, even though not made by a judge. In re Sealed Case, 310 F.3d at 739-40; Bin Laden, 126 F. Supp. 2d at 279. The District Court specifically found it necessary that the Attorney General or the President make the probable cause findings, id. at 279, while the FISCR was satisfied that other senior executive branch officials make at least some of the necessary findings. In re Sealed Case, 310 F.3d at 739. The

⁷⁰The District Court seemed to accept the defendant's assertion that the surveillance against him had continued for many months. Bin Laden, 126 F. Supp. 2d at 285-86. It is unclear from the District Court opinion the significance it attached to the fact that the Attorney General, in accordance with E.O. 12333, re-authorized the surveillance 90 days after her initial authorization. Id. at 279.

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

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

FISCR explicitly relied upon the fact that there was a finding as to the facilities being targeted, distinct from and in addition to the finding that the targeted individual is an agent of a foreign power. *Id.* at 739-40. The District Court, while it did not directly hold that there is a requirement for a prior finding concerning the targeted facilities, favorably noted that it was "highly relevant" that the targeted telephones were "'communal' phones which were regularly used by al Qaeda associates." *Bin Laden*, 126 F. Supp. 2d at 286.

ii. Factors Weighed Differently by the Two Courts

Two of the factors considered by the courts appear to have been weighed differently. The District Court explicitly rejected the requirement of prior judicial review of the government's application, *id.* at 275-77, while the FISCR found this to be an important consideration, *In re Sealed Case*, 310 F.3d at 738. And, while the FISCR explicitly addressed the requirement that there be a prior finding of probable cause to believe that a particular facility is being or will be used by the targeted agent, *id.* at 739-40, the District Court referred to this consideration only peripherally, *Bin Laden*, 126 F. Supp. 2d at 286.

* Prior Judicial Review Not Required

The FISCR favorably noticed that FISA orders are subject to prior judicial approval. The District Court, on the other hand, determined that such approval was not necessary under the circumstances of the case before it. While the FISCR was considering a request to conduct surveillance of a United States person located within the United States, the individual targeted in the matter presented to District Court, also a United States person, was located outside the United States.

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

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

Without question, Congress is aware, and has been for quite some time, that the intelligence community conducts electronic surveillance of United States persons abroad without seeking prior judicial authorization. In fact, when Congress enacted FISA in 1978, it explicitly excluded overseas surveillance from the statute, as reflected in a House of Representatives Report that states, "this bill does not afford protections to U.S. persons who are abroad . . ." H.R. Rep. No. 95-1283, pt. 1 at 51 (1978). See also Bin Laden, 126 F.Supp. 2d at 272 n.8 (noting that FISA only governs foreign intelligence searches conducted within the United States). The Bin Laden Court examined the issue of prior judicial approval in the same context presented to the Court in this case, and observed that "[w]arrantless foreign intelligence collection has been an established practice of the Executive Branch for decades." *Id.* at 273 (citation omitted). Citing Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 610 (1952) ("[A] systematic, unbroken, executive practice, long pursued to the knowledge of Congress and never before questioned, engaged in by Presidents who have also sworn to uphold the Constitution, making as it were such exercise of power part of the structure of our government, may be treated as a gloss on 'Executive Power' vested in the President by § 1 of Art. II.") and Payton v. New York, 445 U.S. 573, 600 (1980) ("A longstanding, widespread practice is not immune from constitutional scrutiny. But neither is it to be lightly brushed aside."), the District Court further noted that, "[w]hile the fact of [congressional and Supreme Court silence with regard to foreign intelligence collection abroad] is not dispositive of the question before this Court, it is by no means insignificant." Bin Laden, 126 F. Supp. 2d at 273. This Court finds the reasoning of the District Court persuasive and therefore accepts as a general principle, that prior judicial approval of an

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

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

acquisition of foreign intelligence information targeted against a United States person abroad is not an essential element for a finding of reasonableness under the Fourth Amendment.

* Probable Cause to Believe that the Targeted Facility is Being or is About to be Used

The FISCR directly, and favorably, addressed the requirement in FISA that a prior showing be made that the targeted individuals were using or were about to use the targeted facilities. In re Sealed Case, 310 F.3d at 739-40. The District Court considered this factor more obliquely. Bin Laden, 126 F. Supp. 2d at 286.

The FISCR characterized the judicial finding of probable cause to believe the targeted facility is being or is about to be used by the targeted agent as a particularity requirement, and therefore, one of the required elements of a Fourth Amendment warrant. Given that the FISCR analyzed reasonableness in relation to the warrant requirement, it is not surprising that the FISCR found this factor to be constitutionally significant in assessing reasonableness. In re Sealed Case, 310 F.3d at 739-40. The District Court in Bin Laden expressed no direct view on this factor, nor does its opinion make clear if the Attorney General's authorizations included a probable cause finding regarding the use of the facilities to be targeted. However, as noted above, the District Court did consider the use of the targeted facilities in its reasonableness assessment. Bin Laden, 126 F. Supp. 2d at 286. The disparity between the attention given to this factor by the two Courts may well be explained by the fact that the FISCR was considering the conduct of electronic surveillance within the United States while the District Court was analyzing surveillance conducted overseas. The Fourth Amendment particularity requirement serves, in large part, as a check to minimize the likelihood that persons who have a reasonable expectation

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

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

of privacy are not mistakenly subjected to government surveillance.⁷⁹ When the surveillance activity is conducted against persons outside the United States, the persons who would be inappropriately surveilled most likely would be non-United States persons. And, this is not a class of persons who enjoy the protections of the Fourth Amendment. Therefore, it seems reasonable that, in the overseas context, there is less of a need to require a prior showing of probable cause to believe that a properly targeted individual is using or is about to use a specific, targeted facility.

iii. Necessity

The FISCR noted that FISA incorporates a “necessity” provision, as does Title III. In re Sealed Case, 310 F.3d at 740. The District Court in Bin Laden, however, makes no mention of necessity. A showing of necessity is not always a prerequisite for reasonableness. Illinois v. Lafayette, 462 U.S. 640, 647 (1983) (“[t]he reasonableness of any particular governmental activity does not necessarily or invariably turn on the existence of alternative ‘less intrusive’ means”). And, this Court is not persuaded that, in the context of the PAA, any ameliorative purpose would be served by requiring the government to demonstrate that less intrusive means have been attempted. Indeed, the very purpose of the PAA is to provide the government with “flexible procedures to collect foreign intelligence from foreign terrorists overseas . . . [that do]

⁷⁹While discussions of the particularity requirement typically focus on the “property to be sought” rather than the person using that property, Berger v. New York, 388 U.S. 41, 59 (1967), it is clearly the privacy interests of the individual that the Constitution protects. Verdugo-Urquidez, 494 U.S. at 266. Thus, in the context of electronic surveillance of email communications, if the government surveils the wrong email account, the harm would be against the privacy interests of persons whose communications were improperly acquired.

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

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

not impose unworkable, bureaucratic requirements that would burden the intelligence community.” 153 Cong. Rec. H9954 (daily ed. Aug. 4, 2007) (statement of Rep. Smith). Therefore, this Court will not consider the availability of less intrusive means as a factor in determining the reasonableness of the directives issued to Yahoo.

iv. Warrant Exception Criteria Are Factors to Consider in Assessing Reasonableness.

The factors that provide the basis for the foreign intelligence exception to the warrant requirement (a significant foreign intelligence purpose and probable cause to believe that any United States person who is targeted is an agent of a foreign power) are also key elements that weigh in assessing reasonableness.

d. Application of the Reasonableness Factors to the Acquisition of Targeted United States Persons’ Communications Through the Directives Issued to Yahoo

In assessing the Fourth Amendment reasonableness of the acquisition of foreign intelligence information through the directives issued to Yahoo, this Court relies on the findings made above in Part III.B.1 of this Opinion, in which it found that the surveillance satisfies the requirements for the foreign intelligence exception to the warrant requirement. In addition, this Court will consider the following factors relied upon by the FISCR in In re Sealed Case and the District Court in Bin Laden: (1) minimization, (2) duration, (3) authorization by a senior government official, and (4) identification of facilities to be targeted.

But, first, this Court must acknowledge the statutory framework that governs the proposed acquisitions. The PAA only authorizes “the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States ...” 50

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

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

U.S.C.A. § 1805b(a) (emphasis added). The statute further requires that “there are reasonable procedures in place for determining that the acquisition of foreign intelligence under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 105C of this Act.” 50 U.S.C.A. § 1805b(a)(1) (emphasis added).⁸⁰

This Court sees no reason to question the presumption that the vast majority of persons who are located overseas are not United States persons and that most of their communications are with other, non-United States persons,⁸¹ who also are located overseas. Thus, most of the communications that will be obtained through the directives issued to Yahoo likely will be communications between non-United States persons abroad, *i.e.*, persons who do not enjoy the protection of the Fourth Amendment.⁸² So, to the extent “reasonable” procedures represent an effort to minimize the likelihood of targeting the wrong facility or the wrong person or of obtaining the communications of non-targeted communicants, a program such as this, which is focused on overseas collection, presents fewer Fourth Amendment concerns than does a program

⁸⁰See supra Part II.B for this Court’s resolution of the ambiguities related to this provision.

⁸¹This common sense presumption is embodied in the Department of Defense procedures governing the collection of information about United States persons, which state, “[a] person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person’s communications or other available information concerning the person give rise to a reasonable belief that such person is a United States citizen or permanent resident alien.” DoD Procedures, Procedure 5, Part 3.B.4.

⁸²Supra note 69.

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

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

that focuses on domestic communications within the United States.⁸³ It is against this backdrop that this Court will assess the appropriate reasonableness factors.

i. Minimization

By statute, the communications that will be acquired through the directives issued to Yahoo will be subject to minimization procedures that are supposed to comport with the definition of "minimization procedures" under 50 U.S.C.A. § 1801(h). 50 U.S.C.A. § 1805b(a)(5). This Court has reviewed the minimization procedures applicable to these directives and finds that they are virtually the same procedures the government uses for many non-PAA FISA collections. Feb. 2008 Classified Appendix at [REDACTED]

[REDACTED] In other contexts, this Judge has (as other Judges on the FISC have) found these non-PAA procedures to be reasonable under circumstances in which the government is intercepting private email communications.

This Court, therefore, finds the minimization procedures filed by the government to be sufficiently robust to protect the interests of United States persons whose communications might be acquired through the acquisition of information obtained through the directives issued to

⁸³This Court appreciates Yahoo's concern that "it is possible that the 'target' may return to the U.S. during the surveillance period. Therefore, the Directives may target U.S. citizens who may be in the U. S. when under surveillance." Yahoo's Mem. in Opp'n at 9. However, the Court has reviewed the government's targeting procedures and notes that the government has specifically addressed this issue and has robust procedures in place to [REDACTED] cease such surveillance "without delay[]" when it is determined that the target is in the United States. Feb. 2008 Classified Appendix at [REDACTED] see also *id.* at [REDACTED]

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

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

Yahoo, and that these procedures satisfy the definition of "minimization procedures" under 50 U.S.C.A. § 1801(h).

ii. Duration

The PAA permits the Director of National Intelligence and the Attorney General to authorize the acquisition of foreign intelligence information for a period of up to one year. 50 U.S.C.A. § 1805b(a). However, in each of the certifications filed with this Court, the Director of National Intelligence and the Attorney General assert that prior to targeting a United States person, the government must obtain Attorney General authorization using the procedures under E.O. 12333, § 2.5. Feb. 2008 Classified Appendix at [REDACTED]. One of the provisions of those procedures is that surveillance conducted pursuant to the Attorney General's authorization may not exceed 90 days. DoD Procedures, Procedure 5, Part 2.C.6. Thus, for those targeted individuals who have Fourth Amendment protection, *i.e.*, United States persons, the Court assumes that the Attorney General will re-authorize the acquisition every 90 days in order for the acquisition under the PAA to continue.⁸⁴

Ninety days is the identical duration the FISC found reasonable in the matter it considered. The FISC noted in *In re Sealed Case* that the longer duration under FISA (*i.e.*, 90 days rather than the 30-day duration in Title II) "is based on the nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information.'" 310 F.3d at 740 (citations omitted). However, the FISC also suggested

⁸⁴It is therefore also this Court's assumption that if the Attorney General does not issue a new authorization, surveillance of the targeted account will cease.

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

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

that the 90-day duration was reasonable in part because the FISC exercised oversight over the minimization procedures while a surveillance is being conducted. *Id.* But, the PAA does not provide a similar role for the FISC. Notably, though, under the PAA, the target of the surveillance will be located overseas, and presumably, so will be a significant number of the persons who communicate with that target, while under a domestic FISA surveillance, it is feasible, and indeed likely, that the bulk of the information obtained would be to, from, or about United States persons. Therefore, to the extent judicial oversight over minimization serves to enhance the protection afforded United States persons whose communications are intercepted, the importance of such oversight wanes when a reduced proportion of United States person information will be acquired. Indeed, in Bin Laden, there was no judicial oversight of the minimization procedures whatsoever. And, in that case, the Court did not find a duration of approximately eight months to be unreasonable.¹⁵ Therefore, on balance, this Court finds a 90-day duration for the acquisition of communications targeting United States persons under the circumstances presented in this case, even without judicial oversight of the application of the minimization procedures, reasonably limited.

iii. Senior Official Approval

Prior to the issuance of its directives to Yahoo, as required by the statute, the Attorney General and the Director of National Intelligence determined, through written certifications under

¹⁵Supra note 78 and accompanying text.

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

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

oath, that were supported by affidavits from the Director of NSA, that

there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under section 105B . . . concerns persons reasonably believed to be located outside the United States[,] . . . the acquisition does not constitute electronic surveillance as defined in section 101(f) of the Act[,] the acquisition involves obtaining foreign intelligence information from or with the assistance of communications service providers . . .[,] a significant purpose of the acquisition is to obtain foreign intelligence information and [,] the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h) of the Act.

Feb. 2008 Classified Appendix at [REDACTED] see also *id.* at [REDACTED]

[REDACTED] It is this Court's view that the certifications of these two officials represent a sufficient restraint on the exercise of arbitrary action by those in the executive branch who are effecting the actual acquisition of information, see *In re Sealed Case*, 310 F.3d at 739 (characterizing congressional intent that the certification by senior officials, "typically the FBI Director [with approval by] the Attorney General or the Attorney General's Deputy," would provide written accountability and serve as "an internal check on Executive Branch arbitrariness") (citation omitted); H.R. Rep. 1283 at 80, and thus weighs favorably in assessing the reasonableness of the directives issued to Yahoo.

iv. Identifying Targeted Facilities

The final factor to consider in determining the reasonableness of the directives is the identification of the accounts to be targeted. As discussed above, the manner in which accounts are targeted for surveillance is an important consideration in determining the reasonableness of a

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

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

warrantless surveillance.⁸⁶ For the following reasons, the Court finds that the current procedures employed by the government are reasonable, given all the facts and circumstances of the anticipated acquisition.

In a typical foreign intelligence case where the intelligence activity is conducted within the United States, the government first establishes probable cause to believe that a particular individual is an agent of a foreign power and then identifies the specific facility the person is using that the government wants to monitor. By establishing probable cause to believe that the target is using a particular facility (as is required under the non-PAA provisions of FISA, 50 U.S.C.A. §§ 1804(a)(3)(B) & 1805(a)(3)(B)), the government is demonstrating the nexus between the person being targeted and the facility that is going to be monitored. This nexus requirement diminishes the likelihood that the government will monitor the communications of a completely innocent United States person, which would, on its face, appear to be an unreasonable search, and thus, violative of the Fourth Amendment.

The PAA, by its terms, however, only allows the acquisition of communications which are reasonably believed to be used by persons located outside the United States. 50 U.S.C.A. §§ 1805a & 1805b(a). As stated above,⁸⁷ this Court can envision no reason to question the presumption that most people who are located outside the United States are not United States

⁸⁶The Court is mindful that the PAA specifically provides that “[a] certification under subsection (a) is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.” 50 U.S.C.A. § 1805b(b); see also supra Part II.C.

⁸⁷Supra note 81.

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

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

persons. So, even if, after establishing probable cause to believe a particular United States person is an agent of a foreign power, the government, pursuant to the PAA, mistakenly targets an account used by someone other than that United States person, the likelihood is that the person whose privacy interests are implicated is a person who does not enjoy the protection of the Fourth Amendment.

Moreover, by the terms of Lt. Gen. Alexander's affidavit, upon which the Director of National Intelligence and the Attorney General relied when making their certifications, Feb. 2008 Classified Appendix at [REDACTED] the government will only target accounts (whether the user is a United States person or not) if there is some basis for believing that such account will likely be used to communicate information concerning one of the foreign powers specified in the certification. So, even if a targeted account is mistakenly associated with an incorrect user, that account would have been targeted only after United States intelligence analysts had assessed that there is some basis for believing the particular account is being used to convey information of foreign intelligence interest related to the certifications. Therefore, given the provision of the statute that limits acquisition to persons reasonably believed to be located outside the United States, coupled with the process articulated by Lt. Gen. Alexander for limiting surveillance to those accounts that are likely to provide foreign intelligence information related to the certifications, this Court finds that the procedures in place to identify the facilities to be targeted contribute favorably to the reasonableness of the directives issued to Yahoo.

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

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

- v. In Sum, the Acquisition of Foreign Intelligence Information Targeting United States Persons Abroad Obtained Pursuant to the Directives Issued to Yahoo is Reasonable Under the Fourth Amendment.

Having considered the totality of the facts and circumstances, including:

- (1) the statute, which by its terms, limits acquisition to foreign intelligence communications of persons reasonably believed to be located outside the United States and requires written procedures for establishing the basis for making these determinations, procedures that have been reviewed by the Court;
- (2) United States persons will not be targeted unless the Attorney General has determined, in accordance with E.O. 12333, § 2.5 procedures, that there is probable cause to believe that such person is an agent of a foreign power;
- (3) the Director of National Intelligence and the Attorney General have certified that a significant purpose of the acquisition is to obtain foreign intelligence information;
- (4) each authorization for the acquisition of targeted United States person communications is limited to 90 days;
- (5) there are reasonable minimization procedures in place, which meet the definition of "minimization procedures" under 50 U.S.C.A. § 1801(h); and
- (6) there are written procedures in place to ensure that surveillance of the facilities to be targeted likely will obtain foreign intelligence information,

this Court is satisfied that the government currently has in place sufficient procedures to ensure that the Fourth Amendment rights of targeted United States persons are adequately protected and

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

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

that the acquisition of the foreign intelligence to be obtained through the directives issued to Yahoo, as to these individuals, is reasonable under the Fourth Amendment.

c. The Reasonableness of Incidentally Acquiring Communications of United States Persons

The previous section of this Opinion concerned the Fourth Amendment rights of those United States persons whose communications are targeted. However, the universe of communications that will be acquired through the directives issued to Yahoo will include the communications of persons who communicate with the targeted accounts.⁸⁸ Yahoo argues, Yahoo's Mem. in Opp'n at 9, and the government concedes, "[t]he directives therefore, implicate, to varying degrees, the Fourth Amendment rights of ... persons, whether abroad or inside the United States, who are communicating with foreign intelligence targets outside the United States." Gov't.'s Supp. Brief on the Fourth Amend. at 2. This Court agrees that some subset of non-target communicants located in the United States and non-target communicants who are United States persons, whether located in the United States or abroad, enjoy Fourth Amendment protection. United States v. Verdugo-Urquidez, 494 U.S. 259.

As the District Court in Bin Laden noted, "... incidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment." 126 F. Supp. 2d at 280 (citations omitted). Likewise, the Second Circuit has held,

⁸⁸It is this Court's understanding that the directives issued to Yahoo will result in the acquisition of non-target communications only if the non-targeted account is in direct communication with a targeted account or if a communication of the non-targeted account is forwarded to a targeted account. See Declaration of [REDACTED] January 16, 2008; Declaration of [REDACTED] January 23, 2008.

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

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

"[i]f probable cause has been shown as to one such participant, the statements of the other participants may be intercepted if pertinent to the investigation." United States v. Tortorello, 480 F.2d 764, 775 (2d Cir. 1973). As discussed earlier in this opinion, supra Part II, this Court has found that the acquisition of communications obtained through the directives issued to Yahoo adheres to the requirements of the PAA. And, as discussed immediately above, this Court has found that the acquisition of the communications of targeted United States persons obtained through the directives issued to Yahoo is reasonable and therefore complies with the Fourth Amendment.

This Court also notes that, in addition to the underlying surveillance being lawful, the government has in place minimization procedures designed to protect the privacy interests of United States persons. As required by the PAA, the government must have procedures in place that comport with the definition of minimization procedures under section 1801(h) of FISA.

That definition specifies that such procedures must be

- (1) specific procedures ... reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
- (2) procedures that require that nonpublicly available information, which is not foreign intelligence information ... shall not be disseminated in a manner that identifies any United States person, without such person's consent unless such person's identity is necessary to understand foreign intelligence information or assess its importance[.]

50 U.S.C.A. § 1801(h)(1) & (2) (emphasis added). This Court agrees with the government that these minimization procedures adequately protect the privacy interests of persons whose

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

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

communications might be incidentally acquired. Mem. in Support of Gov't Motion at 19; see also Feb. 2008 Classified Appendix at [REDACTED]

Based on the above considerations, this Court finds that any incidental acquisition of the communications of non-targeted persons located in the United States and of non-targeted United States persons, wherever they may be located, is also reasonable under the Fourth Amendment.

IV. Conclusion

There are times when there is an inevitable tension between the interests protected by the Fourth Amendment on the one hand and the federal government's obligation to protect the security of the nation on the other hand. This reality has been particularly acute in an era of ever increasing communications and intelligence technology, when at the same time the threat of global terrorism has intensified, ultimately reaching the American mainland with devastating consequences on September 11, 2001. That is the landscape which confronted the United States Congress when the legislation that is the subject of this Opinion was enacted. Congress obviously sought to strike the proper balance between the sometime conflicting interests of individual privacy and national security when it adopted the PAA. But as illustrated by the painstaking and complex constitutional and statutory analysis this Court had to conduct to resolve the dispute in this case, the balance is not easily achieved. Despite the concerns the Court has expressed regarding several aspects of the legislation, for the reasons set forth above, this Court finds that the directives issued by the government to Yahoo satisfy the requirements of the PAA, do not offend the Fourth Amendment, and are otherwise lawful. Accordingly, Yahoo

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

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

is instructed to comply with the directives and an Order directing Yahoo to do so is being issued contemporaneously with this Opinion.

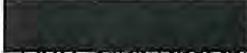
ENTERED this 25th day of April, 2008 in Docket Number 105B(g): 07-01.



REGGIE B. WALTON

Judge, Foreign Intelligence Surveillance Court

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

 Deputy Clerk
FISC, certify that this document
is a true and correct copy of
the original. 

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE PRODUCTION OF TANGIBLE THINGS FROM :

[REDACTED] :
[REDACTED] :
[REDACTED] :

Docket No.: BR 08-13

SUPPLEMENTAL OPINION

This Supplemental Opinion memorializes the Court’s reasons for concluding that the records to be produced pursuant to the orders issued in the above-referenced docket number are properly subject to production pursuant to 50 U.S.C.A. § 1861 (West 2003 & Supp. 2008), notwithstanding the provisions of 18 U.S.C.A. §§ 2702-2703 (West 2000 & Supp. 2008), amended by Public Law 110-401, § 501(b)(2) (2008).

As requested in the application, the Court is ordering production of telephone “call detail records or ‘telephony metadata,’” which “includes comprehensive communications routing information, including but not limited to session identifying information . . . , trunk identifier, telephone calling card numbers, and time and duration of [the] calls,” but “does not include the substantive content of any communication.” Application at 9; Primary Order at 2. Similar productions have been ordered by judges of the Foreign Intelligence Surveillance Court (“FISC”). See Application at 17. However, this is the first application in which the government has identified the provisions of 18 U.S.C.A. §§ 2702-2703 as potentially relevant to whether such orders could properly be issued under 50 U.S.C.A. § 1861. See Application at 6-8.

Pursuant to section 1861, the government may apply to the FISC “for an order requiring the production of any tangible things (including books, records, papers, documents, and other items).” 50 U.S.C.A. § 1861(a)(1) (emphasis added). The FISC is authorized to issue the order, “as requested, or as modified,” upon a finding that the application meets the requirements of that section. Id. at § 1861(c)(1). Under the rules of statutory construction, the use of the word “any” in a statute naturally connotes “an expansive meaning,” extending to all members of a common set, unless Congress employed “language limiting [its] breadth.” United States v. Gonzales, 520 U.S. 1, 5 (1997); accord Ali v. Federal Bureau of Prisons, 128 S. Ct. 831, 836 (2008)

(“Congress’ use of ‘any’ to modify ‘other law enforcement officer’ is most naturally read to mean law enforcement officers of whatever kind.”).¹

However, section 2702, by its terms, describes an apparently exhaustive set of circumstances under which a telephone service provider may provide to the government non-content records pertaining to a customer or subscriber. See § 2702(a)(3) (except as provided in § 2702(c), a provider “shall not knowingly divulge a record or other [non-content] information pertaining to a subscriber or customer . . . to any governmental entity”). In complementary fashion, section 2703 describes an apparently exhaustive set of means by which the government may compel a provider to produce such records. See § 2703(c)(1) (“A governmental entity may require a provider . . . to disclose a record or other [non-content] information pertaining to a subscriber . . . or customer . . . only when the governmental entity” proceeds in one of the ways described in § 2703(c)(1)(A)-(E)) (emphasis added). Production of records pursuant to a FISC order under section 1861 is not expressly contemplated by either section 2702(c) or section 2703(c)(1)(A)-(E).

If the above-described statutory provisions are to be reconciled, they cannot all be given their full, literal effect. If section 1861 can be used to compel production of call detail records, then the prohibitions of section 2702 and 2703 must be understood to have an implicit exception for production in response to a section 1861 order. On the other hand, if sections 2702 and 2703 are understood to prohibit the use of section 1861 to compel production of call detail records, then the expansive description of tangible things obtainable under section 1861(a)(1) must be construed to exclude such records.

The apparent tension between these provisions stems from amendments enacted by Congress in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (“USA PATRIOT Act”), Public Law 107-56, October 26, 2001, 115 Stat. 272. Prior to the USA PATRIOT Act, only limited types of records, not

¹ The only express limitation on the type of tangible thing that can be subject to a section 1861 order is that the tangible thing “can 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.” *Id.* at § 1861(c)(2)(D). Call detail records satisfy this requirement, since they may be obtained by (among other means) a “court order for disclosure” under 18 U.S.C.A. § 2703(d). Section 2703(d) permits the government to obtain a court order for release of non-content records, or even in some cases of the contents of a communication, upon a demonstration of relevance to a criminal investigation.

including call detail records, were subject to production pursuant to FISC orders.² Section 215 of the USA PATRIOT Act replaced this prior language with the broad description of “any tangible thing” now codified at section 1861(a)(1). At the same time, the USA PATRIOT Act amended sections 2702 and 2703 in ways that seemingly re-affirmed that communications service providers could divulge records to the government only in specified circumstances,³ without expressly referencing FISC orders issued under section 1861.

The government argues that section 1861(a)(3) supports its contention that section 1861(a)(1) encompasses the records sought in this case. Under section 1861(a)(3), which Congress enacted in 2006,⁴ applications to the FISC for production of several categories of sensitive records, including “tax return records” and “educational records,” may be made only by the Director, the Deputy Director or the Executive Assistant Director for National Security of the Federal Bureau of Investigation (“FBI”). 18 U.S.C.A. § 1861(a)(3). The disclosure of tax return records⁵ and educational records⁶ is specifically regulated by other federal statutes, which do not by their own terms contemplate production pursuant to a section 1861 order. Nonetheless, Congress clearly intended that such records could be obtained under a section 1861 order, as demonstrated by their inclusion in section 1861(a)(3). But, since the records of telephone service providers are not mentioned in section 1861(a)(3), this line of reasoning is not directly on point. However, it does at least demonstrate that Congress may have intended the sweeping description of tangible items obtainable under section 1861 to encompass the records of telephone service providers, even though the specific provisions of sections 2702 and 2703 were not amended in order to make that intent unmistakably clear.

² See 50 U.S.C.A. § 1862(a) (West 2000) (applying to records of transportation carriers, storage facilities, vehicle rental facilities, and public accommodation facilities).

³ Specifically, the USA PATRIOT Act inserted the prohibition on disclosure to governmental entities now codified at 18 U.S.C.A. § 2702(a)(3), and exceptions to this prohibition now codified at 18 U.S.C.A. § 2702(c). See USA PATRIOT Act § 212(a)(1)(B)(iii) & (E). The USA PATRIOT Act also amended the text of 18 U.S.C.A. § 2703(c)(1) to state that the government may require the disclosure of such records only in circumstances specified therein. See USA PATRIOT Act § 212(b)(1)(C)(i).

⁴ See Public Law 109-177 § 106(a)(2) (2006).

⁵ See 26 U.S.C.A. § 6103(a) (West Supp. 2008), amended by Public Law 110-328 § 3(b)(1) (2008).

⁶ See 20 U.S.C.A. § 1232g(b) (West 2000 & Supp. 2008).

The Court finds more instructive a separate provision of the USA PATRIOT Act, which also pertains to governmental access to non-content records from communications service providers. Section 505(a) of the USA PATRIOT Act amended provisions, codified at 18 U.S.C.A. § 2709 (West 2000 & Supp. 2008), enabling the FBI, without prior judicial review, to compel a telephone service provider to produce “subscriber information and toll billing records information.” 18 U.S.C.A. § 2709(a).⁷ Most pertinently, section 505(a)(3)(B) of the USA PATRIOT Act lowered the predicate required for obtaining such information to a certification submitted by designated FBI officials asserting its relevance to an authorized foreign intelligence investigation.⁸

Indisputably, section 2709 provides a means for the government to obtain non-content information in a manner consistent with the text of sections 2702-2703.⁹ Yet section 2709 merely requires an FBI official to provide a certification of relevance. In comparison, section 1861 requires the government to provide to the FISC a “statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant” to a foreign intelligence investigation,¹⁰ and the FISC to determine that the application satisfies this

⁷ This process involves service of a type of administrative subpoena, commonly known as a “national security letter.” David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 19:2 (2007).

⁸ Specifically, a designated FBI official must certify that the information or records sought are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.” 18 U.S.C.A. § 2709(b)(1)-(2) (West Supp. 2008). Prior to the USA PATRIOT Act, the required predicate for obtaining “local and long distance toll billing records of a person or entity” was “specific and articulable facts giving reason to believe that the person or entity . . . is a foreign power or an agent of a foreign power.” See 18 U.S.C.A. § 2709(b)(1)(B) (West 2000).

⁹ Section 2703(c)(2) permits the government to use “an administrative subpoena” to obtain certain categories of non-content information from a provider, and section 2709 concerns use of an administrative subpoena. See note 7 supra.

¹⁰ 50 U.S.C.A. § 1861(b)(2)(A). More precisely, the investigation must be “an authorized investigation (other than a threat assessment) . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities,” id., “provided that such investigation of a United States
(continued...)

requirement, see 50 U.S.C.A. § 1861(c)(1), before records are ordered produced. It would have been anomalous for Congress, in enacting the USA PATRIOT Act, to have deemed the FBI's application of a "relevance" standard, without prior judicial review, sufficient to obtain records subject to sections 2702-2703, but to have deemed the FISC's application of a closely similar "relevance" standard insufficient for the same purpose. This anomaly is avoided by interpreting sections 2702-2703 as implicitly permitting the production of records pursuant to a FISC order issued under section 1861.

It is the Court's responsibility to attempt to interpret a statute "as a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into an harmonious whole." Food & Drug Admin. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000) (internal quotations and citations omitted). For the foregoing reasons, the Court is persuaded that this objective is better served by the interpretation that the records sought in this case are obtainable pursuant to a section 1861 order.

However, to the extent that any ambiguity may remain, it should be noted that the legislative history of the USA PATRIOT Act is consistent with this expansive interpretation of section 1861(a)(1). See 147 Cong. Rec. 20,703 (2001) (statement of Sen. Feingold) (section 215 of USA PATRIOT Act "permits the Government . . . to compel the production of records from any business regarding any person if that information is sought in connection with an investigation of terrorism or espionage;" "all business records can be compelled, including those containing sensitive personal information, such as medical records from hospitals or doctors, or educational records, or records of what books somebody has taken out from the library") (emphasis added). In this regard, it is significant that Senator Feingold introduced an amendment to limit the scope of section 1861 orders to records "not protected by any Federal or State law governing access to the records for intelligence or law enforcement purposes," but this limitation was not adopted. See 147 Cong. Rec. 19,530 (2001).

ENTERED this 12th day of December, 2008, regarding Docket No. BR 08-13.


REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

¹⁰(...continued)

person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Id. § 1861(a)(1). The application must also include minimization procedures in conformance with statutory requirements, which must also be reviewed by the FISC. Id. § 1861(b)(2)(B), (c)(1), & (g).

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

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



:
:
:
:

: Docket Number: [redacted]

ORDER

On April 3, 2007, I entered an Order and Memorandum Opinion in the above-captioned docket number (April 3 Order), in response to the first application filed in the above-captioned docket number on March 21, 2007. The April 3 Order held that the proposed electronic surveillance was directed at individual telephone numbers and e-mail addresses, rather than the [redacted] facilities [redacted] [redacted] identified by the Government. *Id.* at 6-16. It also granted a motion by the Government for leave to file for an extension of the prior order, in Docket No. [redacted] [redacted] under which this surveillance was previously authorized. *Id.* at 20-21. Leave to

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

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

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

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

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

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

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

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

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

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

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

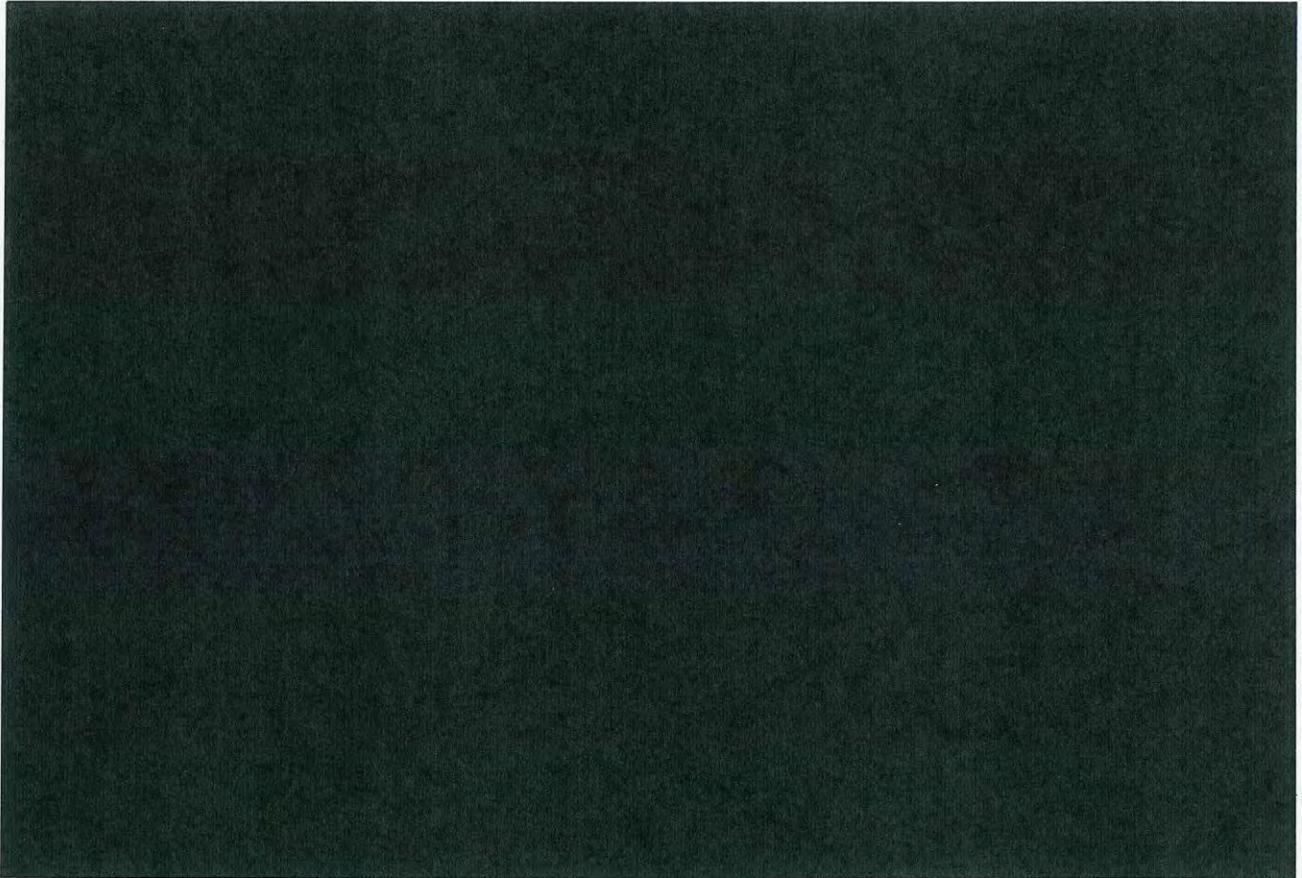
~~TOP SECRET//COMINT//NOFORN~~

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

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

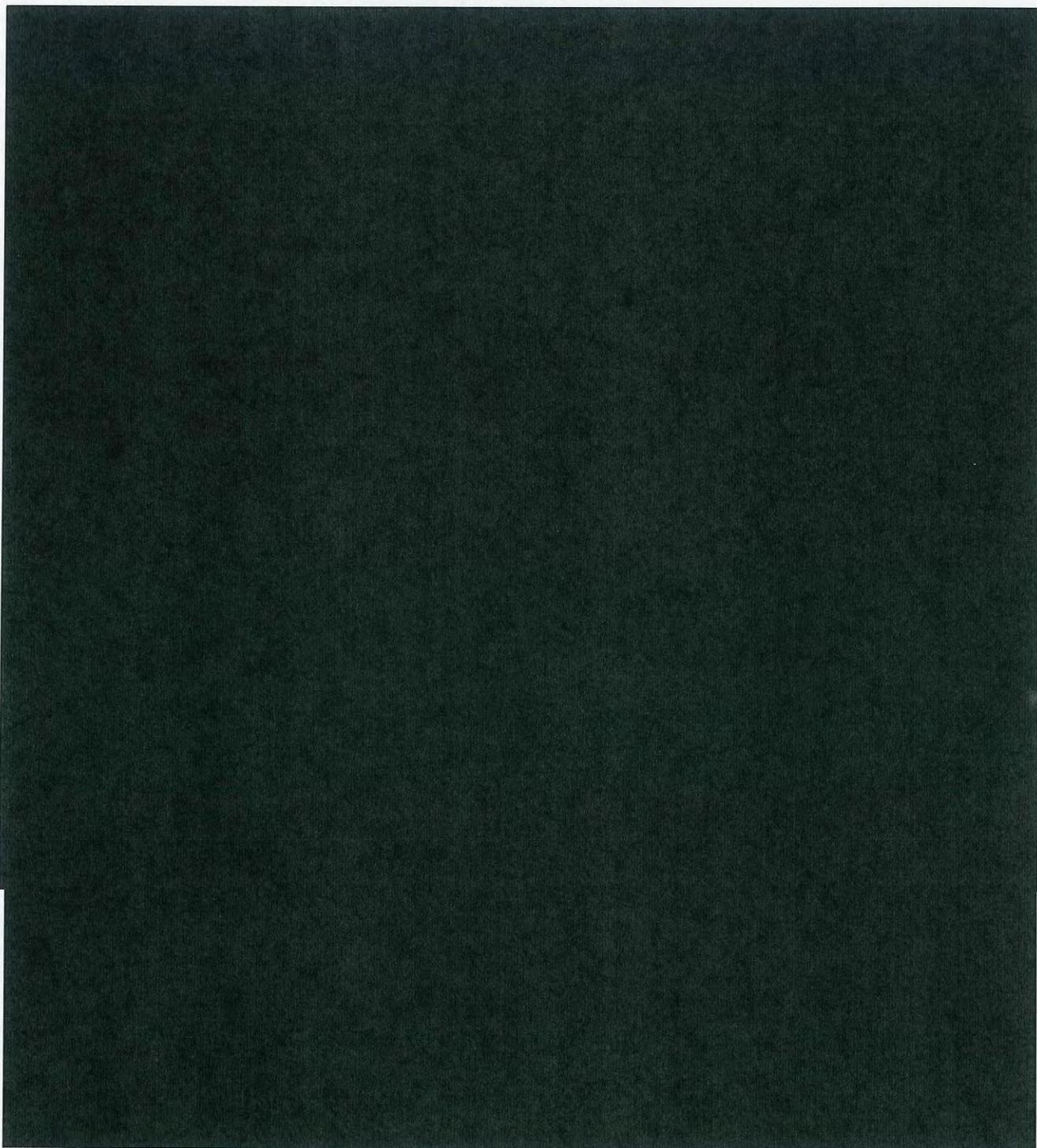
2. The application has been made by a Federal officer and approved by the Attorney General [50 U.S.C. § 1805(a)(2)];

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



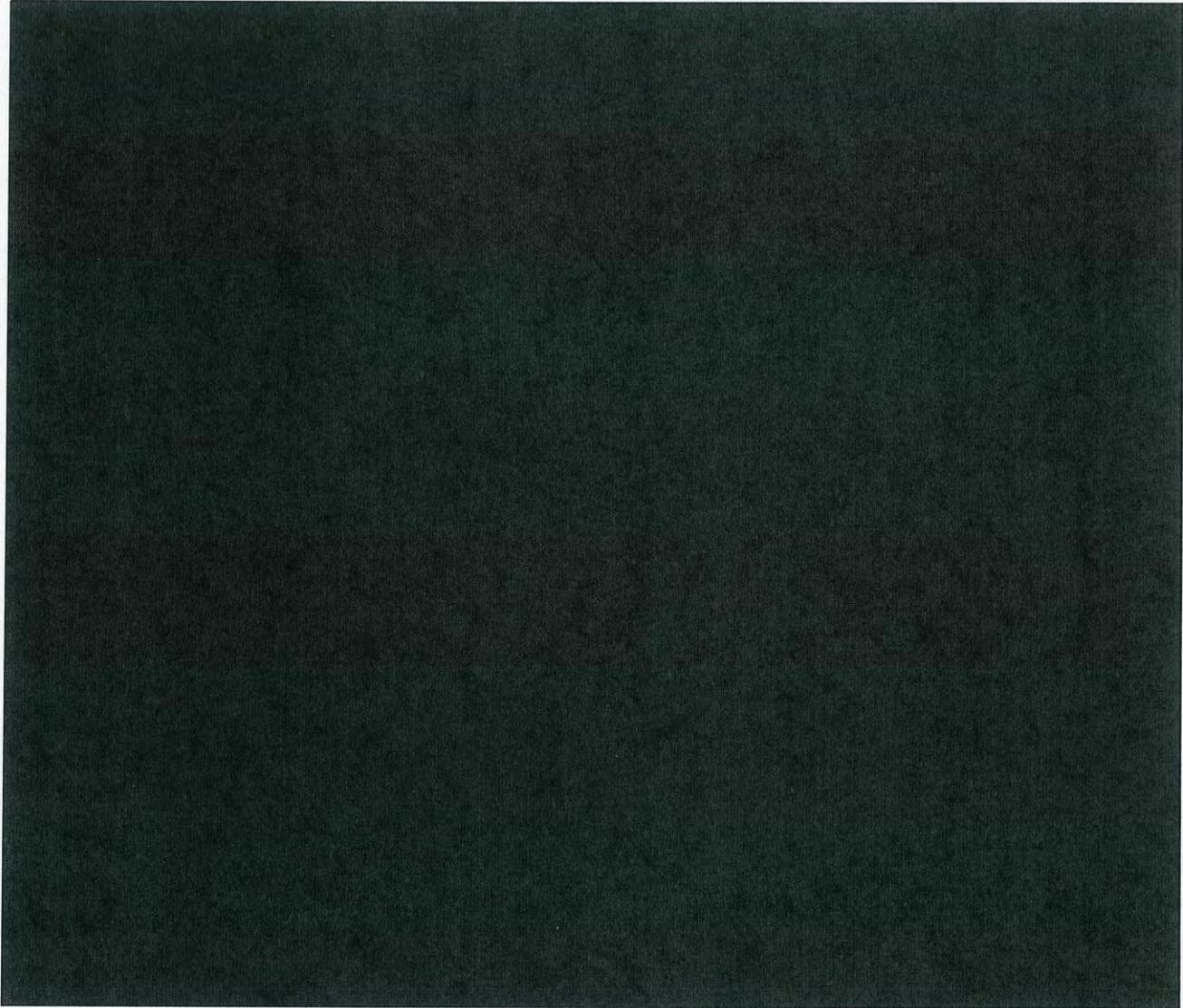
~~TOP SECRET//COMINT//NOFORN~~

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



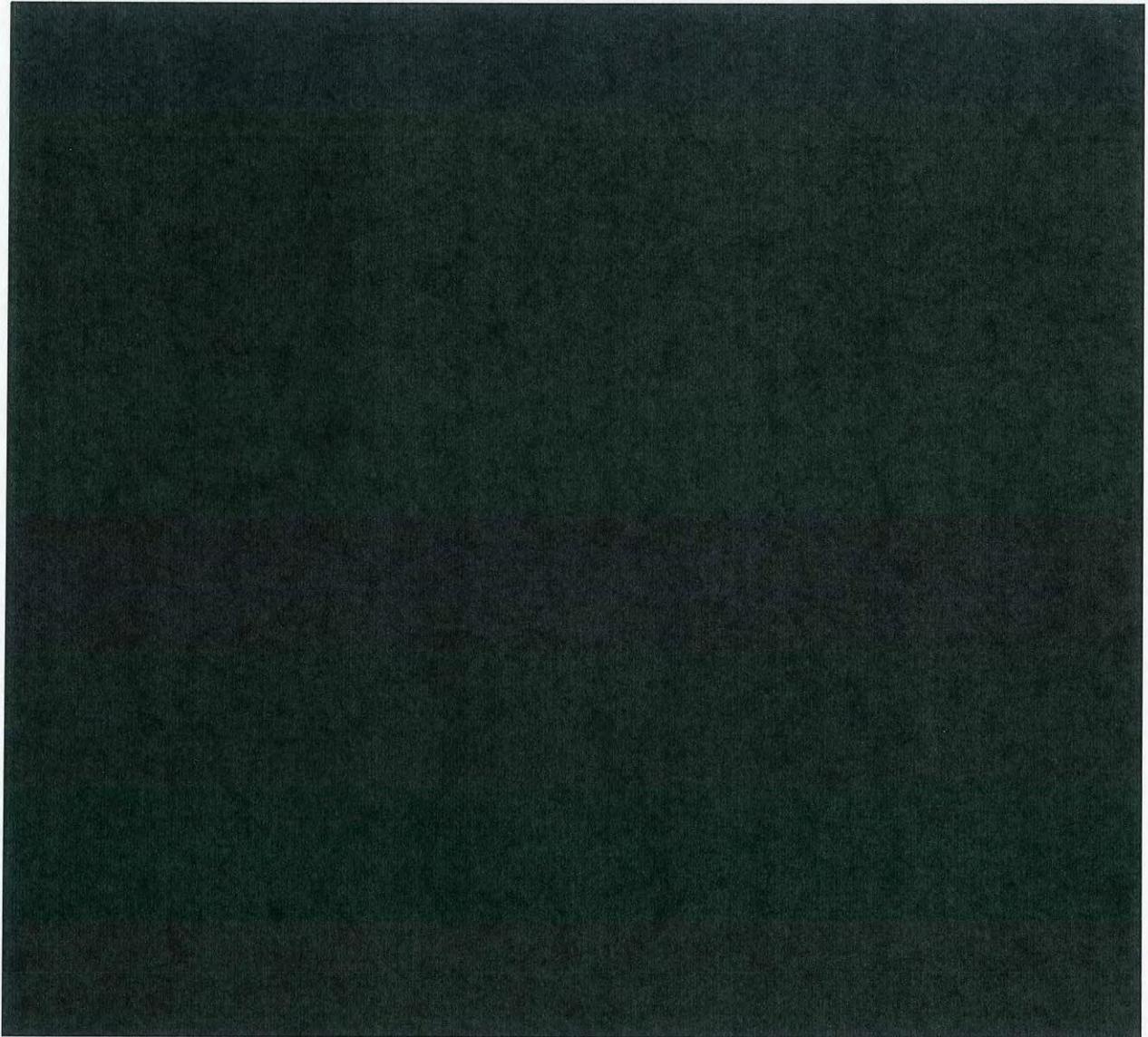
~~TOP SECRET//COMINT//NOFORN~~

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

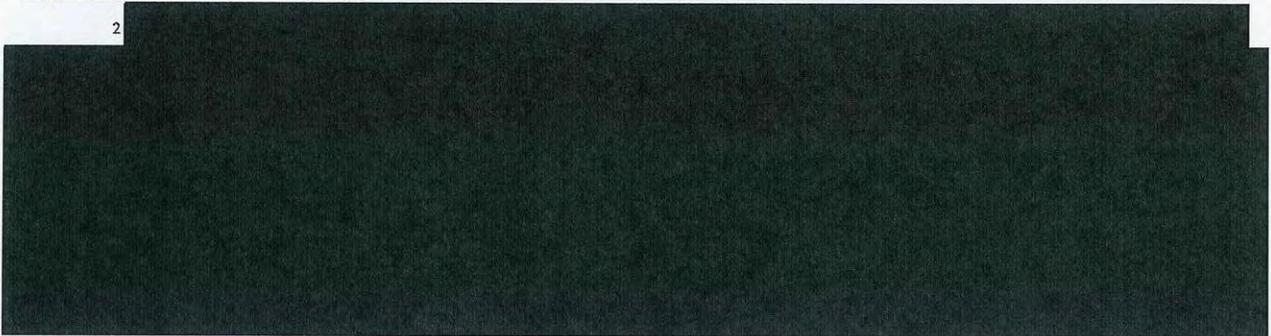


~~TOP SECRET//COMINT//NOFORN~~

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



2



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

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

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

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

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



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

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

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

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

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

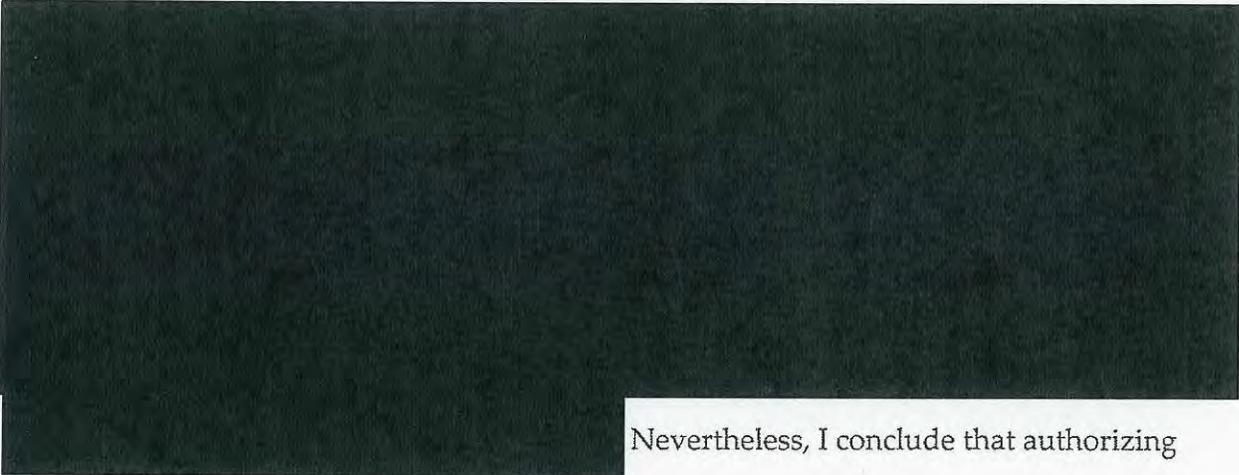
(b). It is well established that the targeted foreign powers pose a grave terrorist threat to the United States. ^{(b)(6); (b)(7)(C)} Declaration, at 10-12, 61-64. The evidence further establishes that the members and agents of the targeted foreign powers engage in a variety of activities in order to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


 Id., at 89, 94-98.

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

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

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



Nevertheless, I conclude that authorizing

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

⁴ The legislative history for the USA PATRIOT Act’s amendment to § 1805(c)(2)(B) states that the new language was “included... to modify [FISA] to allow surveillance to follow a person who uses multiple communications devices or locations, a modification which conforms FISA to the parallel criminal procedures for electronic surveillance in 18 U.S.C. § 2518(11)(b).” 147 Cong. Rec. S11006 (Daily ed. Oct. 25, 2001)(section-by-section analysis of Sen. Leahy). The subsequent addition of “if known” to § 1805(c)(1)(B) was intended “to avoid any uncertainty about the kind of specification required in a multipoint wiretap case, where the facility to be monitored is typically not known in advance.” H.R. Conf. Rep. No. 107-328, at 24 (2001). The notice requirements set forth in § 1805(c)(3) were added in 2006 by section 108(b)(4) of the USA PATRIOT Improvement and Reauthorization Act, Pub. L. No. 109-177, to add “an extra layer of judicial review and to ensure that intelligence investigators will not abuse the multipoint authority.” Conf. Rep. H.R. 3199, reprinted in Cong. Rec. at H11303.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[REDACTED]

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

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

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

[REDACTED]

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

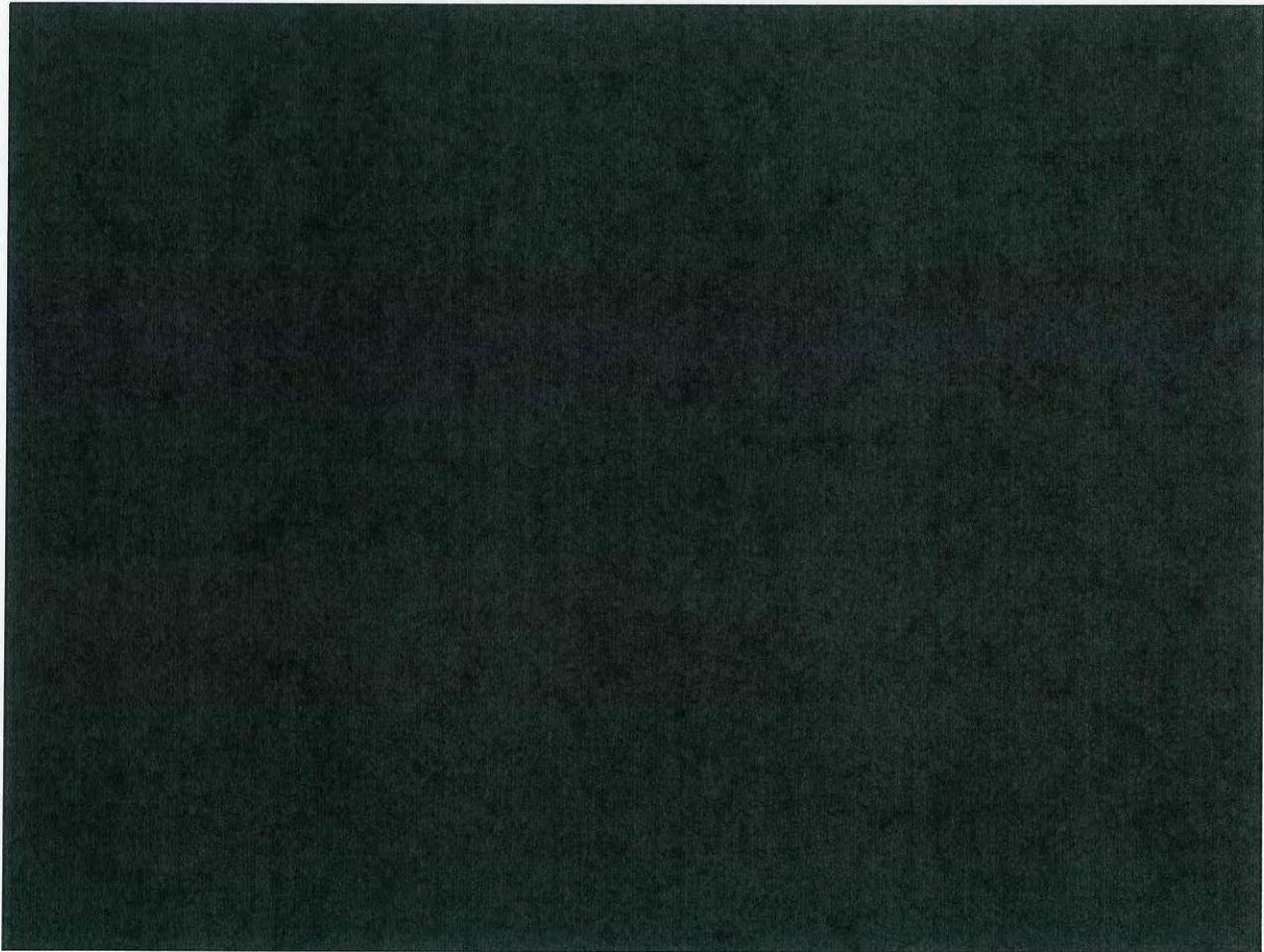
[REDACTED]

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

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

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

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



[redacted] Therefore, separate authority is required to direct this form of electronic surveillance at a new facility, i.e., a separate [redacted] and I grant such authority here.

⁷ For purposes of this Order, [redacted]

⁸ For example, if the user [redacted]

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

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

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

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

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

[REDACTED] and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Such notice shall include:

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

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

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

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

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

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

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

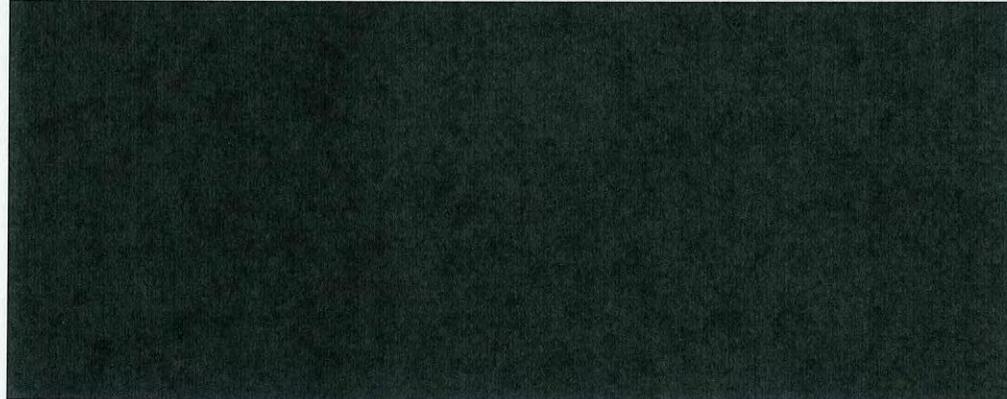
I also hereby find that the Government has established "good cause" within the meaning of 50 U.S.C. § 1806(j) that a subject of emergency surveillance initiated by the Government during the period of this Order, but not authorized by this Court, should not be notified of the emergency employment of electronic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

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



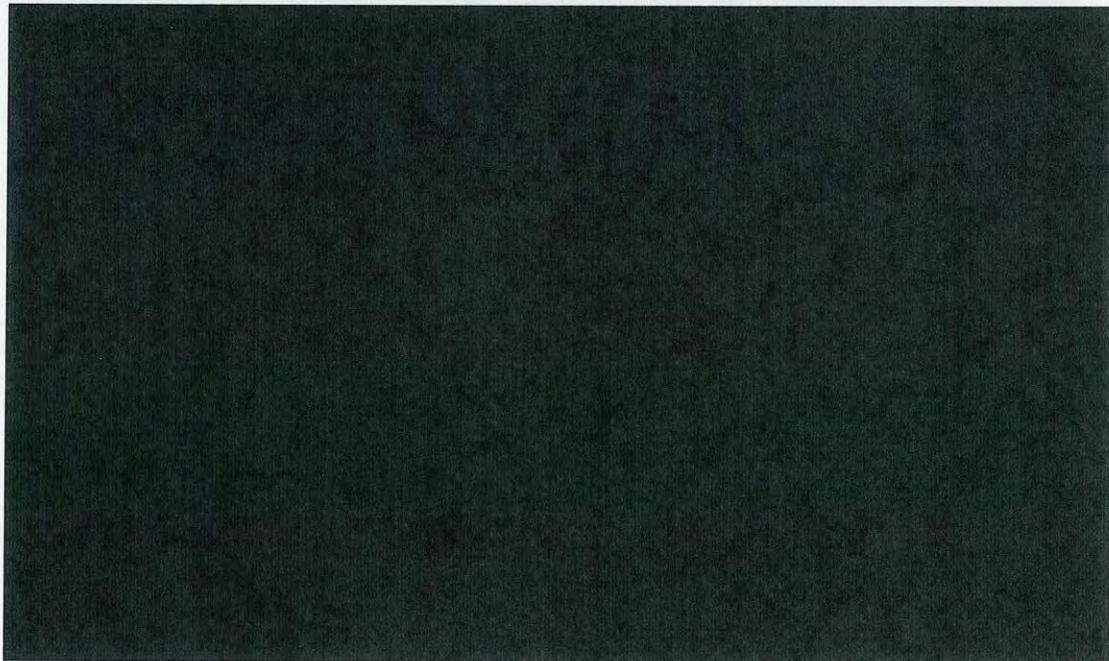
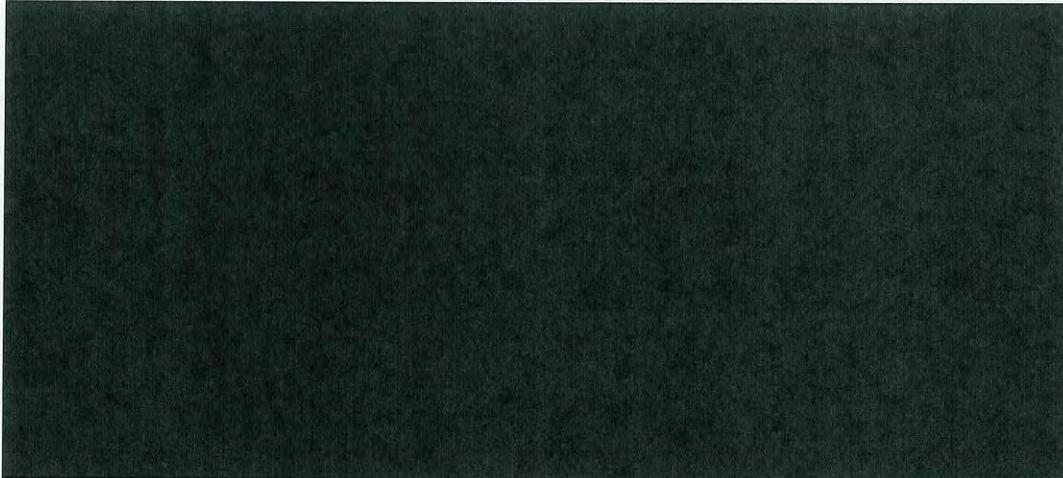
~~TOP SECRET//COMINT//NOFORN~~

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



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

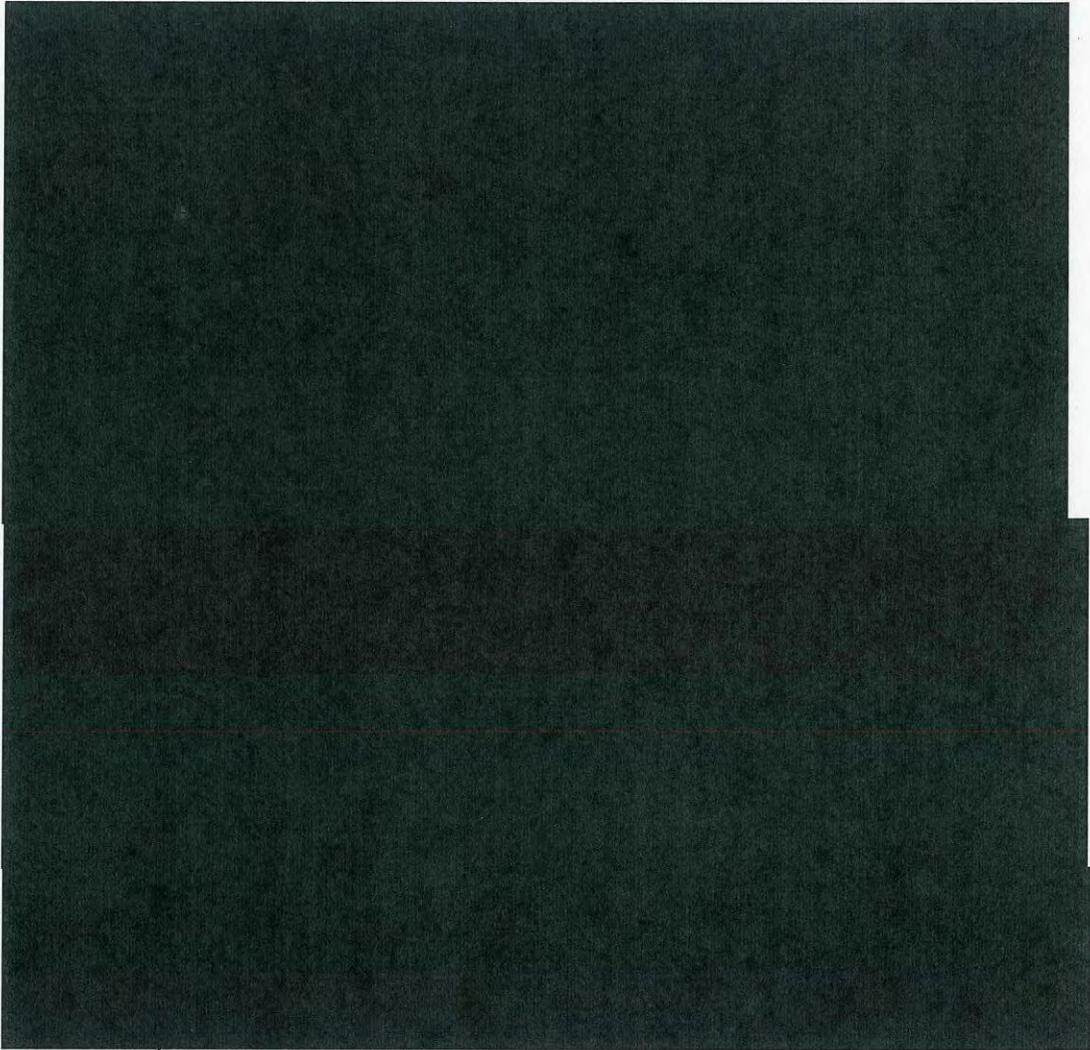
~~TOP SECRET//COMINT//NOFORN~~



¹¹ This Order is based on the principle that the NSA surveillance will be designed to acquire only international communications where a communicant is located outside the United States, but the Court understands that the communications infrastructure and the manner in which it routes communications do not permit complete assurance that no domestic communications will be acquired. In such cases, NSA shall apply its standard FISA minimization procedures, as described and modified herein, to any domestic communications it may inadvertently acquire.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~



§1801(f)(4) surveillance. This surveillance will be effected by using either, or both, of two techniques, as follows: (1) The first technique constitutes



TOP SECRET//COMINT//NOFORN

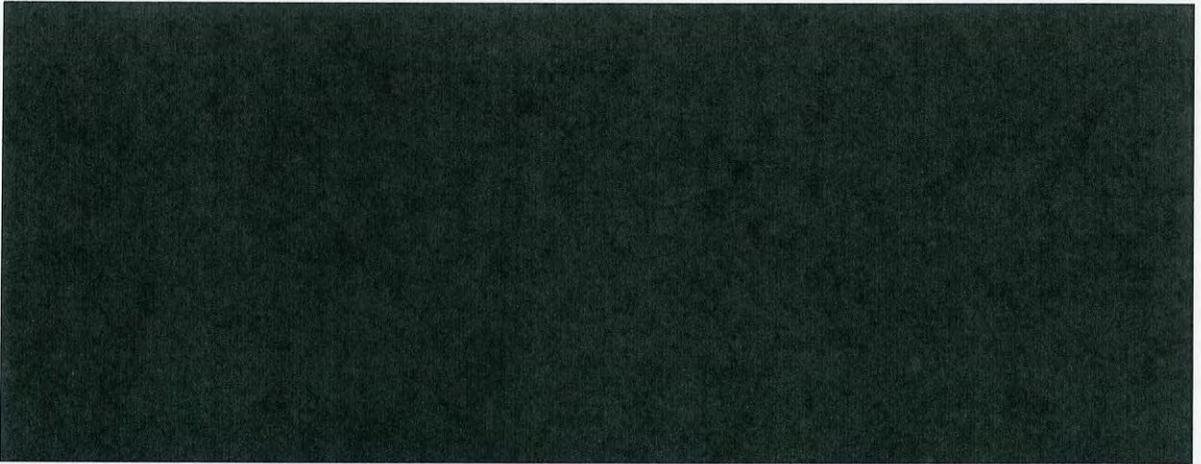
~~TOP SECRET//COMINT//NOFORN~~

"Internet communications surveillance" as described above; or (2) NSA



Unconsented physical entry is not authorized to implement the electronic surveillance approved herein.

III. The person(s) specified in the secondary orders attached hereto, specifically:



~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

including all assigns and/or other successors in interest to said specified persons with regard to the facilities and/or places targeted herein, shall:

(a) furnish the United States all information, facilities, or technical assistance necessary to effect the authorities granted herein in accordance with the orders of this Court directed to said specified person; and

(b) maintain all records concerning this matter, or the aid furnished to the United States, under the security procedures approved by the Attorney General and the Director of Central Intelligence (or the Director of National Intelligence) that have previously been or will be furnished to the specified persons and are on file with this Court,

and the United States shall compensate any such person(s) providing assistance at the prevailing rate for all assistance furnished in connection with the activities described herein [50 U.S.C. § 1805(c)(2)(B)-(D)].

IV. As to all information gathered through the authorities requested herein, the NSA shall follow:

(a) The Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency (also known as Annex A to United States

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with this Court;

(b) and (b)(7)(E)



1. The following shall be added to the end of Section 3(f) of these standard NSA FISA procedures:

(7) The National Security Division of the Department of Justice shall periodically determine that information concerning communications of or concerning United States persons that is retained meets the requirements of these procedures and the Foreign Intelligence Surveillance Act.

2. The following shall be added to the end of Section 4(b) of these standard NSA FISA procedures:

With respect to any other communication where it is apparent to NSA processing personnel that the communication is between a person and the person's attorney (or someone acting on behalf of the attorney) concerning legal advice being sought by the former from the latter, such communications relating to foreign intelligence information may be retained and disseminated within the U.S. Intelligence Community if the communications are specifically labeled as being privileged. However, such communications may not be disseminated outside of

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

the U.S. Intelligence Community without the prior approval of the Assistant Attorney General for the National Security Division or his designee.

3. The following shall replace subsections (a), (b), and (c) of Section 8 of these standard NSA FISA procedures:

NSA may disseminate nonpublicly-available identity or personally identifiable information concerning United States persons to foreign governments provided that such information is foreign intelligence information and either (i) the Attorney General approves the dissemination; or (ii) NSA disseminates the information under procedures approved by the Attorney General. In addition, NSA may disseminate such foreign intelligence information, to the extent authorized by the Director of National Intelligence (DNI) and in accordance with DNI directives, subject to the following procedures:¹⁴

(1) Disseminations to [REDACTED] may be made upon the approval of any person designated for such purpose by the Director of NSA.

(2) Disseminations to [REDACTED] foreign governments may be made upon the approval of the NSA's Office of General Counsel, upon consideration of the following factors: the national security benefit the United States may reasonably expect to obtain from making the dissemination; the anticipated uses to which the foreign government will put the information; and any potential for economic injury, physical harm, or other restriction of movement to be reasonably expected from providing the information to the foreign government. If the proposed recipient(s) of the dissemination have a history of human rights abuses, that history should be considered in assessing the potential for economic injury, physical harm, or other restriction of movement, and whether the

14

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

dissemination should be made. In cases where there is a reasonable basis to anticipate that the dissemination will result in economic injury, physical harm, or other restriction of movement: (i) the approval of the NSA's Signals Intelligence Director will also be required; and (ii) if dissemination is approved, NSA will undertake reasonable steps to ensure that the disseminated information will be used in manner consistent with United States law, including Executive Order No. 12333 and applicable federal criminal statutes.

(3) NSA will make a written record of each dissemination approved pursuant to these procedures, and information regarding such disseminations and approvals shall be made available for review by the National Security Division, United States Department of Justice, on at least an annual basis.

4. Regarding dissemination of evidence of a crime, Sections 5(a)(2) and 6(b)(8) of these standard NSA FISA procedures shall be superseded by the following:

Information that is not foreign intelligence information, but reasonably appears to be evidence of a crime that has been, is being, or is about to be committed, may be disseminated (including United States person identities) to the FBI and other appropriate federal law enforcement authorities, in accordance with 50 U.S.C. § 1806(b), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 'Memorandum of Understanding: Reporting of Information Concerning Federal Crimes,' or any successor document.

5. The following shall be added to end of Section 6 of these standard NSA FISA procedures:

NSA may disseminate all communications acquired to the CIA, which shall process any such communications in accordance with minimization procedures approved by this Court.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

(c) The following additional modifications to the standard NSA FISA minimization procedures for electronic surveillance:

1. Notwithstanding sections 3(c)(2) and (e), 5(b), and 6(a) of the standard NSA FISA procedures, communications acquired under this Order may be retained for five years, unless this Court approves retention for a longer period. The communications that may be retained under this Order include electronic communications acquired because of limitations on NSA's ability to filter communications, as described in Exhibit B to the application.

2. Section 3(c)(6) of these standard NSA FISA minimization procedures is deleted and replaced with:

To the extent reasonably possible, NSA personnel with access to the data acquired pursuant to this authority shall query the data in a manner designed to minimize the review of communications of or concerning U.S. persons that do not contain foreign intelligence information or evidence of a crime.

3. Section 3(g)(1) of these standard NSA FISA minimization procedures, relating to absences "from premises under surveillance" by agents of a foreign power, shall not apply to this surveillance.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

V. The CIA shall minimize all communications received under this order as provided in Exhibit E to the application.

Signed _____ Eastern Time
Date Time

This authorization regarding



expires at 5:00 p.m.

on the 24th day of August, 2007.

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//COMINT//NOFORN~~

(b)(6); (b)(7)(C)

Deputy Cler.
FISC, certify that this document
is a true and correct copy of
the original (b)(6); (b)(7)(C)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE

[REDACTED]

:

[REDACTED]

:

Docket No.: (b)(7)(E)

:

:

ORDER AND MEMORANDUM OPINION

This case involves an extremely important issue regarding probable cause findings that determine what persons and what communications may be subjected to electronic surveillance pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA"), 50 U.S.C. §§ 1801-1811: Are they required to be made by a judge of this Court, through procedures specified by statute for the issuance of a FISA order under 50 U.S.C. § 1805? Or may the National Security Agency (NSA) make these probable cause findings itself, as requested in the application in this case, under an alternative mechanism adopted as "minimization procedures"?

I. INTRODUCTION

When the government believes that a telephone number or e-mail address is being used in furtherance of international terrorism, it will appropriately want to acquire communications relating to that number or e-mail address. Under FISA, the government may obtain an electronic surveillance order from this Court, upon a judge's finding, *inter alia*, of probable cause to believe that the telephone number or e-mail address is used by a foreign power (to include an international terrorist group) or an agent of a foreign power. § 1805(a)(3)(B). In an emergency, the government may begin the electronic surveillance before obtaining the Court order, upon the approval of the Attorney General and provided that a Court order, supported by such a judicial probable cause finding, is obtained within 72 hours thereafter. § 1805(f).

Until recently, these were the only circumstances in which the government had sought, or this Court had entered, a FISA order authorizing electronic surveillance of the telephone or e-

¹ This order and opinion rests on an assumption, rather than a holding, that the surveillance at issue is "electronic surveillance" as defined at 50 U.S.C. § 1801(f), and that the application is within the jurisdiction of this Court. See note 12 *infra*.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

mail communications of suspected international terrorists. However, on December 13, 2006, in Docket No. (b)(7)(E), the government filed an application seeking an order that would authorize electronic surveillance of telephone numbers and e-mail addresses thought to be used by international terrorists without a judge's making the probable cause findings described above, either before initiation of surveillance or within the 72 hours specified in § 1805(f). The proposed electronic surveillance targeted [REDACTED] and involved acquisition by NSA of international telephone and Internet communications [REDACTED].

That application was presented to another judge of this Court. After considering the application and supporting materials, that judge orally advised the government that he would not authorize, on the terms proposed in the application, electronic surveillance of "selector" phone numbers and e-mail addresses, as described below, believed to be used by persons in the United States. The government then filed a second application regarding surveillance of the previously identified phone numbers used by persons in the United States on January 9, 2007, in Docket No. (b)(7)(E).

On January 10, 2007, the judge entered orders in Docket No. (b)(7)(E) that granted the requested electronic surveillance authority, subject to a number of modifications, and specifically limiting the authorized surveillance to "selector" phone numbers and e-mail addresses believed to be used by persons outside the United States. Primary Order at 12. On the same date, the judge also entered orders granting the surveillance authority requested by the application in Docket No. (b)(7)(E) for the identified phone numbers believed to be used by persons in the United States.

The authorization in Docket No. (b)(7)(E) comported with the long-established probable cause determination described above, but the authorization in Docket No. (b)(7)(E) did not. The Primary Order in Docket No. (b)(7)(E) identified [REDACTED] phone numbers as the facilities at which the electronic surveillance is directed and, pursuant to § 1805(a)(3)(B), found probable cause to believe that each phone number was being used or about to be used by an agent of a foreign power. Primary Order at 4-5. This finding rested on specific facts provided in the application regarding the use of each phone number.²

² Declaration of (b)(3), (b)(6), (b)(7)(C) NSA, at 4-59 (Exhibit A to application in Docket No. [REDACTED]). In subsequent supplemental orders, the judge authorized additional phone numbers for surveillance in Docket No. [REDACTED] based on the same kind of judicial probable cause findings, for a total of [REDACTED] telephone numbers covered in Docket No. [REDACTED]. See, e.g., Amendment to Order at (continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

On the other hand, the Primary Order in Docket No. [REDACTED] did not identify, or make probable cause findings regarding, [REDACTED] phone numbers and e-mail addresses subject to surveillance under that order. Instead, that order identified [REDACTED] which the authorized electronic surveillance is directed and found probable cause to believe that [REDACTED] was being or about to be used by the targeted terrorist organizations. Docket No. [REDACTED] Primary Order at 2-5.

On March 21, 2007, the government filed the application in this case, Docket No. [REDACTED] seeking renewal of the surveillance authority granted in Docket No. [REDACTED].³ This application follows Docket No. [REDACTED] in identifying [REDACTED] which the electronic surveillance is directed for purposes of the judge's probable cause findings under § 1805(a)(3)(B).⁴

II. THE SURVEILLANCE AT ISSUE

For surveillance of international telephone communications, [REDACTED] identified in the application. Alexander Decl. at 16. The devices acquire only communications to or from the telephone numbers entered as "selectors." Alexander Decl. at 16, 20-21.

²(...continued).

2 (entered Jan. 16, 2007); Primary Order in Docket No. [REDACTED] at 2 (entered Jan. 22, 2007); Primary Order in Docket No. [REDACTED] at 2 (entered Feb. 2, 2007).

³ On March 22, 2007, in Docket No. [REDACTED], the government filed an application for renewal of the authority granted in Docket No. [REDACTED]. The renewal application identifies [REDACTED] U.S. phone numbers as the facilities at which the surveillance is directed, and requests that the Court find probable cause to believe that each of these phone numbers is being used or is about to be used by an agent of a foreign power, based on specific information set out in the application regarding the use of each number. Docket [REDACTED], proposed Order at 2-5, Declaration of [REDACTED] NSA, at 6-64 (submitted as Exhibit A to Application).

⁴ Docket No. [REDACTED], Application at 4-5; Declaration of Lt. Gen. Keith B. Alexander, Director, NSA, at 26-42 (submitted as Exhibit C to Application) (hereinafter "Alexander Decl."); proposed Order at 6.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

For Internet communications, NSA uses e-mail addresses as selectors.⁵ [redacted] Id. at 34-42. [redacted] acquire only communications that are to or from, or that contain a reference to,⁶ a selector e-mail address. Id. at 14-15, 21-23.

NSA uses telephone numbers or e-mail addresses as selectors only if "it reasonably believes [they] are being used or are about to be used by persons located overseas and . . . has determined there is probable cause to believe [they] are being used or about to be used by a member or agent of [redacted]

[redacted] Id. at 43. The government submits that applying this standard for selectors "narrowly focus[es] NSA's collection efforts on communications" of the targeted terrorist groups, id. at 15. [redacted]

[redacted] Id. at 14. [redacted] overseas e-mail addresses and phone numbers have been adopted as selectors under this standard pursuant to the order in Docket No. [redacted] (b)(7)(E). Id. at 19.

In most relevant respects, the means of electronic surveillance at issue in this case are quite similar to how [redacted] FISA surveillance orders have been implemented. The means of conducting the phone surveillance is, for all relevant purposes, indistinguishable from many prior cases in which communications to or from particular phone numbers are acquired by use of [redacted]

The e-mail surveillance is also quite similar to what has been [redacted]

⁵ [redacted]

⁶ This surveillance acquires an Internet communication containing a reference to a selector e-mail address [redacted]

Id. at 22 n.34.

⁷ [redacted]

(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

authorized previously, to the extent that it acquires communications to or from selector e-mail addresses.⁸ The acquisition of e-mail communications because they refer to a selector e-mail

⁷(...continued)

[Redacted]

In addition, the standard description of ^{b(1), b(7)(E)} [Redacted] ^{b(1)} conducted by the FBI states that such surveillance

and ^{b(6) and b(7)(C)} [Redacted]

⁸

[Redacted]

and ^{b(6), b(7)(C) and (E)} [Redacted]

[Redacted]

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//XI~~

address does not appear to have been authorized under FISA prior to Docket No. [REDACTED] and is discussed further below.

III. PROBABLE CAUSE FINDINGS

Under FISA, a judge of this Court may enter an electronic surveillance order only upon finding, inter alia, that

on the basis of the facts submitted by the applicant there is probable cause to believe that --

(A) the target⁹ of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.

§ 1805(a)(3) (emphasis added). FISA defines "foreign power," in relevant part, as including "a group engaged in international terrorism or activities in preparation therefor." § 1801(a)(4).

In this case, the government contends that, for purposes of § 1805(a)(3)(B) the "facilities" at which the electronic surveillance is directed are [REDACTED] E.g., Alexander Decl. at 13; Government's Memorandum of Law at 32 (attached to Application as part of Exhibit A). The government acknowledges that the telephone numbers and e-mail addresses selected for

[REDACTED] and b(6), b(7) (C) and (E)

⁹ The target of a surveillance "is the individual or entity . . . about whom or from whom information is sought." In re Sealed Case, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (quoting H.R. Rep. 95-1283, pt. 1 at 73 (1978)).

~~TOP SECRET//COMINT//ORCON,NOFORN//XI~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

acquisition are [redacted] "facilities" [Government's Memorandum of Law at 31 n.18] [redacted] Simultaneously, however, the government maintains in another case that [redacted] resulting in an entirely different focus for the judge's assessment of probable cause under § 1805(a)(3)(B).¹⁰ Underlying the government's position, therefore, is the premise that § 1805(a)(3)(B) can be applied so variously that a FISA judge has great discretion in determining what "facilities" should be the subject of the judge's probable cause analysis.

In deciding how to apply § 1805(a)(3)(B), the Court looks first to the language of the statute. See, e.g., Engine Manufacturers Ass'n v. South Coast Air Quality Mgmt. Dist., 541 U.S. 246, 252 (2004). That statutory language specifies that a probable cause finding must be made for each facility "at which the electronic surveillance is directed." The statute provides four alternative definitions of electronic surveillance, but the one most pertinent to this case is at § 1801(f)(2).¹¹ Section 1801(f)(2) defines "electronic surveillance" as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition

¹⁰ For example, the manner of phone surveillance [redacted] proposed in this docket is identical to that proposed in Docket No. [redacted] for phone numbers used in the United States. Compare Docket No. [redacted] Declaration of Lt. Gen. Keith B. Alexander, Director, NSA at 3 (submitted as Attachment C to Application) (defining [redacted] with Alexander Decl. in this docket at 24-25 (same definition, but with references to [redacted] and to the "minimization probable cause standard"). [redacted] and b(7)(E)

[redacted] Proposed Order at 2-6.

¹¹ Section 1801(f)(2) provides the relevant definition of "electronic surveillance" for all of the proposed phone surveillance, as well as the proposed e-mail surveillance [redacted] Application at 19. In the government's view, the relevant definition for [redacted] See note 13 *infra* & accompanying text.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

occurs in the United States.” (Emphasis added.)¹² Thus, the electronic surveillance is the acquisition of the contents of communications.

In this case, communications will be acquired because they are to or from (or, in the case of Internet communications, refer to) a certain class of facilities - - - the telephone numbers and e-mail addresses used as selectors. NSA has no interest in acquiring the contents of [REDACTED]

[REDACTED] Rather, it is interested in acquiring only [REDACTED] Accordingly, NSA [REDACTED] to select for acquisition communications that relate to a selector facility, and to exclude from acquisition [REDACTED]

¹² The record does not disclose to what extent the surveillance conducted under Docket No. [REDACTED] (b)(7)(E)) has in fact acquired communications to or from a person in the United States. See Alexander Decl. at 22 n.36 (the “volume of communications targeted for collection” in Docket No. [REDACTED] (b)(7)(E)) makes it “technically infeasible” to provide such information, but “a central purpose” of such surveillance “is to collect communications to or from terrorist operatives in the United States”). However, given the large number of selectors involved [REDACTED]

[REDACTED] it appears likely that this surveillance would acquire some indeterminate number of communications to or from persons in the United States. See, e.g., id. at 6-8 [REDACTED]

In view of this apparent likelihood, the government’s implicit request that the Court exercise jurisdiction over the submitted application, the Court’s prior acceptance of jurisdiction in Docket No. [REDACTED] (b)(7)(E)) and prior decisions of this Court that have accepted jurisdiction in similar cases [REDACTED] (b)(7)(E))

[REDACTED] I assume for purposes of this order and opinion that this case does involve “electronic surveillance” as defined by FISA, such that this Court has jurisdiction. However, I believe that the jurisdictional issues regarding the application of FISA to phone numbers and e-mail addresses that are used exclusively outside the United States merit further examination. I further believe that Congress should also consider clarifying or modifying the scope of FISA and of this Court’s jurisdiction with regard to such facilities, given the large number of overseas e-mail addresses and phone numbers now identified by the government for surveillance, and the government’s assertions regarding the need for speed and agility in targeting such facilities as new ones are identified in the future. See pages 18-19 infra.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

[REDACTED] These facts strongly suggest that the acquisition of the contents of communications - - - that is, the electronic surveillance itself - - - is directed at the telephone numbers and e-mail addresses used as selectors.

In the government's view, a discrete part of the proposed e-mail surveillance, to be conducted [REDACTED] should be analyzed under the definition of "electronic surveillance" provided at § 1801(f)(4).¹³ Section 1801(f)(4) defines "electronic surveillance" to include "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication . . ." (Emphasis added.) A similar analysis applies under § 1801(f)(4): because the surveillance consists of monitoring to acquire information, and the only information to be acquired relates to the e-mail addresses used as selectors, the electronic surveillance would be directed at those e-mail addresses.

The government argues to the contrary that this surveillance is not [REDACTED]

[REDACTED] Government's Memorandum of Law at 32. But, nothing in the language of the statute identifies the facility at which the surveillance is directed [REDACTED] Congress could have used language that focused [REDACTED] but chose not to do so in § 1805(a)(3)(B). Compare § 1842(d)(2)(A)(iii) (requiring FISA pen register/trap and trace orders to specify, "if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied") (emphasis

¹³ The orders in Docket No. [REDACTED] b(7)(E) authorized surveillance [REDACTED] but NSA has not commenced such surveillance. NSA intends to do so within the next 90 days, but has not determined how such surveillance will be conducted, or even whether some part of its intended activity will involve [REDACTED] Alexander Decl. at 41 nn.49 & 52, 42 n.55.

¹⁴ Certainly the term "directed" cannot be construed to do so. See Webster's II New College Dictionary 321 (2001) (defining "direct" to mean, inter alia, "To move or guide (someone) toward a goal;" "To show or indicate the way to;" "To cause to move in or follow a direct or straight course <directed the arrow at the bull's-eye>;" "To address (e.g., a letter) to a destination.")

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

added). And, the relevant provisions assign no significance to the place where communications are acquired, so long as acquisition "occurs in the United States" (as is the case here).¹⁵

The government further argues that one portion of the proposed surveillance - - - the acquisition of e-mails that contain a reference to, but are not to or from, a selector e-mail address - - - cannot be conducted [REDACTED]

[REDACTED] Government's Supplemental Memorandum of Law at 6-7 (submitted as part of Exhibit A to the Application).¹⁶ However, even for this part of the surveillance, communications [REDACTED]

[REDACTED] The surveillance functions in this way because NSA is not interested in the contents of communications [REDACTED]; rather, it is only interested in the contents of those communications (to include the e-mail addresses of the communicants) that refer to a selector e-mail address. For these reasons, I find that this aspect of the proposed surveillance is not [REDACTED], but rather at particular e-mail addresses.¹⁷

The government also cites several prior cases as precedent for the interpretation of § 1805(a)(3)(B) adopted in Docket No. [REDACTED] b(7)(E) These cases involved very different

¹⁵ § 1801(f)(2); see also § 1801(f)(4) ("installation or use of a [] . . . surveillance device in the United States")

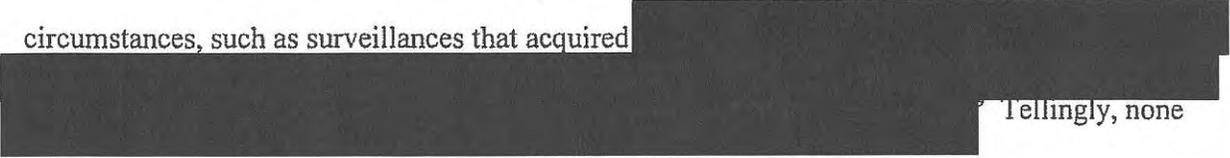
¹⁶ The government identifies [REDACTED] communications acquired by this aspect of the surveillance. Government's Supplemental Memorandum of Law at 6-7; Declaration of [REDACTED] b(3), b(6) and b(7) NSA (" [REDACTED] b(3) Decl.") at 16-18 (submitted as part of Exhibit A to the Application). [REDACTED] and b(6) and b(7) [REDACTED]

¹⁷ On the record before me, I cannot, and do not, decide exactly which particular e-mail addresses are the ones at which this type of surveillance is directed. To the extent it is concluded that surveillance is directed at e-mail addresses [REDACTED] a judge would have to find probable cause to believe that those e-mail addresses, [REDACTED] are being used or are about to be used by a foreign power or an agent of a foreign power before authorizing the surveillance proposed in the application.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

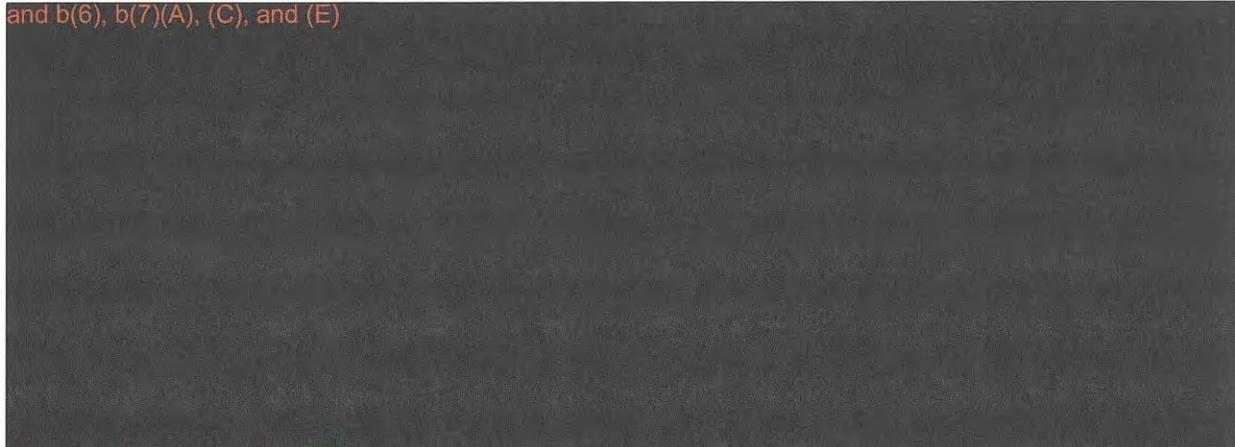
~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

circumstances, such as surveillances that acquired



Tellingly, none

and b(6), b(7)(A), (C), and (E)



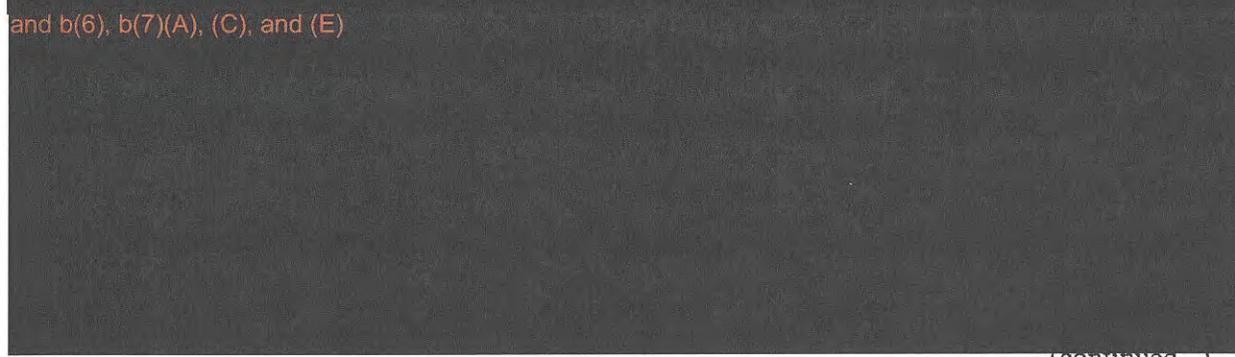
and b(6), b(7)(A), (C), and (E)



and b(6), b(7)(A), (C), and (E)



and b(6), b(7)(A), (C), and (E)



(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

of the cited cases stand for the proposition on which this application rests - - - that electronic surveillance is not "directed" at particular phone numbers and e-mail addresses.

Moreover, in each of the cited cases involving surveillance under § 1805,²⁰ the judge made probable cause determinations that a single target or well-defined set of targets

These determinations constrained the ability of executive branch officials to direct surveillance against persons and communications of their unilateral choosing in a way that, as discussed below, the proposed probable cause findings in this case would not.

Therefore, I conclude that, under the plain meaning of §§ 1805(a)(3)(B) and 1801(f), the proposed electronic surveillance is directed at the telephone numbers and e-mail addresses used as selectors. The result of applying this plain meaning is by no means absurd.²¹

¹⁹(...continued)

²⁰ One case relied on by the government involved different statutory requirements and no probable cause finding at all.

Docket No. PR/TT involved the use of pen registers and trap and trace devices to acquire addressing and routing information; not the full content of communications. Because issuing a FISA pen register/trap and trace order under § 1842 does not require the judge to make probable cause findings, the Opinion and Order entered on July 14, 2004, at 49 n.34, expressly disclaimed any application to full-content surveillances under § 1805.

²¹ See Laimie v. United States Trustee, 540 U.S. 526, 534 (2004) (court is to enforce plain language of a statute, "at least where the disposition required by the text is not absurd") (internal quotations omitted).

²² See notes 7 and 8 *supra*.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

and b(7)(E) [redacted] cases (other than this case and Docket No. [redacted]) consistently reflect the same understanding [redacted]

However, even if the statutory language were as elastic as the government contends, it would still be incumbent on me to apply the language in the manner that furthers the intent of Congress. In determining what interpretation would best further congressional intent, it is appropriate to consult FISA's legislative history.²⁵ That legislative history makes clear that the

²³ See, e.g., *In re* [redacted] and b(6), b(7)(C), and (E)

and b(6), b(7)(C), and (E)

and b(6), b(7)(A), (C), and (E)

²⁵ See *Train v. Colorado Public Interest Research Group*, 426 U.S. 1, 10 (1976). Moreover, if § 1805(a)(3)(B) could be applied in such widely varying ways to the same surveillance, then its terms would be sufficiently unclear that legislative history may be consulted (continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

purpose of pre-surveillance judicial review is to protect the fourth amendment rights of U.S. persons.²⁶ Congress intended the pre-surveillance “judicial warrant procedure,” and particularly the judge’s probable cause findings, to provide an “external check” on executive branch decisions to conduct surveillance.²⁷

Contrary to this intent of Congress, the probable cause inquiry proposed by the government could not possibly restrain executive branch decisions to direct surveillance at any particular individual, telephone number or e-mail address. Under § 1805(a)(3)(B), the government would have the Court assess [REDACTED]

[REDACTED] See Alexander Decl. at 6-8, 11-12], and make a highly abstract and generalized probable cause finding [REDACTED]. However, such a probable cause finding could be made with equal validity [REDACTED]

²⁵(...continued)

to ascertain their proper meaning. See, e.g., Blum v. Stenson, 465 U.S. 886, 896 (1984).

²⁶ “A basic premise behind this bill is the presumption that whenever an electronic surveillance for foreign intelligence purposes may involve the fourth amendment rights of any U.S. person, approval for such a surveillance should come from a neutral and impartial magistrate.” E.g., H. Rep. 95-1283, pt. 1, at 24-25; see also id. at 26 (purpose of extending warrant procedure to surveillances targeting non-U.S. persons “would not be primarily to protect such persons but rather to protect U.S. persons who may be involved with them”). Such protection was deemed necessary in view of prior abuses of national security wiretaps. Id. at 21 (“In the past several years, abuses of domestic national security surveillances have been disclosed. This evidence alone should demonstrate the inappropriateness of relying solely on executive branch discretion to safeguard civil liberties.”).

²⁷

The bill provides external and internal checks on the executive. The external check is found in the judicial warrant procedure which requires the executive branch to secure a warrant before engaging in electronic surveillance for purposes of obtaining foreign intelligence information. . . . For such surveillance to be undertaken, a judicial warrant must be secured on the basis of a showing of “probable cause” that the target is a “foreign power” or an “agent of a foreign power.” Thus the courts for the first time will ultimately rule on whether such foreign intelligence surveillance should occur.

S. Rep. 95-604, pt. 1, at 16, reprinted in 1978 U.S.C.C.A.N. 3904, 3917.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

[REDACTED] On this reading of § 1805(a)(3)(B), facts supporting or contradicting the government's belief that terrorists use the phone numbers and e-mail addresses for which information will be acquired are irrelevant to the judge's probable cause findings.²⁸

Thus, under the government's interpretation, the judge's probable cause findings have no bearing on the salient question: whether the communications to be acquired will relate to the targeted foreign powers.²⁹ As discussed below, the government would have all of the probable cause findings bearing on that question made by executive branch officials, subject to after-the-fact reporting to the Court, through processes characterized by the government as minimization. That result cannot be squared with the statutory purpose of providing a pre-surveillance "external check" on surveillance decisions, or with the expectation of Congress that the role of the FISA judge would be "the same as that of judges under existing law enforcement warrant procedures."³⁰

²⁸ The government argues that the Court has previously, and should here, apply the requirements of § 1805(a)(3) in a flexible, common-sense fashion. See, e.g., Government's Supplemental Memorandum of Law at 12-14. In some cases, the Court's probable cause findings have left the government with a degree of flexibility in precisely how the surveillance is directed

[REDACTED] But, none of the cited cases approach what the government proposes here - - - findings under § 1805(a)(3) that do nothing to limit the government's discretion regarding the persons effectively targeted for surveillance or the communications to be acquired by the surveillance.

²⁹ Judicial authorization and oversight of surveillance under FISA is analogous to the judicial role in domestic criminal surveillance under Title III. After comparing § 1805(a)(3)(B) with the requirements for a Title III wiretap, the Foreign Intelligence Surveillance Court of Review concluded: "FISA requires less of a nexus between the facilities and the pertinent communications than Title III, but more of a nexus between the target and the pertinent communications." In re Sealed Case, 310 F.3d at 740 (emphasis added). However, under the government's theory, the judge's probable cause findings have no bearing whatever on whether the communications actually acquired pertain to a target.

³⁰ H. Rep. 95-1283, pt. 1, at 25. Congress expected the judge to "assess the facts to determine whether certain of the substantive standards have been met," in "the traditional role of a judge in passing on a warrant application." Id.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

The government's proposed probable cause findings under § 1805(a)(3)(A) do not alter these conclusions. No matter how well-founded, a judge's assessment of probable cause to believe that [REDACTED] are foreign powers cannot, in the context of the government's proposal, provide any check on what or whose communications are intercepted.³¹ These foreign powers can only communicate (or otherwise act) through individual members or agents, who use particular phone numbers and e-mail addresses. Because none of the probable cause findings proposed by the government, under either prong of § 1805(a)(3), concerns these particular individuals, phone numbers, or e-mail addresses, the judge's role in making such findings cannot provide the "external check" intended by Congress.

Accordingly, I must conclude that, for purposes of § 1805(a)(3)(B), the phone numbers and e-mail addresses used as selectors are facilities at which the electronic surveillance is directed. I am unable, "on the basis of the facts submitted by the applicant," to find probable cause to believe that each of these facilities "is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* The application contains no facts that would support such a finding. Instead, it is represented that NSA will make the required probable cause finding for each such facility before commencing surveillance. Alexander Decl. at 43. The application seeks, in effect, to delegate to NSA the Court's responsibility to make such findings "based on the totality of circumstances." *See* proposed Order at 14-15.³² Obviously, this would be inconsistent with the statutory requirement and the congressional intent that the Court make such findings prior to issuing the order.³³

³¹ *See* S. Rep. 95-701 at 54, reprinted in 1978 U.S.C.C.A.N. 3973, 4023 (requirement that "the court, not the executive branch, make[] the finding of whether probable cause exists that the target of surveillance is a foreign power or its agent" is intended to be a "check[] against the possibility of arbitrary executive action").

³² Compare, e.g., H. Rep. 95-1823, pt. 1, at 43 ("judge is expected to take all the known circumstances into account" in assessing probable cause to believe that an individual is an agent of an international terrorist group) (emphasis added).

³³ This analysis of congressional purpose applies equally to the aspect of the surveillance that acquires communications that refer to a selector e-mail address, and supports the conclusion that such surveillance is not [REDACTED] identified by the government. This order and opinion does not decide which e-mail addresses are facilities at which such surveillance is directed. *See* note 17 *supra*.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

IV. MINIMIZATION

Another requirement for an electronic surveillance order under § 1805 is that the Court must also find that “the proposed minimization procedures meet the definition of minimization procedures under section 1801(h).” § 1805(a)(4). That section defines minimization procedures, in pertinent part, as

specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

§ 1801(h)(1). FISA minimization procedures cannot be framed “in a way that is clearly inconsistent with the statutory purpose.” *In re Sealed Case*, 310 F.3d at 730. More importantly, the minimization procedures must be consistent with the statutory text. *See, e.g., Laimie*, 540 U.S. at 538 (stressing the “difference between filling a gap left by Congress’ silence and rewriting rules that Congress has affirmatively and specifically enacted”) (internal quotations omitted). Accordingly, proposed minimization procedures that conflict with other provisions of FISA cannot be “reasonably designed” within the meaning of § 1801(h)(1).³⁴

It follows from this principle, and from the foregoing analysis of § 1805(a)(3)(B), that the record in this case will not support the finding required by § 1805(a)(4). The minimization procedures first approved in Docket No. [REDACTED] and proposed in this matter conflict with specific provisions of FISA that govern the initiation and extension of electronic surveillance authority. For example, under the proposed procedures, NSA may initiate surveillance of a foreign phone number or e-mail address unilaterally; express judicial approval is not required,

³⁴ This conclusion holds even if the proposed procedures arguably concern the “acquisition” of information under § 1801(h)(1). All of 50 U.S.C. §§ 1801-1811 regulates the acquisition of information by electronic surveillance. The requirement to adopt and follow reasonable minimization procedures is in addition to the statute’s other requirements for authorizing electronic surveillance, including the requirement that the judge make the probable cause findings specified at § 1805(a)(3). Minimization does not provide a substitute for, or a mechanism for overriding, the other requirements of FISA.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

even after the fact.³⁵ However, § 1805(f) provides that emergency approvals can only be granted by the Attorney General,³⁶ after which an application for electronic surveillance authority must be presented to a judge of this Court within 72 hours of emergency authorization, and surveillance must terminate within 72 hours of the emergency authorization unless a Court order, supported by the necessary probable cause findings, is obtained.

The proposed minimization procedures are also inconsistent with other express statutory requirements regarding the duration and extension of surveillance authorizations. Surveillances targeting foreign powers as defined by § 1801(a)(4) may be initially authorized for up to 90 days [§ 1805(e)(1)] and “extensions may be granted . . . upon an application for an extension and new findings made in the same manner as required for an original order.” § 1805(e)(2). Such “findings” must include a judge’s finding of probable cause to believe that each phone number or e-mail address at which surveillance is directed is being used or is about to be used by a foreign power or an agent of a foreign power. However, the proposed procedures make no provision for review of probable cause at any time after the surveillance is first reported to the Court.

The clear purpose of these statutory provisions is to ensure that, as a general rule, surveillances are supported by judicial determinations of probable cause before they commence; that decisions to initiate surveillance prior to judicial review in emergency circumstances are made at politically accountable levels; that judicial review of such emergency authorizations follows swiftly; and that decisions to continue surveillance receive the same degree of scrutiny as decisions to initiate. The law does not permit me, under the rubric of minimization, to approve or authorize alternative procedures to relieve the government of burdensome safeguards expressly imposed by the statute.

The government argues that alternative, extra-statutory procedures are necessary to provide or enhance the speed and flexibility with which NSA responds to terrorist threats. Government’s Memorandum of Law at 11-12; Government’s Supplemental Memorandum of Law at 4-5. It notes that, in the time it takes to get even an Attorney General emergency

³⁵ A report “briefly summariz[ing] the basis” for NSA’s probable cause findings in support of surveillance of new phone numbers and e-mail addresses would be submitted to the Court at 30-day intervals. Application at 8-9. If the Court concluded that there is not probable cause to believe that such a phone number or e-mail address is used by a targeted foreign power, it could direct that surveillance terminate “expeditiously.” *Id.* at 9.

³⁶ “Attorney General” is defined at § 1801(g) to include also the Acting Attorney General, the Deputy Attorney General, and, “upon designation,” the Assistant Attorney General for National Security.

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

authorization, vital foreign intelligence information may be lost. Government's Memorandum of Law at 11-12; Alexander Decl. at 20; [REDACTED] Decl. at 13-15. These matters concern me as well. But, these are risks that Congress weighed when it adopted FISA's procedural requirements,³⁷ over dissenting voices who raised some of the same concerns the government does now.³⁸ These requirements reflect a balance struck by Congress between procedural safeguarding of privacy interests and the need to obtain foreign intelligence information.

The procedures approved in Docket No. [REDACTED] and proposed in this application strike this balance differently for surveillance of phone numbers and e-mail addresses used overseas. However, provided that a surveillance is within the scope of FISA at all,³⁹ the statute applies the same requirements to surveillance of facilities used overseas as it does to surveillance of facilities used in the United States. Congress could well take note of the grave threats now presented by international terrorists and changes in the global communications system,⁴⁰ and conclude that FISA's current requirements are unduly burdensome for surveillances of phone numbers and e-mail addresses used overseas.⁴¹ Unless and until legislative action is taken, however, the judges of this Court must apply the procedures set out in the statute. See § 1803(a) (Court has "jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter") (emphasis added).

³⁷ See H.R. Rep. 95-1283, pt. 1, at 26 (acknowledging potential "risks of impeding or barring needed intelligence collection").

³⁸ FISA's "warrant requirement . . . would pose serious threats to the two most important elements in effective intelligence gathering: (1) speed and (2) security The real possibilities of delay . . . are risks the intelligence community should not be required to take." *Id.* at 113 (Dissenting views of Reps. Wilson, McClory, Robinson, and Ashbrook).

³⁹ This condition is assumed, but not decided, for purposes of this order and opinion. As noted elsewhere, I believe that there are jurisdictional issues regarding the application of FISA to communications that are between or among parties who are all located outside the United States. See note 12 *supra*.

⁴⁰ See, e.g., Alexander Decl. at 11 ([REDACTED])

⁴¹ *Id.* at 19 (burden of preparing FISA applications for [REDACTED]); Government's Supplemental Memorandum of Law at 4 (same); [REDACTED] Decl. at 13-14 (same).

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//XI~~

Fidelity to this principle “allows both [the legislative and judicial] branches to adhere to our respected, and respective, constitutional roles.” Laimie, 540 U.S. at 542.

For the foregoing reasons, I conclude that I cannot grant the application in Docket No. [REDACTED] in the form submitted. I recognize that the government maintains that the President may have “constitutional or statutory authority to conduct the electronic surveillance detailed herein without Court authorization.” Application at 25 n.12; see also Alexander Decl. at 6 n.6

[REDACTED] Nothing in this order and opinion is intended to address the existence or scope of such authority, or this Court’s jurisdiction over such matters.

V. REQUEST FOR LEAVE TO SEEK EXTENSION IN DOCKET NO. [REDACTED]

On March 29, 2007, I orally advised attorneys for the government that, after careful review of the application and supporting materials, I had reached the above-stated conclusion, and provided a brief summary of the reasoning more fully stated herein. I also stated that, if it chose to do so, the government could supplement the record at a formal hearing.

Based on ensuing discussions, I believe that the government may be able to submit a revised and supplemented application, on the basis of which I could grant at least a substantial portion of the surveillance authorities requested herein, consistent with this order and opinion. The government has undertaken to work toward that goal; however, it is understood that the government has not yet decided on a particular course of action and may, after further consideration, conclude that it is not viable to continue this surveillance within the legal framework stated in this order and opinion.

On April 2, 2007, the government filed in the above-captioned docket a Motion for Leave to File an Application for an Extension of the Orders Issued in Docket No. [REDACTED]. That motion requests leave to file an application for a 60-day extension of those authorities. Motion at 3. On April 3, 2007, the government informally advised that it did not wish to have a hearing on the record prior to my ruling on the motion. I have decided to grant the government leave to file such an application in Docket No. [REDACTED], subject to the requirements stated below.

The sole purpose for granting such leave is to give the government a reasonable amount of time to work in good faith toward the preparation and submission of a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion. I have concluded that an extension for this purpose is appropriate, in view of the following circumstances: that the government has commendably devoted substantial resources to bring the NSA’s surveillance program, which had been conducted under the President’s assertion

~~TOP SECRET//COMINT//ORCON,NOFORN//XI~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

of non-FISA authorities, within the purview of FISA; that a judge of this Court previously authorized this surveillance in Docket No. [REDACTED], on substantially the same terms as the government now proposes; that it would be no simple matter for the government to terminate surveillance of [REDACTED] phone numbers and e-mail addresses under FISA authority, and to decide whether and how it should continue some or all of the surveillance under non-FISA authority; and, importantly, that within the allotted time the government may be able to submit an application that would permit me to authorize at least part of the surveillance in a manner consistent with this order and opinion.

Accordingly, it is hereby ORDERED as follows:

(1) The government may submit an application for a single extension of the authorities granted in Docket No. [REDACTED]. Any authorities granted pursuant to such an application shall terminate no later than 5:00 p.m., Eastern Time, on May 31, 2007. There shall be no extensions beyond May 31, 2007.

(2) If an extension is obtained under paragraph (1), the government shall periodically submit written reports to me regarding its efforts to prepare and submit for my consideration a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion. The first report shall be submitted on or before April 20, 2007; the second report shall be submitted on or before May 4, 2007; and the third report shall be submitted on or before May 18, 2007.

(3) If, during the period of an extension obtained under paragraph (1), the government determines that it is not feasible or not desirable to submit a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion, it shall immediately notify me in writing of this determination. The submission of such notification shall relieve the government of the requirement to submit reports under paragraph (2). I contemplate that, upon receipt of such notification, I would enter an order formally denying the application in the above-captioned docket.

(4) If authorities obtained pursuant to any extension under paragraph (1) should expire before the government has submitted, and I have ruled on, a revised and supplemented application that would meet the requirements of FISA as described in this order and opinion, then this order and opinion shall be deemed a denial of the above-captioned application, on the grounds stated herein.

(5) Without my prior approval, the government may not submit additional briefing on the bases for my conclusion that I cannot grant this application in its present form. However, if the government continues to seek authority for the type of surveillance discussed at note 17 supra

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

and accompanying text, its further submissions shall include an analysis of the extent to which such surveillance is directed at selector e-mail addresses, and the extent to which it is directed at e-mail addresses that send or receive communications that are acquired because they refer to a selector e-mail address.

Done and ordered this 3^d day of April, 2007 in Docket No. [REDACTED]


ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

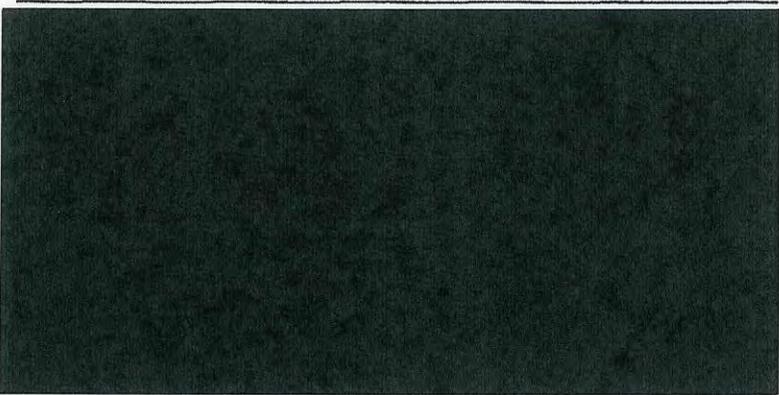
~~TOP SECRET//COMINT//ORCON,NOFORN//X1~~

[REDACTED] Clerk,
I, [REDACTED] that this document
is a true and correct copy
of the original. [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

All redacted information
exempt under b(1) and/
or b(3) except where
otherwise noted.

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.



Docket Number: PR/TT

PRIMARY ORDER

A verified application having been made by a designated attorney for the Government and approved 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 that:

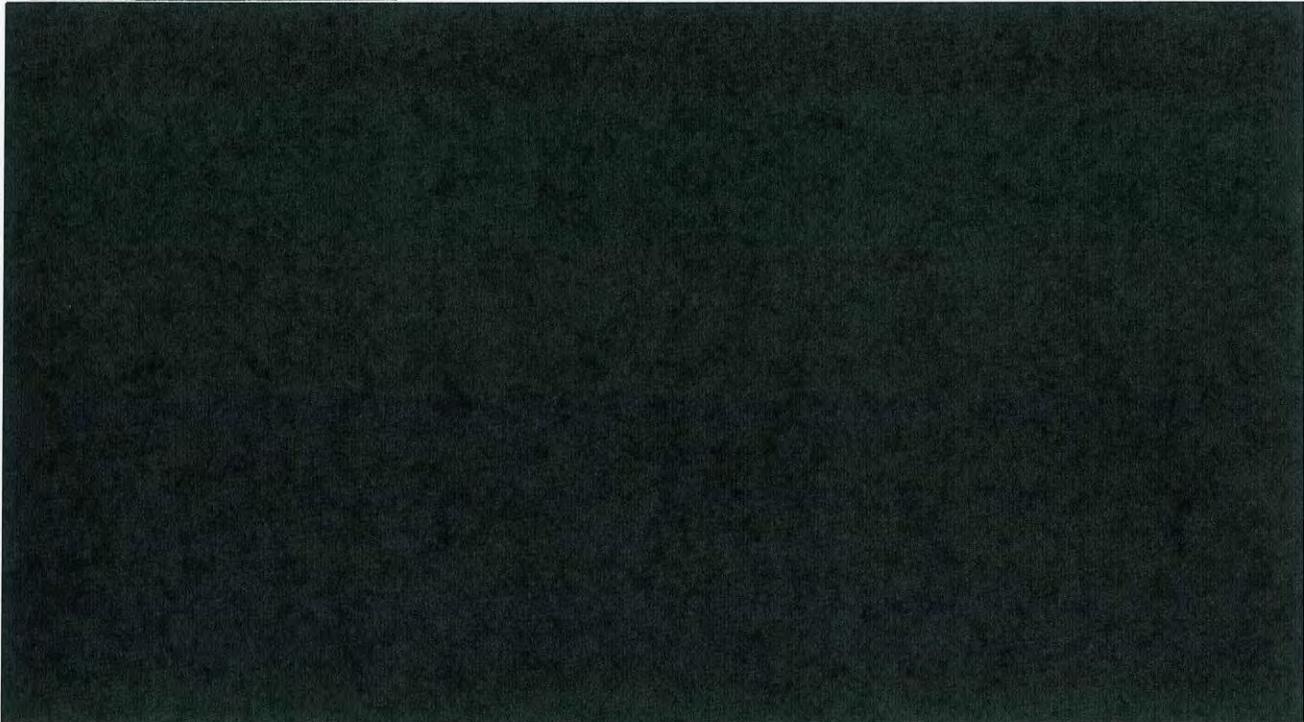
~~TOP SECRET//COMINT//NOFORN~~

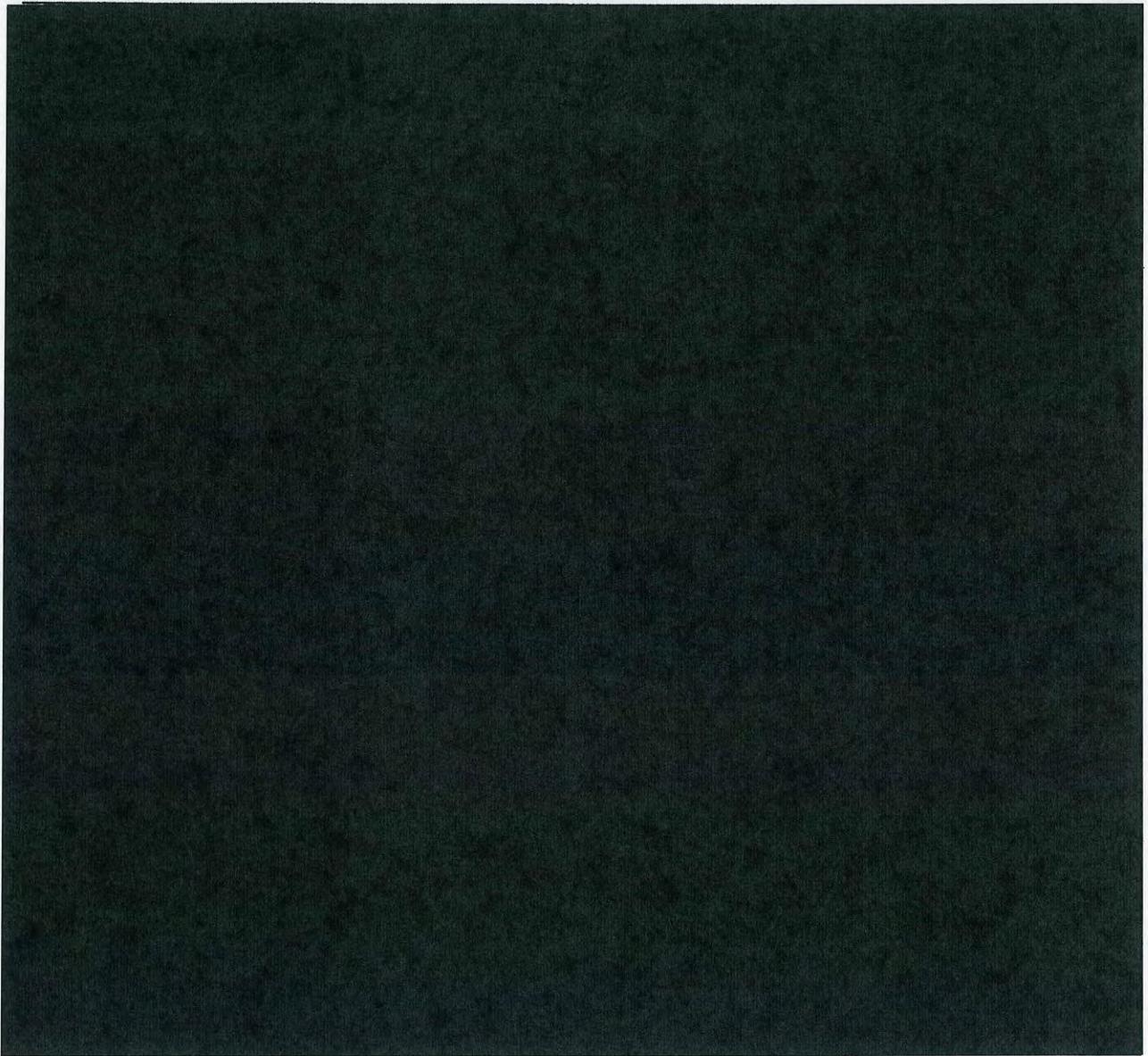
Derived from: Pleadings in the above-captioned docket
Declassify on:

1. The Attorney General is authorized to approve applications for pen registers and trap and trace devices under the Act, and the Attorney General or a designated attorney for the Government is authorized 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 ongoing investigations to protect against international terrorism that are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

3. 





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 12333, as amended.

4. The pen registers and trap and trace devices shall be [REDACTED] described in Tab 1 to the Declaration of [REDACTED] Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate (SID), NSA, which is attached to the Government's Application as Exhibit A.³

WHEREFORE, relying on and adopting the conclusions and analysis set out in its July 14, 2004, Opinion and Order in docket number PR/TT [REDACTED] and the Supplemental Opinion issued on [REDACTED] in docket number PR/TT [REDACTED] which the Court finds applicable to each authorized [REDACTED] as described in Tab 1 to Exhibit A of the Application, the Court finds that the Application of the United States to install and use pen registers and trap and trace devices, as described in the

³ [REDACTED]

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, 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 are authorized for a period of ninety days from the date of this 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 the [REDACTED] identified above, including the "to," "from," "cc," and "bcc" fields for those communications [REDACTED]

[REDACTED]

[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]

[REDACTED] (specified persons) are directed to furnish the NSA with any information, facilities, or technical assistance necessary to accomplish the installation and operation of pen registers and trap and trace devices, for purposes of targeting [REDACTED]

[REDACTED]

[REDACTED] 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 and the Director of Central Intelligence 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 persons 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 authorized 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 registers 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.⁴

b. The ability to retrieve information derived from the pen register and trap and trace devices shall be limited to [REDACTED] specially cleared analysts

⁴

[REDACTED]

and to specially cleared technical personnel.⁵ 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] [REDACTED] described at page 43 of the Court's July 14, 2004, Opinion and Order in docket number PR/TT [REDACTED]. 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 such [REDACTED] [REDACTED] is associated with [REDACTED] [REDACTED] [REDACTED] provided, however, that

⁵ The Court understands that certain processes must be performed by NSA technical personnel in order to make the metadata collected pursuant to this Order usable by analysts. The restrictions on access contained in this Order shall not apply to those processes.

an [REDACTED] believed to be used by a U.S. person shall not be regarded as [REDACTED]

[REDACTED] solely on the basis of activities that are protected by the First

Amendment to the Constitution. Further, all metadata queries shall be performed in accordance with this Court's

[REDACTED] Orders in docket numbers PR/TT [REDACTED], PR/TT [REDACTED] and PR/TT [REDACTED]. Queries shall only be conducted with the approval of one of the following twenty-three NSA officials: the Chief, Special Foreign Intelligence Surveillance Act (FISA) Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate (SID), NSA; the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. E-mail [REDACTED] that are the subject of electronic surveillance and/or physical search authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by agents of [REDACTED]

[REDACTED] including those used by U.S. persons, may be deemed approved for metadata querying without approval of an NSA official. The preceding sentence is not meant to apply to e-mail [REDACTED] [REDACTED] under surveillance pursuant to any certification of the Director of National Intelligence and the Attorney General, pursuant to Section 105B of FISA as added by the Protect America Act of 2007, or Section 702 of FISA, as added by the FISA Amendments Act of 2008. Nor is it intended to apply to e-mail [REDACTED] under surveillance pursuant to an Order of this Court issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

d. The Court understands that the processes described in paragraph (c)(i) and (c)(ii) at pages 7-11 of the 90-Day Report attached to the Application at Tab B are no longer in use. The Government shall not resume use of either of those processes without obtaining prior Court approval.

e. 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 metadata in online storage based on seed accounts used by U.S. persons;⁶ and

iv) at least twice during the 90-day authorized period of surveillance, conduct random spot checks on [REDACTED] to ensure that the collection is functioning as authorized by the Court. Such spot checks shall include an examination of a sample of the data.

⁶ The Court notes that, in conventional pen register/trap and trace surveillances, there is judicial review of the application before any particular e-mail account is targeted. In this case, the analogous decision to use a particular e-mail account as a seed account takes place without prior judicial review. In these circumstances, it shall be incumbent on NSA's Office of General Counsel to review the legal adequacy for the bases of such queries, including the First Amendment proviso, set out in paragraph c. above.

f. The NSA shall apply the Attorney General-approved guidelines in United States Signals Intelligence Directive 18 (Attachment D to the application in docket number PR/TT [REDACTED] 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 Information Sharing Services 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.

g. Information obtained from the authorized pen registers and trap and trace devices shall be available online for querying, as described in paragraphs b. and c. above, for four and one-half years. Metadata shall be destroyed no later than four and one-half years after its initial collection.

h. Every thirty days during the authorized period of surveillance, NSA shall file with the Court a report that includes: (i) a discussion of the queries that have been made since the prior report to the Court and the NSA's application of the standard set out in paragraph c. above

to those queries; and (ii) any changes in the description of the [REDACTED] described above [REDACTED]

[REDACTED]

i. **Additional Oversight Mechanisms.** In addition, the Government shall implement the following additional oversight mechanisms to ensure compliance with this Order:

i) NSA's OGC shall consult with the Department of Justice's National Security Division (NSD) on all significant legal opinions that relate to the interpretation, scope, and/or implementation of the authorizations granted by the Court in this matter. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

ii) NSA's OGC shall promptly provide NSD with copies of all formal briefing and/or training materials (including all revisions thereto) currently in use or prepared and used in the future to brief/train NSA personnel concerning the authorizations granted by this Order.

iii) At least once before the expiration of the authorities granted herein, a meeting for the purpose of assessing compliance with this Court's orders in

this matter shall be held with representatives from NSA's OGC, NSD, and appropriate individuals from NSA's SID. 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 authorities granted herein.

iv) At least once before the expiration of the authorities granted herein, NSD shall meet with NSA's Office of Inspector General (OIG) to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders in this matter.

v) Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC and NSD.

vi) At least once every ninety days, NSA's OGC and NSD shall review a sample of the justifications for querying the metadata, including e-mail [REDACTED] placed on an alert list.

In addition, should the United States seek renewal of these authorities, at that time it shall file a report that includes:

(i) detailed information regarding any new facilities proposed to be added to such authority; and (ii) any changes in the proposed means of collection, [REDACTED]

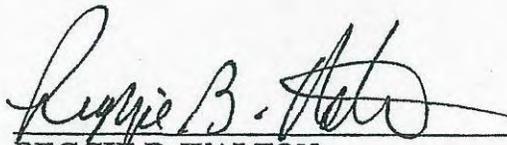
[REDACTED] of the pen registers and/or trap and trace devices.

Signed. [REDACTED] P04:06 E.T.
Date Time

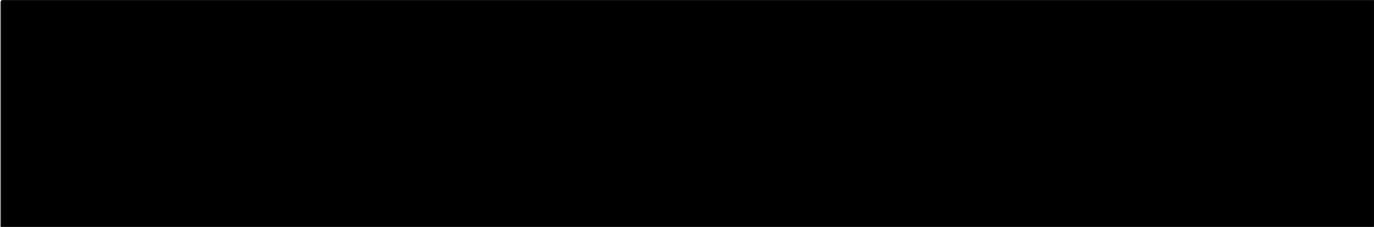
This authorization regarding [REDACTED]

[REDACTED]

[REDACTED] expires on the [REDACTED] at 5 p.m., Eastern Time.


REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.



MEMORANDUM OPINION
and
ORDER

This matter is before the Court on the Government's Ex Parte Submission of

[REDACTED] and Related Procedures and Request for an Order Approving [REDACTED]

[REDACTED] and Procedures, filed on [REDACTED] 2009 ([REDACTED] Submission" [REDACTED]

[REDACTED] pursuant to 50 U.S.C. § 1881a(g). For the reasons stated below, the government's request for approval is granted.

I. BACKGROUND

A. [REDACTED] Certifications Submitted Under Section 1881a

The [REDACTED] Submission includes [REDACTED] filed by the government pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which was enacted as part of the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (Jul. 10, 2008)

(“FAA”), and is now codified at 50 U.S.C. § 1881a [REDACTED] certifications were submitted [REDACTED] (collectively, the “Original 702 Dockets”). Like the government’s submissions in the Original 702 Dockets, the [REDACTED] Submission in the above-captioned docket includes [REDACTED] by the Attorney General and the Director of National Intelligence (“DNI”); supporting affidavits by the Director of the National Security Agency (“NSA”), the Director of the Federal Bureau of Investigation (“FBI”), and the Director of the Central Intelligence Agency (“CIA”); two sets of targeting procedures, for use by the NSA and FBI respectively; and three sets of minimization procedures, for use by the NSA, FBI, and CIA respectively.

[REDACTED] now before [REDACTED] [REDACTED] in Docket No. 702(i)-08-01, which governs the collection of foreign intelligence information [REDACTED]

[REDACTED] Like the acquisitions authorized in the certifications approved by the Court in the Original 702 Dockets, [REDACTED] under review [REDACTED] limited to “the targeting of non-United States persons reasonably believed to be located outside the United States.” [REDACTED] Or [REDACTED] 2008, [REDACTED] April 7, 2009, the Court issued Memorandum Opinions and accompanying orders approving the certifications [REDACTED]

[REDACTED]

On [REDACTED] 2009, respectively, the Director of National Intelligence and the Attorney General executed amendments to the certifications [REDACTED] [REDACTED] for the purpose of authorizing the FBI to use, under those certifications, the same revised FBI minimization procedures that were submitted to and approved by the Court in connection with [REDACTED]. See [REDACTED] 2009 Memorandum Opinion at 3. On [REDACTED] 2009, the Court issued a Memorandum Opinion and accompanying order approving the amendments. *Id.* at 6. Each of the Court's Memorandum Opinions in the Original 702 Dockets (to include the [REDACTED] 2009 Memorandum Opinion) is incorporated by reference herein.

B. The Government's Representations

On [REDACTED] 2009, following a meeting with the Court staff, the United States submitted the Government's Response to the Court's Questions Posed by the Court (the [REDACTED] [REDACTED] Submission").¹ In that submission, the government indicates that each set of targeting and minimization procedures now before the Court is either substantively identical, or very similar, to procedures previously approved by the Court in the Original 702 Dockets.² [REDACTED]

¹ [REDACTED]

² See Procedures Used by NSA for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended ("NSA Targeting Procedures") (attached [REDACTED]) (continued...)

Submission at 13-14. Notwithstanding such similarity, the government notes a few cross-cutting changes from the earlier approved procedures. First, in the various procedures submitted [REDACTED] [REDACTED] the government throughout uses “will” rather than “shall, which had been used in the prior sets of procedures. [REDACTED] Submission at 1.³ The government avers that this change ‘[is] purely stylistic and ... not intended to suggest that each agency’s obligation to comply with the requirements set forth in their respective targeting and/or minimization procedures submitted with [REDACTED] diminished in any way.’ Id. Second, the government has changed the deadline for complying with various reporting requirements from “seven days” to “five business days.” Id. at 2. According to the government, this change “is intended to remove any potential ambiguity in calculating the deadline for reporting matters as required.” Id. Finally, the government has added to the NSA and CIA Minimization Procedures an emergency provision similar to that which already had

²(...continued)

[REDACTED] as Exhibit A); Procedures Used by the FBI for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended (“FBI Targeting Procedures”) (attached [REDACTED] as Exhibit C).

See Minimization Procedures Used by the NSA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended (“NSA Minimization Procedures”) (attached [REDACTED] as Exhibit B); Minimization Procedures Used by the FBI in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended (“FBI Minimization Procedures”) (attached [REDACTED] as Exhibit D); Minimization Procedures Used by the CIA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA, as Amended (“CIA Minimization Procedures”) (attached [REDACTED] as Exhibit E).

³This change also is reflected in the Affidavit submitted by Lt. Gen. Keith B. Alexander, U.S. Army, Director, NSA (attached [REDACTED] at Tab 1) at 3-4.

been included in the FBI Minimization Procedures. [REDACTED] NSA Minimization Procedures at 1, CIA Minimization Procedures at 6 [REDACTED] Submission at 2.

Apart from these across-the-board changes, the government confirms that the NSA and FBI targeting procedures are virtually identical to those submitted to and approved by the Court

[REDACTED] Submission at 13. Similarly, the

government represents that the FBI Minimization Procedures now before the Court are in all

material respects identical to the FBI Minimization Procedures approved by the Court [REDACTED]

[REDACTED] and again in connection with the [REDACTED] amendments to the certifications [REDACTED]

[REDACTED] Id. at 14. Likewise, the NSA Minimization

Procedures at bar are nearly identical to the corresponding procedures approved by the Court [REDACTED]

[REDACTED] ⁴ Id. at 13-14.⁵

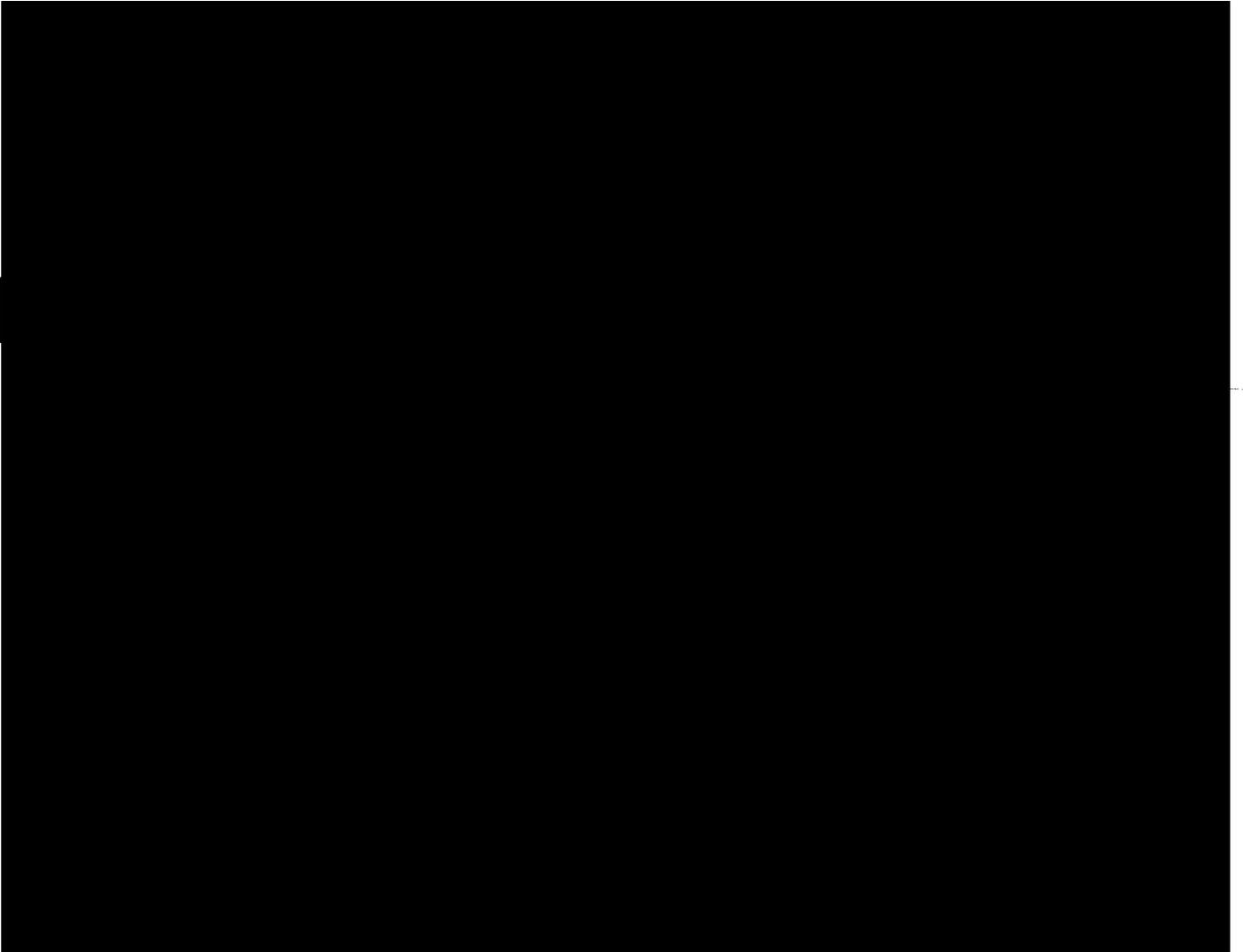
The CIA Minimization Procedures, while substantially similar to the procedures approved by the Court [REDACTED] include a few material

⁴

⁵In a departure from the previous minimization procedures, the NSA Minimization Procedures submitted in this docket do not characterize the transfer of unminimized information from NSA to the FBI and the CIA as “disseminations,” but rather as the provision of information. The government made this change “so that the description of the information-sharing regime established by the NSA minimization procedures ... is consistent with the Court’s opinion in [REDACTED]

[REDACTED] Submission at 4-5. The Court does not understand this change of wording to modify or limit the requirements governing such “provision” or “dissemination” of information.

differences. The procedures submitted in this Docket incorporate a handful of provisions that had not been in the prior minimization procedures but are part of [REDACTED]



6

7

The Court has carefully reviewed the instant Procedures and has found that, with the exception of the above-described differences and certain non-material changes, the procedures submitted in the current Docket, as informed by the [REDACTED] Submission, mirror those submitted and approved by the Court in the Original 702 Dockets and their amendments.

II. REVIEW [REDACTED]

The Court must review a certification submitted pursuant to Section 702 of FISA “to determine whether [it] contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court’s examination [REDACTED] submitted in the above-captioned docket confirms that:

- (1) [REDACTED] been made under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), [REDACTED]
- (2) [REDACTED] each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), *id.* at 1-3;
- (3) as required by 50 U.S.C. § 1881a(g)(2)(B), [REDACTED] accompanied by the applicable targeting procedures⁸ and minimization procedures;⁹
- (4) [REDACTED] supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);¹⁰ and

⁸ See [REDACTED] NSA Targeting Procedures and FBI Targeting Procedures.

⁹ See [REDACTED] NSA Minimization Procedures, FBI Minimization Procedures, and CIA Minimization Procedures.

¹⁰ See [REDACTED] Affidavit of Lt. Gen. Keith B. Alexander, U.S. Army, Director, NSA (attached [REDACTED] at Tab 1); Affidavit of Robert S. Mueller, III, Director, (continued...)

(5) [REDACTED] an effective date for the authorization in compliance with 50 U.S.C. § 1881a(g)(2)(D) [REDACTED]

Accordingly, the Court finds that [REDACTED] submitted [REDACTED] “contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A).

III. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is required to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). 50 U.S.C. § 1881a(i)(2)(B) and (C). Section 1881a(d)(1) provides that the targeting procedures must be “reasonably designed” to “ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States” and to “prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” Section 1881a(e)(1) requires that the “minimization procedures [] meet the definition of minimization procedures under section 1801(h) or 1821(4) of [the Act]...” In addition, the Court must determine whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A).

¹⁰(...continued)

FBI (attached [REDACTED] at Tab 2); Affidavit of Leon E. Panetta, Director, CIA (attached [REDACTED] at Tab 3).

¹¹ The statement described in 50 U.S.C. § 1881a(g)(2)(E) is not required in this case because there has been no “exigent circumstances” determination under Section 1881a(c)(2).

Based on the Court's review of the targeting and minimization procedures in the above-captioned Docket, the representations of the government made in this matter and those carried forward from the Original 702 Dockets, and the analysis set out below and in the Memorandum Opinions of the Court in the Original 702 Dockets and their amendments, the Court finds that the targeting and minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.

As discussed above, the targeting and minimization procedures are, in substantial measure, the same as those previously found to comply with the requirements of the statute and with the Fourth Amendment to the Constitution. The few substantive changes noted do not change the Court's assessment. There is no statutory or constitutional significance to the change from a seven day reporting deadline to five business days. Nor is the Court concerned about the government's use of "will" rather than "shall," given the government's assurance that the change is merely stylistic. And, the Court is satisfied that U.S. person information will be properly protected through the processes described in the CIA Minimization Procedures, [REDACTED] [REDACTED] In fact, only two changes even have the potential to require that the Court re-assess its prior determinations.

For the first time, both NSA and CIA include a provision in their Minimization Procedures that allows the agency to act in apparent departure from the procedures to protect against an immediate threat to human life. [REDACTED] NSA Minimization Procedures at 1, CIA Minimization Procedures at 6. However, these emergency provisions are

virtually identical to a provision in the FBI Minimization Procedures that were approved [REDACTED]

[REDACTED] The government has informed the Court that the one substantive difference - the absence of a time frame by which the agency must notify the DNI and NSD of the exercise of the emergency authority - was inadvertent and that both the NSA and CIA have represented to the Department of Justice that they, like the FBI, will promptly report any emergency departure. [REDACTED]

Submission at 2.



The new standard, [REDACTED] continues to require a foreign intelligence purpose for retaining such information; the procedures only permit the retention of such [REDACTED] [REDACTED] “consistent with the need of the United States to ... produce and disseminate foreign intelligence information.” 50 U.S.C. §1801(h)(1). As the Court noted in its September 4, 2008 Memorandum Opinion, procedures that meet this requirement contribute to the Court’s assessment that such procedures comport with the Fourth

Amendment. Id. at 40.

In addition to the procedures themselves, however, the Court must examine the manner in which the government has implemented them. In its April 7, 2009 Memorandum Opinion, the Court acknowledged that while the potential for error was not a sufficient reason to invalidate surveillance, the existence of actual errors may “tip the scales toward prospective invalidation of the procedures under review...” Id. at 27. In its [REDACTED] Submission, the government reports on [REDACTED] compliance matters that had previously been the subjects of preliminary notices to the Court, [REDACTED] which involve NSA and one of which involves the CIA.¹² Id. at 5-11.

The NSA problems principally involve analysts improperly acquiring the communications of U.S. persons. Id. In response to these incidents, NSA’s Office of Oversight and Compliance has instituted several procedures designed to ensure more rigorous documentation of targeting decisions in order to minimize the likelihood that NSA analysts will improperly target U.S. persons or persons located within the U.S. Id. at 7, 8. In addition, NSA has conducted remedial training not only of the individual analysts who committed the errors, but the offices and management chains involved. Id. at 6-9.

The CIA problem is more discrete although arguably more troubling because it reflects a profound misunderstanding of minimization procedures, the proper application of which contribute significantly to the Court’s finding that such procedures comport with the statute and

¹²The government reports that it is aware of no new compliance incidents resulting from [REDACTED] over-collection [REDACTED]. See April 7, 2009 Memorandum Opinion at 17-27 for a full discussion [REDACTED] incident before the Court [REDACTED]

the Fourth Amendment. A [REDACTED] who no longer works with or has access to FISA information, improperly minimized at least [REDACTED] reports that were disseminated to NSA, FBI, and DOJ. [REDACTED] 2009, Preliminary Notice of Compliance Incident Regarding Collection Pursuant to Section 105B of the Protect America Act and Section 702 of the FISA, as Amended; [REDACTED] Submission at 9-11. Recognizing that if one person so significantly misunderstood the minimization regime, others might as well, the “ODNI, NSD, and CIA have been working together to implement procedures that will facilitate more comprehensive oversight of CIA’s applications of its minimization procedures in the future.” [REDACTED] Submission at 10. In addition, “CIA has made several process and training changes as a result of [this incident]. *Id.* at 11.

Given the remedial measures implemented in both agencies as a result of the compliance incidents reported to the Court, the Court is satisfied that these incidents do not preclude a finding that the targeting and minimization procedures submitted in the above-captioned docket satisfy the requirements of the FAA and the Fourth Amendment.

The Court, however, is aware that both NSA and FBI have identified additional compliance incidents that have not been reported to the Court. Through informal discussion between NSD attorneys and the Court staff, and later confirmed at a hearing held on [REDACTED] 2009 to address these matters, the Court learned that the government’s practice has been to report only certain compliance incidents to the Court: those that involve systemic or process issues, those that involve conduct contrary to a specific representation made to the Court, and those that involve the improper targeting of U.S. persons under circumstances in which the analyst knew or

should have known that the individual was a U.S. person.

Consistent with the government's practice, the Court was not notified of numerous incidents that involved the failure to de-task accounts once NSA learned that non-U.S. person targets had entered the United States. Indeed, in the ██████████ 2009 hearing, the government informed the Court that in addition to ██████████ incidents informally reported on ██████████, 2009 to the FISC staff, there were approximately ██████████ other similar incidents, all of which occurred since ██████████ 2008. The government reported at the hearing that while the de-tasking errors did not all stem from the same problem, NSA has instituted new ██████████ processes to minimize the likelihood of these types of de-tasking errors recurring. In addition, the government informed the Court that NSA's system for conducting post-targeting checks provides an effective backstop in the government's efforts to de-task accounts ██████████ ██████████. Finally, the government confirmed to the Court that NSA has purged from its systems all communications acquired during the period of time when these accounts should have been de-tasked. Based on these representations, the Court is satisfied that these incidents do not rise to the level of undermining the Court's assessment that the targeting and minimization procedures comport with the statute and the Fourth Amendment.

However, the Court is concerned that incidents of this sort were not reported to the Court, in apparent contravention of Rule 10(c) of Foreign Intelligence Surveillance Court Rules of Procedures.¹³ Section 702(i)(2)(B) specifically directs the Court to review the targeting

¹³The Court appreciates the assurances offered by the Department of Justice at the ██████████
(continued...)

procedures “To assess whether [they] are reasonably designed to ensure that any acquisition ... is limited to targeting persons reasonably believed to be located outside the United States and prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” Given the Court’s obligations under the statute, and consistent with 50 U.S.C. § 1803(i), the Court

HEREBY ORDERS the government, henceforth, to report to the Court in accordance with the Rule 10(c) of Foreign Intelligence Surveillance Court Rules of Procedure, every compliance incident that relates to the operation of either the targeting procedures or the minimization procedures approved herein.

IV. CONCLUSION

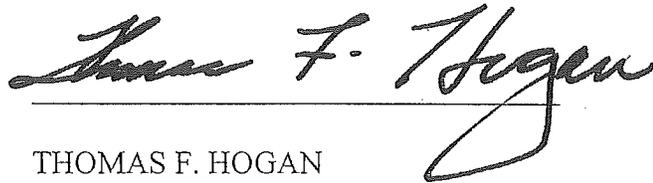
For the foregoing reasons, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that [REDACTED] submitted in the above-captioned docket “in accordance with [Section 1881a(g)] [REDACTED] all the required elements and that the targeting and minimization procedures adopted in accordance with [Section 1881a(d)-(e)] are consistent with the requirements of those

¹³(...continued)

[REDACTED] 2009 hearing that, henceforth, the government will work with the Court, through the Court’s counsel, to ensure that the government’s guidelines for notifying the Court of compliance incidents satisfy the needs of the Court to receive timely, effective notification of such incidents.

subsections and with the fourth amendment to the Constitution of the United States.” A separate order approving [REDACTED] and the use of the procedures pursuant to Section 1881a(i)(3)(A) is being entered contemporaneously herewith.

ENTERED this [REDACTED] 2009.



THOMAS F. HOGAN
Judge, United States Foreign
Intelligence Surveillance Court

exempt under b(6)

Deputy Clerk
is a true and correct copy of
the original
exempt
under b(6)

~~SECRET~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.



ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the above-captioned [REDACTED] submitted in accordance with [50 U.S.C. § 1881a(g)] [REDACTED] all the required elements and that the targeting and minimization procedures adopted in accordance with [50 U.S.C. § 1881a(d)-(e)] are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States.”

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that [REDACTED] [REDACTED] and the use of such procedures are approved.

ENTERED this [REDACTED] 2009.

THOMAS F. HOGAN
Judge, United States Foreign
Intelligence Surveillance Court

exempt under b(6)

Deputy Clk.
This copy of the document
is a true and correct copy of
the original

exempt
under b(6)

~~SECRET~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, DC

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM

[REDACTED]

Docket Number: BR 09-15

[REDACTED]

SUPPLEMENTAL OPINION AND ORDER

On October 30, 2009, the Court authorized the acquisition by the National Security Agency (“NSA”) of the tangible things sought in the government’s application in the above-captioned docket (“BR metadata”). This supplemental opinion and order reiterates the manner in which query results may be shared within the NSA, as informed by the testimony provided by government, and elaborates on the reporting requirement imposed in the Court’s order of October 30.

Sharing of BR Metadata Query Results Within the NSA

The Court's order permits NSA analysts who are authorized to query the BR metadata to share the results of authorized queries among themselves and with other NSA personnel, "provided that all NSA personnel receiving such query results in any form (except for information properly disseminated outside NSA) shall first receive appropriate and adequate training and guidance regarding the rules and restrictions governing the use, storage, and dissemination of such information." Primary Order at 15, Docket No. BR 09-15 (October 30, 2009) ("October 30 Order"). The order further provides: "[a]ll persons authorized for access to the BR metadata and other NSA personnel who are authorized to receive query results shall receive appropriate and adequate training by NSA's [Office of General Counsel] concerning the authorization granted by this Order, the limited circumstances in which the BR metadata may be accessed, and/or other procedures and restrictions regarding the retrieval, storage, and dissemination of the metadata." *Id.* at 13. The Court's prior order in this matter contained identical provisions. Primary Order at 12, 14-15, Docket No. BR 09-13 (September 3, 2009) ("September 3 Order").

In September, 2009, the Court received oral notification that NSA analysts had, on two occasions, shared the results of queries of the BR metadata with NSA analysts involved in the [REDACTED] investigation who had not received "appropriate and adequate training and guidance" as required under the September 3 Order. Order Regarding Further Compliance Incidents at 2-3, Docket No. BR 09-13 (September 25, 2009). On September 25, 2009, the Court ordered representatives of the NSA and the National Security Division ("NSD") of the

Department of Justice to appear for a hearing in order to inform the Court more fully of the scope and circumstances of the incidents, and to allow the Court to assess whether the Court's order should be modified or rescinded and whether other remedial steps should be imposed. *Id.* at 4.

At the hearing, which was conducted on September 28, 2009, the government confirmed that NSA analysts authorized to query the BR metadata had sent query results to NSA personnel who had not received the training and guidance required by the Court's September 3 Order. Transcript at 6-7, Docket No. BR 09-13. Specifically, the government reported that the NSA had created an e-mail distribution list (the NSA representative referred to this list as an "alias") for the 189 NSA analysts who were working on the "[REDACTED]" threat, only 53 of whom had received the required training and guidance. *Id.* at 6-7, 12-13. On September 17th, an NSA analyst authorized to query the BR metadata sent an e-mail to the [REDACTED] alias that included a "general analytic summary" of the results of a query of the BR metadata. *Id.* at 7. After a recipient brought the e-mail to the attention of the NSA's Oversight and Compliance Office and Office of General Counsel, the Oversight and Compliance Office issued guidance on September 21st, "reemphasizing the point, no dissemination of query results in any form." *Id.* at 14. The NSA's Counter-terrorism organization sent a similar reminder on the morning of September 22nd, however, that afternoon, a second NSA analyst who was authorized to query the BR metadata sent a situation report to the [REDACTED] alias that contained information derived from a query of the BR metadata. *Id.* at 15.

The government testified at the hearing that the NSA has taken steps to ensure that any sharing of the results of queries of the BR metadata within the NSA is fully consistent with the

Court's orders. First, the NSA has issued guidance interpreting "query results in any form," to mean any information of any kind derived from the BR metadata. *Id.* at 16. Second, NSA aliases for sharing information that could include BR metadata query results, will be limited to NSA personnel who have received the necessary training and guidance to receive those query results. *Id.* at 21-22. The Court hereby affirms that the NSA may share BR metadata query results in this manner consistent with the Court's October 30 Order. The only exception to this practice is under circumstances in which the Court has expressly authorized a deviation.¹

Report on Queries Described in Footnote 6 of the Court's October 30 Order

According to the government, one advantage of the BR metadata repository is that it is historical in nature, reflecting contact activity from the past that cannot be captured in the present or prospectively. Declaration of [REDACTED] at 7, Docket No. BR 09-15. At the government's request, the Court's September 3 Order and October 30 Order both acknowledge that the government may query the BR metadata for historical purposes, using a telephone identifier that is not currently associated with one of the targeted foreign powers, but that was for a period of time in the past.²

¹ For example, pursuant to paragraph (3)J of the Court's order, NSA personnel authorized to query the BR metadata may use and share the identity of high-volume telephone identifiers and other types of identifiers not associated with specific users for purposes of metadata reduction and management, without regard to whether the recipient has received the training and guidance required for access to BR metadata query results.

² Both orders contain the following footnote: "The Court understands that from time to time the information available to designated approving officials will indicate that a telephone identifier was, but may not presently be, or is, but was not formerly, associated with [REDACTED]. In such a circumstance, so long as the designated approving official can determine that the reasonable, articulable suspicion standard can be met for a particular period of time with respect to the telephone identifier, NSA may query the BR metadata using that telephone identifier. However, analysts conducting queries using such telephone identifiers must be made aware of the time period for (continued...)"

Nevertheless, the NSA's querying of the BR metadata using telephone identifiers that do not currently satisfy the "reasonable articulable suspicion" standard has been a source of concern for the Court. Given that telephone providers regularly re-assign telephone identifiers, and in light of the fact that the NSA acquires approximately [REDACTED] call detail records per day, the vast majority of which are irrelevant to the Federal Bureau of Investigation's ("FBI") investigations and concern communications of United States persons in the United States, it would appear likely that such a query could produce results that include metadata from United States persons not under investigation by the FBI. In order to allay these concerns, the Court's September 3 Order mandated that any application to renew or reinstate the authority granted therein must include a report describing, among other things, how the NSA has conducted [these types of queries] and minimized any information obtained or derived therefrom. September 3 Order at 18.

The government's report submitted as Exhibit B to its Application in Docket Number 09-15, stated:

From time to time, NSA may have information indicating that a particular identifier was used by an individual associated with [REDACTED] only for a particular timeframe. In these circumstances, NSA would seek and grant as appropriate, RAS approval, with the understanding that contact chaining would be conducted in a manner that covered a limited timeframe that has been identified.

(...continued) which the telephone identifier has been associated with [REDACTED] in order that the analysis and minimization of the information retrieved from their queries may be informed by that fact." September 3 Order at 9, n. 5; October 30 Order at 9, n. 6.

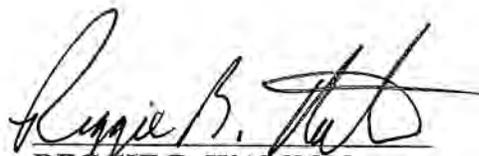
The report then provided one example of how the NSA had conducted such a query. NSA Report to the Foreign Intelligence Surveillance Court (BR 09-13) at 15-16.

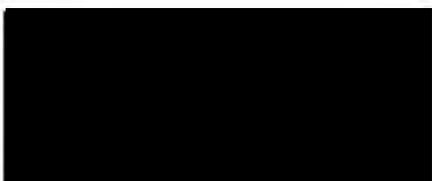
This report was not sufficiently detailed to allay the Court's concerns, and the Court therefore continues to be concerned about the likelihood that these queries could reveal communications of United States person users of the telephone identifier who are not the subject of FBI investigations. As a result, the Court's October 30 Order contains the same reporting requirements as the September 3 Order. October 30 Order at 18-19. However, to assist the government in providing a report that satisfies its needs, the Court HEREBY ORDERS that any report submitted by the government pursuant to paragraph (3)S of the Court's October 30 Order shall include the following information with regard to how the NSA has conducted queries of the BR metadata using telephone identifiers determined to satisfy the reasonable articulable suspicion standard at some time in the past, but that do not currently meet the standard, and how the NSA minimized any information obtained or derived therefrom:

1. The total number of such queries run during the reporting period and what percentage those queries constitute of the total number of queries run.
2. Would the status of a telephone identifier that was approved for querying under these circumstances be changed on the Station Table to non-RAS approved once a single query using that identifier has been run? If not, does the NSA have an automated process to limit queries of that telephone identifier to the specified time frame? If not, how will an NSA analyst know that any query of that telephone identifier must be limited to the time period for which the reasonable articulable suspicion existed?

3. Are NSA analysts permitted to conduct more than one query using any telephone identifier determined to have met the reasonable articulable suspicion standard under circumstances described above, and if so, for what purpose? If query results from the first query indicated that the telephone identifier's association with the foreign power terminated earlier than the date the NSA believed the identifier no longer met the reasonable articulable suspicion, would the timeframe restriction be adjusted for any subsequent query?
4. If this type of query is run, and the NSA analyst who ran the query determines that the query results include records of communications that were made after the telephone identifier was re-assigned to a United States person who is not associated with the foreign power, must the analyst delete or otherwise mask such records prior to sharing the query results with NSA analysts authorized to receive query results pursuant to paragraph (3)I of the Court's order?

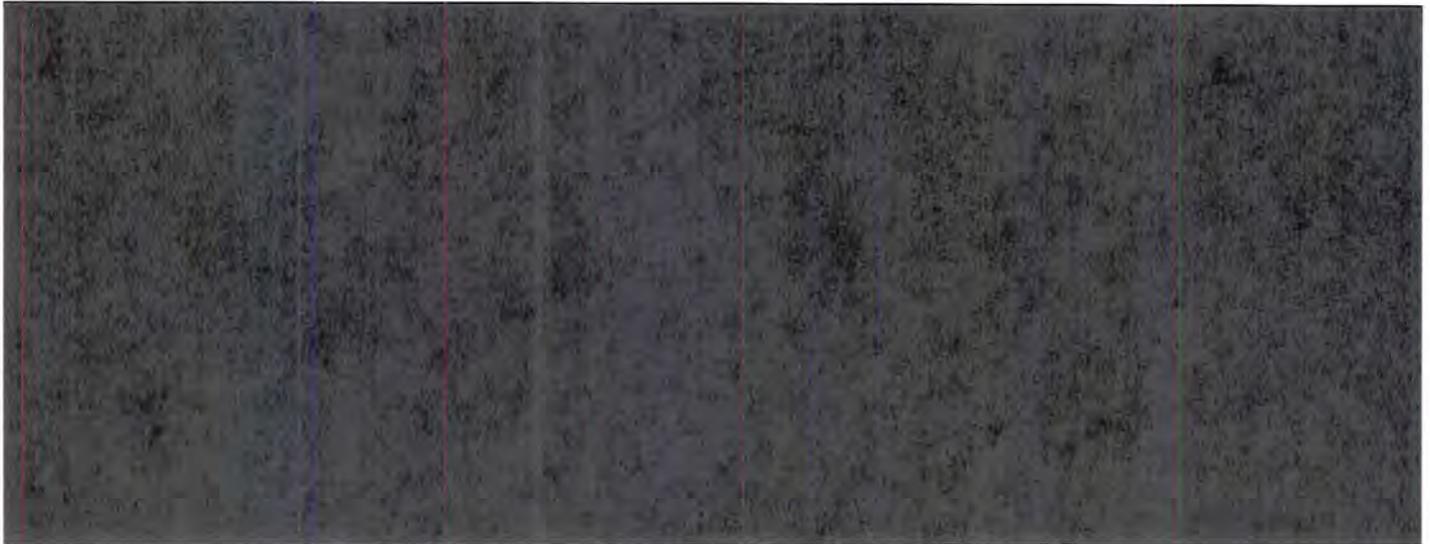
ENTERED this 5th day of November, 2009.


REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court



~~TOP SECRET/COMINT/OC,NF~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.



SUPPLEMENTAL OPINION AND AMENDMENT TO PRIMARY ORDER

On [REDACTED] the Court issued a Primary Order in the above-captioned docket authorizing the National Security Agency (NSA) to install and use pen register/trap and trace (PR/TT) devices to engage in the bulk collection of certain forms of metadata about Internet communications. At that time, the Court also issued a Memorandum Opinion that explained, inter alia, the reasons for approving some parts of the proposed PR/TT collection, but not others. See Docket No. PR/TT [REDACTED] Memorandum Opinion issued on [REDACTED] (“Memorandum Opinion”). The Primary Order stated that “NSA shall, pursuant to this Order, collect only metadata approved for acquisition in Part II” of the Memorandum Opinion. Primary Order at 5.

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

Subsequently, the government requested clarification of certain issues addressed in the Memorandum Opinion. See Letter submitted on [REDACTED] (“[REDACTED] Letter”). The government separately submitted additional information pertaining to one of the issues for which it sought clarification. See Letter submitted on [REDACTED] (“[REDACTED] Letter”). In response to the government’s request, and in view of the importance and complexity of the issues involved, the Court is issuing this Supplemental Opinion and Amendment to Primary Order.¹ For ease of reference, the discussion below employs the government’s enumeration of the issues identified in the [REDACTED] Letter.

Issue No. 1: [REDACTED]



¹ Familiarity with the terminology and reasoning of the Memorandum Opinion is assumed. Matters discussed in the Memorandum Opinion are addressed herein only insofar as they particularly relate to a request for clarification.

² See Memorandum Opinion at 35 n.36 (“For purposes of this Opinion, the term ‘e-mail communications’ refers to e-mail messages sent between e-mail users, [REDACTED]”).

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

After describing what it perceives as a potential ambiguity in the Memorandum Opinion,³ the government requests confirmation of its understanding that NSA is [REDACTED]

[REDACTED]

Letter at 2. As explained below, however, the government's formulation is an overly broad description of the authority granted by the Court.

The Memorandum Opinion largely tracks the government's application in describing [REDACTED] [REDACTED] metadata for which approval was requested. See Memorandum Opinion at 35-41. The Memorandum Opinion limits the collection authority for several of these categories. Although many of the limitations imposed by the Court mirror the government's factual description of how the PR/TT devices would operate,⁴ the government did not, for the most part, incorporate such limitations into the scope of the requested collection authority. Under the expansive interpretation of the relevant statutory provisions put forward by the government, the

³ Specifically, the government observed that its submissions had defined [REDACTED] [REDACTED] See [REDACTED] Letter at 2 (comparing Application, Exhibit D, [REDACTED] Response at 2, 8 with Memorandum Opinion at 62).

⁴ See, e.g., Application, Exhibit D, [REDACTED] Response at 1 [REDACTED]; Application, Exhibit B, Memorandum of Law and Fact in Support of Application for PR/TT Devices for Foreign Intelligence Purposes at 23-24, 43 [REDACTED].

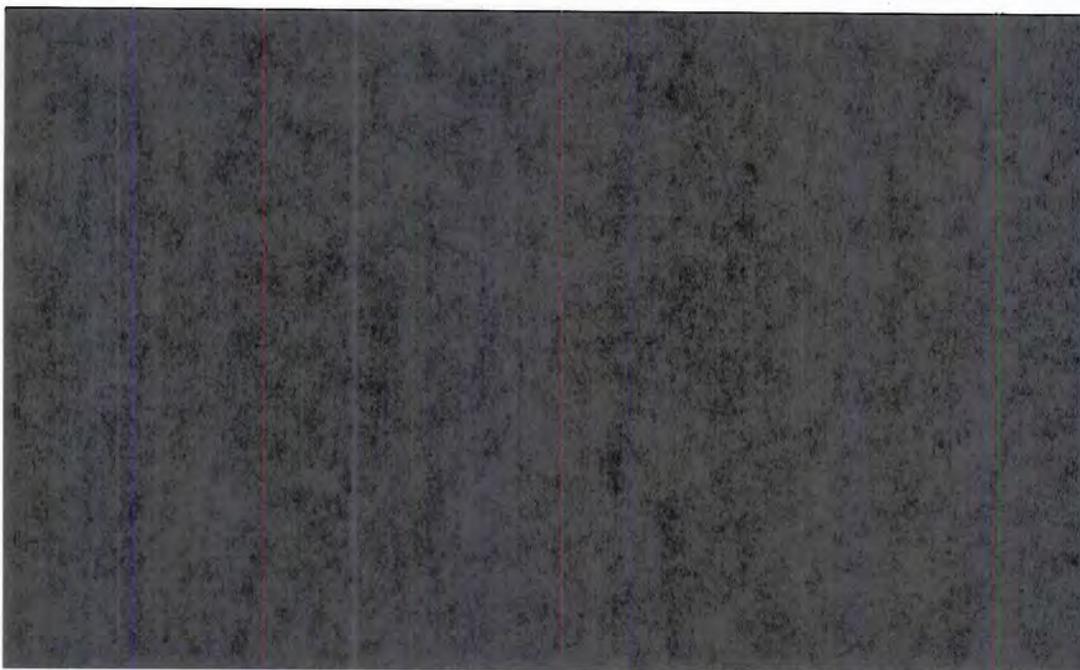
~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

limitations may not have been warranted. But after careful consideration, the Court adopted a less expansive interpretation of the statute, see Memorandum Opinion at 30-35, 51-62, thereby requiring a more careful examination of the circumstances of collection for some types of metadata, and particularly an assessment of 

See, e.g., id. at 37-38, 42-44, 51-62.

The principal limitations adopted by the Memorandum Opinion are:



~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

[REDACTED]

In sum, as the Memorandum Opinion explains,

[REDACTED]

They, therefore, may be collected only in the circumstances approved by the Court in the Memorandum Opinion.

Issue No. 2: [REDACTED]

The government seeks clarification regarding the scope of metadata it may collect from a communication [REDACTED]

See [REDACTED], Letter at 2-3. The Memorandum Opinion states:

[REDACTED]

[REDACTED]

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

[REDACTED]

Memorandum Opinion at 48 (citation omitted). After analyzing the relevant statutory provisions, the Court concluded that

[REDACTED]

Id. at 62-71.

The government understands that, even in circumstances when

[REDACTED]

Letter at 3. This understanding is

correct, subject to a proper understanding of what constitutes “authorized metadata” in the circumstances in question, as discussed above with respect to Issue No. 1.

Issue No. 3:

[REDACTED]

Memorandum Opinion at 37. The Memorandum Opinion describes two general circumstances in

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

which the collection of [REDACTED]

See id. The government now seeks clarification regarding the scope of these circumstances. See [REDACTED] Letter at 3.

The first circumstance is [REDACTED]

[REDACTED] Memorandum Opinion at 37-38. In

such a case, the Court authorized collection of [REDACTED]

[REDACTED] Id. at 38. The government now seeks clarification that collection of [REDACTED]

[REDACTED]

[REDACTED] Letter at 3 (footnote omitted).

[REDACTED] Id. at 3 n.1.⁶

In the above-quoted example, [REDACTED]

⁶ This example is similar to one previously provided by the government to illustrate how [REDACTED]

See Application, Exhibit D, [REDACTED] Response at 2.

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

[REDACTED]

As the Memorandum Opinion stated, [REDACTED]

[REDACTED] Memorandum

Opinion at 55 (emphasis in original). In this example, [REDACTED]

[REDACTED]

The second circumstance discussed in the Memorandum Opinion is [REDACTED]

[REDACTED]

[REDACTED] Memorandum Opinion at 37. The government

understands that, in this circumstance, [REDACTED]

⁷ See Memorandum Opinion at 36-37 [REDACTED]

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

[REDACTED]

[REDACTED] Letter at 3. This understanding is correct. Footnote 37 of the Memorandum

Opinion⁸ is intended to address the opposite case:

[REDACTED]

Issue No. 4: [REDACTED]

The government correctly notes that some [REDACTED] approved for collection [REDACTED]. See [REDACTED] Letter at 4; Memorandum Opinion at 65. When collecting these [REDACTED]

[REDACTED]

The government requests clarification that NSA's collection process may also infer the

[REDACTED]

[REDACTED] See [REDACTED] Letter at 4. For example, [REDACTED]

[REDACTED]

⁸ Footnote 37 states: [REDACTED] Memorandum Opinion at 38 n.37 (citation omitted).

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

See Memorandum Opinion at 42-43. The government requests confirmation that, in such a case,

[REDACTED]

[REDACTED] Letter at 1.

The Court concludes that [REDACTED]

[REDACTED] may be authorized as a form of PR/TT collection under the analysis adopted in the Memorandum Opinion.

[REDACTED]

[REDACTED] Memorandum Opinion at 51-65.

[REDACTED]

Cf. Memorandum Opinion at 59 [REDACTED]

Issue No. 5: [REDACTED]

As described in the Memorandum Opinion, the collection process involves [REDACTED]

[REDACTED]

[REDACTED] Memorandum Opinion at 27-28. During the

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

collection process,

Id. at 27.

The government has now advised that some of this

See

Letter at 4.

Id.

Memorandum

Opinion at 27 (internal quotations omitted).

Under these circumstances, the fact that

poses no legal difficulty. This Court has approved other forms of

PR/TT collection that involve See,

e.g., Docket No. PR/TT, Supplemental Opinion issued on

In this case,

Memorandum Opinion at 29 (emphasis added). Accordingly, the collection process

~~TOP SECRET/COMINT/OC,NF~~

~~TOP SECRET/COMINT/OC,NF~~

described in the Memorandum Opinion and authorized in the Primary Order may, as necessary,



* * *

For the reasons stated above, it is permissible for NSA to collect metadata as described in Part II of the Memorandum Opinion, as supplemented herein. Accordingly, it is hereby ORDERED that the Primary Order issued on [redacted] in the above-captioned docket is amended as follows:

Paragraph 5(A), on page 5 of the Primary Order, is amended to read:

“(5) NSA shall implement the authority granted herein in the following manner:

A. Pursuant to this Order, NSA shall only collect metadata as approved in Part II of the [redacted] Memorandum Opinion, as supplemented by the Supplemental Opinion and

Amendment to Primary Order issued in the above-captioned docket on [redacted]



Entered this [redacted] day of [redacted] in Docket No. PR/TT [redacted]



JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET/COMINT/OC,NF~~

I, [redacted] Deputy Clerk,
FISC, certify that this document
is a true and correct copy of
the original. [redacted]

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE PROCEEDINGS REQUIRED BY § 702(i)
OF THE FISA AMENDMENTS ACT OF 2008

Docket Number: MISC 08-01

ORDER

IT IS HEREBY ORDERED that the Motion of the American Civil Liberties Union for Leave to Participate in Proceedings Required by Section 702(i) of the FISA Amendments Act of 2008 is DENIED, for the reasons set forth in the Memorandum Opinion issued on this date.

Mary A. McLaughlin
MARY A. McLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

August 27, 2008
DATE

Beverly C. Queen Deputy Clerk
FISC, certify that this document
is a true and correct copy of
the original. *BQ*

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE PROCEEDINGS REQUIRED BY § 702(i)
OF THE FISA AMENDMENTS ACT OF 2008

Docket Number: MISC 08-01

MEMORANDUM OPINION¹

This matter comes before the Court on the “Motion for Leave to Participate in Proceedings Required by § 702(i) of the FISA Amendments Act of 2008,” filed by the American Civil Liberties Union (“ACLU”) on July 10, 2008 (“ACLU motion”). In accordance with a scheduling order issued on July 17, 2008, the Government filed its “Opposition to the American Civil Liberties Union’s Motion for Leave to Participate in Proceedings Required by § 702(i) of the FISA Amendments Act of 2008” on July 29, 2008. The ACLU filed a “Reply Memorandum in Support of Motion for Leave to Participate in Proceedings Required by § 702(i) of the FISA Amendments Act of 2008” on August 5, 2008. For the reasons described below, the Court denies the ACLU’s motion.

BACKGROUND

Section 702 of the Foreign Intelligence Surveillance Act

In its motion, the ACLU seeks information about, and the opportunity to participate in, judicial proceedings required under Section 702(i) of the Foreign Intelligence Surveillance Act (“FISA”), as most recently amended by the FISA Amendments Act of 2008 (“FAA”), Pub L.

¹ The Government’s filing in this case was unclassified; this opinion does not go beyond the factual assertions that were contained in the Government’s filing.

No. 110-261, 122 Stat. 2436. Section 702 of FISA (codified at 50 U.S.C. § 1881a) specifies circumstances under which the Government can authorize the targeting of non-United States persons reasonably believed to be outside the United States, to acquire foreign intelligence information. The FAA imposes several limitations upon and requirements for the exercise of this authority.

Among other requirements, the FAA provides that “[t]he Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to – (A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and (B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” 50 U.S.C. § 1881a(d)(1).

The FAA further provides that the Attorney General, again in consultation with the Director of National Intelligence, “shall adopt minimization procedures that meet the definition of minimization procedures under section 1801(h) or 1821(4) . . . as appropriate, for acquisitions authorized under subsection (a).” *Id.* § 1881a(e)(1).

Finally, the Attorney General and the Director of National Intelligence are required to submit to the Foreign Intelligence Surveillance Court (“FISC”) a written certification. Among other things, this certification must attest (1) that there are procedures in place that are reasonably designed to ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication as to which the sender and all intended recipients

are known at the time of the acquisition to be located in the United States; (2) that the minimization procedures to be used with respect to such an acquisition meet the definition of minimization procedures under section 1801(h) or 1821(4) of FISA, as appropriate; and (3) that both the targeting and the minimization procedures either have been approved, have been submitted for approval, or will be submitted with the certification for approval by the FISC. Id. § 1881a(g)(2)(A)(i)-(ii).

Judicial Review under Section 702(i)

The FAA provides that the FISC shall have jurisdiction to review the certification, the targeting procedures and the minimization procedures. Id. § 1881a(i)(1)(A). As the ACLU notes in its motion, however, the Court's role here is "narrowly circumscribed." ACLU Mot. at 5. With respect to the certification, the FISC is merely to "determine whether the certification contains all the required elements." Id. § 1881a(i)(2)(A). The Court is to review the targeting procedures to "assess whether the procedures are reasonably designed to – (i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and (ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." Id. § 1881a(i)(2)(B). As for the minimization procedures, the Court must "assess whether such procedures meet the definition of minimization procedures under section 1801(h) or section 1821(4) of this title, as appropriate." Id. § 1881a(i)(2)(C).

The FAA further provides that the FISC shall enter an order approving the certification and the use, or continued use, of the targeting and minimization procedures if the Court finds that

the certification contains all the required elements, and that the targeting and minimization procedures are consistent with the requirements of Sections 1881a(d)(1) and 1881a(e)(1) and "with the Fourth Amendment to the Constitution of the United States." Id. § 1881a(i)(3)(A). Should the Court conclude that it cannot make these findings, the Court shall either order the Government to correct any deficiency identified by the Court or cease or not begin implementation of the authorization for which the certification was submitted. Id. § 1881a(i)(3)(B).

The ACLU's Motion

In its motion, the ACLU requests:

- (1) that it be notified of the caption and briefing schedule for any proceedings under Section 702(i) in which this Court will consider legal questions relating to the scope, meaning and constitutionality of the FAA;
- (2) that, in connection with such proceedings, the Court require the Government to file public versions of its legal briefs, with only those redactions necessary to protect information that is properly classified;
- (3) that, in connection with such proceedings, the ACLU be granted leave to file a legal brief addressing the constitutionality of the FAA and to participate in oral argument before the Court; and
- (4) that any legal opinions issued by the Court at the conclusion of such proceedings be made available to the public, with only those redactions necessary to protect information that is properly classified.

ACLU Mot. at 2. The relief sought by the ACLU can be viewed as falling into two categories, which to a certain degree overlap: (1) a request for the release of records (i.e., any legal briefs filed by the Government and legal opinions issued by the Court in connection to § 702(i) proceedings) similar to that which was considered by this court last year in In re Motion for Release of Court Records, 526 F. Supp. 2d 484 (Foreign Intel. Surv. Ct. 2007); and (2) a more general request to participate in the Court's review under § 702(i) (i.e., to be granted leave to file a legal brief and to participate in oral argument). The ACLU's request to be notified of the

caption and briefing schedule of particular proceedings under § 702(i) is a bit of a hybrid; it is in effect a request for release of records, made in order to facilitate the ACLU's participation in the matter.

1. The ACLU's Request for the Release of Records

The ACLU's request is similar to a request it made on August 9, 2007. At that time, the ACLU filed a motion with the FISC seeking the release of what it identified as court orders and Government pleadings regarding a surveillance program conducted by the National Security Agency. The court denied the motion, finding (1) that the common law provided no public right of access to the requested records; and (2) that the First Amendment provided no public right of access to the requested records. In re Motion for Release of Court Records, 526 F. Supp. 2d at 490-497. The court further declined to exercise any "residual discretion," should it exist, to release any portions of the records at issue, Id. at 497.

Although the records sought by the ACLU in the present motion are different from those it requested in 2007, this Court finds no reason to reach a different conclusion. These records also are to be maintained under the comprehensive statutory scheme described by Judge Bates in In re Motion for Release of Court Records as "designed to protect FISC records from routine public disclosure" and found to supercede any common law right of access. Id. at 491.

Nor is there a First Amendment right of access to the records. Application of the "experience and logic" tests adopted by the Supreme Court for assessing the existence of a qualified First Amendment right of access in Press-Enterprise Co. v. Superior Court, 478 U.S. 1

(1986) (Press-Enterprise II) confirms that there is no such right of access to these documents.² First, the “experience” test is not satisfied because neither the “place” nor the “process” has “historically been open to the press and general public.” Id. at 8. The FISC has no tradition of openness, either with respect to its proceedings, its orders, or to Government briefings filed with the FISC. See In re Motion for Release of Court Records, 526 F. Supp. 2d at 492. Moreover, the specific process at issue here, proceedings under Section 702(i) of the FAA, is brand-new, and therefore cannot be said to have such a tradition.

Under Press-Enterprise II, the failure to satisfy the “experience” test alone defeats a claim for a First Amendment right of access. 478 U.S. at 9. See also In Re Motion for Release of Court Records, 526 F. Supp. 2d at 493. But should the “logic” test even apply in this case, it is not satisfied because public access to these documents will not play a significant positive role in the functioning of the FISA process. The Government asserts that its certification, targeting procedures, and minimization procedures will provide the details of its sources and methods for collecting foreign intelligence information under the FAA and therefore will be classified. Gov’t. Opp’n at 8. The ACLU responds that it is not seeking access to “properly classified information,” ACLU Reply at 1, but contends that the Court should determine whether the Government’s procedures are “properly” classified. Id. at 7.

² “First, because a tradition of accessibility implies the favorable judgment of experiences, we have considered whether the place and process have historically been open to the press and general public.” Press-Enterprise II, 478 U.S. at 8 (citations and internal quotation marks omitted). “Second, in this setting the Court has traditionally considered whether public access plays a significant positive role in the functioning of the particular process in question.” Id. “If the particular proceeding in question passes these tests of experience and logic, a qualified First Amendment right of public access attaches.” Id. at 9.

Assuming, arguendo, that the Court does have the authority to undertake this type of inquiry, the "logic" test would still not be satisfied. Absent the Government's wholesale abuse of classification authority, which there is no reason to presume here, any disclosure resulting from such a review can be expected to be limited and incremental in nature. The fact that at most, only partial access to the documents could be provided undercuts the ACLU's ability to satisfy the "logic" test. As with the records at issue in In re Motion for Release of Court Records, "[t]he benefits from a partial release of declassified portions of the requested materials would be diminished, insofar as release with redactions may confuse or obscure, rather than illuminate, the decisions in question." 526 F. Supp. 2d at 495. Moreover, such a review could result in the release of information that should have remained classified.

Although it is possible to identify some benefits which might flow from public access to Government briefs and FISC orders related to Section 702(i) proceedings, the "logic" test is not satisfied because any such benefits would be outweighed by the risks to national security created by the potential exposure of the Government's targeting and minimization procedures. In short, the proceedings in Section 702(i) seem to be of the type "that would be totally frustrated if conducted openly." Press-Enterprise II, 478 U.S. at 8-9.

In the alternative, the ACLU contends that the Court should exercise its discretion to grant the relief it requests because the FAA has "sweeping implications for the rights of U.S. citizens and residents," ACLU Reply at 7, and the Section 702(i) proceedings "should be adversarial and as informed and transparent as possible." ACLU Mot. at 9. Assuming that such discretion resides with the Court, it declines to exercise that authority here. Providing the ACLU with access to the materials provided to the FISC in connection with the Section 702(i) review, and with the Court's assessment of the Government submissions, would create risks to national

security that far outweigh any potential benefit to be gained by providing the ACLU with access to the requested records.³

2. The ACLU's Request to Participate in Section 702(i) Proceedings before the FISC

The ACLU also seeks leave, in connection with proceedings under Section 702(i), to file a legal brief addressing the constitutionality of the FAA, and to participate in oral argument before the Court. The Court denies this request as well. First, the ACLU has no right to such participation. The FAA does not provide for such participation by a party other than the Government. Second, assuming that the Court has the discretion to allow such participation, it declines to do so. For the reasons described below, the ACLU's participation is unlikely to provide meaningful assistance to the Court.

First, the FAA itself does not provide for participation by a party other than the Government in the Court's review of the Government's certification and procedures. In fact, it provides that only the Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of the Court's order resulting from its review of the certification and procedures. 50 U.S.C. § 1881a(i)(4)(A). By contrast, Section 702(h) explicitly provides for the participation of parties other than the Government, in that electronic communication service providers can bring a challenge in the FISC to directives issued to them under the FAA. Id.

³ Even in a context where a criminal defendant's Sixth Amendment rights are at issue, FISA provides that materials may be disclosed to the aggrieved person "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f) (emphasis added). As Section 702(i) does not include a similar mechanism for disclosing materials when deemed necessary to the Court's review, the Court will decline to disclose such materials in this case, when it believes that disclosure is not only unnecessary to the Court's determination but also unlikely to be useful, for the reasons discussed below.

§ 1881a(h)(4). The FAA also expressly gives these providers a right to appeal. Id.
§ 1881a(h)(6).

In addition, even before the enactment of the FAA, Congress provided for the participation of parties other than the Government in the limited context of providing a right of challenge in the FISC to those receiving orders for the production of tangible things pursuant to 50 U.S.C. § 1861. Id. § 1861(f)(2). The lack of analogous provisions for proceedings under Section 702(i) strongly suggests that Congress did not contemplate the Court's review of the certification and procedures to be anything other than an ex parte proceeding.

Second, as described above, the Court's review under Section 702(i) is limited to three specific components: the certification, the targeting procedures and the minimization procedures. The Court's review of the certification is limited to determining whether the certification contains all of the elements required by the statute. As to the targeting procedures adopted by the Government, the Court must review the procedures to "assess whether the procedures are reasonably designed to – (i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and (ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(i)(2)(B). As to the minimization procedures, the Court must "assess whether such procedures meet the definition of minimization procedures under section 1801(h) or section 1821(4) of this title, as appropriate." Id. § 1881a(i)(2)(C). Finally, the Court must decide whether the targeting and minimization procedures are consistent with the Fourth Amendment. Id. § 1881a(i)(3)(A).

As described above, the Government states that its targeting and minimization procedures will be classified because they provide the details of its sources and methods for collecting foreign intelligence information. The ACLU, therefore, will not have access to either set of procedures. Without such access, it cannot provide meaningful input to the Court on the compliance of those procedures with the FAA or the Fourth Amendment.

The ACLU suggests that judicial review under Section 702(i) will necessarily include review of the constitutionality of the FAA, and the ACLU's input would be helpful in such a constitutional analysis. Such a generalized constitutional review, however, is not contemplated under Section 702(i). The Court is required to consider whether the targeting and minimization procedures adopted by the Government meet the requirements of the statute and whether those procedures are consistent with the Fourth Amendment. The Court is not required, in the course of this Section 702(i) review, to reach beyond the Government's procedures and conduct a facial review of the constitutionality of the statute. Accordingly, the ACLU's participation in Section 702(i) proceedings will not assist the Court.

CONCLUSION

For all the reasons set forth above, the motion of the ACLU for leave to participate in proceedings required by § 702(i) of the FISA Amendments Act of 2008 is denied. A separate order has been issued.

Mary A. McLaughlin
 MARY A. McLAUGHLIN
 Judge, United States Foreign
 Intelligence Surveillance Court

August 27, 2008
 DATE

Dorothy C. Queen Deputy Clerk
 FISC, certify that this document
 is a true and correct copy of
 the original. *39*

~~SECRET//NOFORN~~

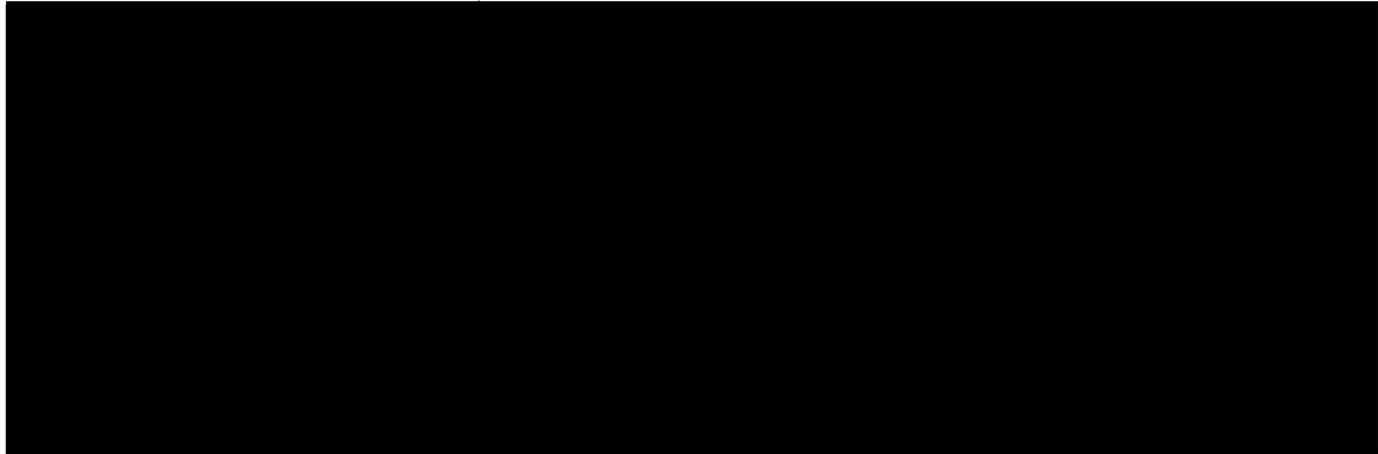
2014

UNITED STATES

U.S. Foreign Intelligence
Surveillance Court

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.



OPINION ON MOTION FOR DISCLOSURE OF PRIOR DECISIONS

On [REDACTED] 2014, [REDACTED]

“Motion for Disclosure of Prior Decisions” (“Motion for Disclosure”). The Court denied this Motion on the record at the adversary hearing held on the underlying matter on [REDACTED] 2014. It writes this Opinion to explain its reasoning.

I. BACKGROUND

This case came before the Court on the Government’s “Petition for an Order to Compel Compliance with Directives of the Director of National Intelligence and Attorney General,” submitted on [REDACTED] 2014 (“Petition”). The directives that the Government is seeking to

~~SECRET//NOFORN~~

enforce were issued pursuant to Section 702(h)(1) of the Foreign Intelligence Surveillance Act, as amended (FISA)¹ and served on [REDACTED]

Pursuant to a schedule set by order of the Court on [REDACTED] 2014, [REDACTED]

[REDACTED] (“Response”) on [REDACTED] 2014, [REDACTED]

[REDACTED] (collectively

“Reply”) on [REDACTED] 2014.² In its Reply, the Government repeatedly cited and quoted two

opinions of the FISC that do not appear to have been made public in any form: one issued on

September 4, 2008, [REDACTED] and the other issued on August 26, 2014, [REDACTED]

[REDACTED] (hereinafter “the Requested Opinions”).

Both of the Requested Opinions resulted from the FISC’s ex parte review of certifications and attendant targeting and minimization procedures pursuant to Section 702(i). The August 26,

2014 opinion approved the certifications and procedures now in effect, and the directives [REDACTED]

[REDACTED] pursuant to those certifications. The

September 4, 2008 opinion approved [REDACTED] certifications and procedures.

¹ FISA is codified at 50 U.S.C. §§ 1801-1885c, within which Section 702 appears at § 1881a.

² [REDACTED]

[REDACTED] Motion for Disclosure, in which it sought “immediate access to [the Requested Opinions] (in appropriately redacted form) to adequately prepare for the hearing scheduled for [REDACTED] [REDACTED]” Motion for Disclosure at 1.³ Pursuant to the Court’s scheduling order of [REDACTED] 2014, the Government submitted its opposition to the Motion for Disclosure (“Opposition”) on [REDACTED] 2014.

II. DISCUSSION

As explained below, the Court concluded that neither FISA nor the Foreign Intelligence Surveillance Court (FISC) Rules of Procedure (“FISC Rules”) require, or provide for discretionary, disclosure of the Requested Opinions in the circumstances of this case. Similarly, the Due Process Clause of the Fifth Amendment does not compel the requested disclosure and, assuming that the Court has some discretion on this matter, no prudential considerations counsel otherwise.

A. FISA and the FISC Rules

The cases handled by the FISC involve classified intelligence gathering operations. From a security perspective, FISC operations “are governed by FISA, by Court rule,^[4] and by statutorily mandated security procedures issued by the Chief Justice of the United States.

[REDACTED] its counsel has a Top Secret security clearance [REDACTED] seeking access to the Requested Opinions with any redactions necessary to downgrade the Requested Opinions to a Top Secret, non-compartmented level.

⁴ The FISC explicitly has the authority to establish rules for its proceedings under 50 U.S.C. § 1803(g)(1).

Together, they represent a comprehensive scheme for the safeguarding and handling of FISC proceedings and records.” In re Motion for Release of Court Records, 526 F. Supp.2d 484, 488 (FISA Ct. 2007).

Specifically applicable to this case is the requirement that, in any proceeding under Section 702, “the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.” 50 U.S.C. § 1881a(k)(2). The FISC Rules reiterate this statutory requirement and further provide: “Except as otherwise ordered, if the government files ex parte a submission that contains classified information, the government must file and serve on the non-governmental party an unclassified or redacted version. The unclassified or redacted version, at a minimum, must clearly articulate the government’s legal arguments.” FISC Rule 7(j).

FISC Rule 3 provides: “In all matters, the Court and its staff shall comply with . . . Executive Order 13526, ‘Classified National Security Information’ (or its successor).” Under that executive order, a person may be given access to classified information only if

- (1) a favorable determination of eligibility for access has been made by an agency head or the agency head’s designee;
- (2) the person has signed an approved nondisclosure agreement; and
- (3) the person has a need-to-know the information.

Executive Order 13526 § 4.1(a). “Need-to-know” is defined as “a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective

recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.” Id. § 6.1(dd) (emphasis added).

B. Analysis

The Court has reviewed the redacted copies of the Government’s Reply (to include the supporting affidavit) and finds that it clearly articulates the Government’s legal arguments.

[REDACTED] without the Requested Decisions, it “cannot adequately understand the guidance, and limitations thereof, that this Court has previously issued.” Motion for Disclosure at 1. The Government responds that the Requested Opinions do not bear on the application of its targeting and minimization procedures [REDACTED]

[REDACTED] further contends that its counsel “has a ‘need to know’ with regard to the prior relevant caselaw.” Motion for Disclosure at 1.

The government retorts [REDACTED] does not have a need-to-know more about the contents of the Requested Decisions. Opposition at 3.

The Court has carefully reviewed the Requested Opinions in the context of the issues presented by the Petition⁵ and the parties’ respective arguments on those issues and compared the citations to and quotations from the Requested Opinions that appear in the Government’s Reply to the underlying texts. In no instance does the Reply quote or reference the Requested Opinions

⁵ [REDACTED] “to comply with [each] directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of [Section 702] and is otherwise lawful.” 50 U.S.C. § 1881a(h)(5)(C).

in a manner that is incomplete, wrenched from necessary context or otherwise misleading with regard to the point being addressed. Based on that review, the Court finds that the Requested Opinions would be of little, if any, assistance to [REDACTED] arguments it makes on the merits.⁶

Given that FISC Rule 3 requires the Court to follow the Executive Order, the Court will not lightly second-guess the Government's need-to-know determination, which the Executive Order specifically commits to the Executive Branch. Moreover, there is no indication that the Government is exploiting the need-to-know requirement to mislead or otherwise gain a strategic advantage [REDACTED]

[REDACTED] For these reasons, the Court concludes [REDACTED] does not have the requisite need-to-know the requested information.

Other aspects of the Section 702 framework support [REDACTED] [REDACTED] not entitled to access to the Requested Opinions. The statute and the FISC Rules provide detailed guidance for the conduct of proceedings initiated by a petition to compel compliance with, or to modify or set aside, a Section 702 directive, see 50 U.S.C. § 1881a(h); FISC Rules 20-31, but they provide no mechanism for the recipient of a directive to seek discovery or disclosure of classified information. They do provide for nondisclosure in the

⁶ The Court finds that this would especially be the case once compartmented information was redacted from the Requested Opinions.

context of the FISC's ex parte review of certifications and accompanying procedures. See 50 U.S.C. § 1881a(g)(1)(A); FISC Rule 30.⁷ In the context of a petition to compel compliance with (or to modify or set aside) a directive, in fact, FISA and Rule 7(j) provide just the opposite, i.e., they permit the Government to withhold classified information from the recipient of the directive. See 50 U.S.C. § 1881a(k)(2); FISC Rule 7(j).⁸

Finally, the statute provides a 30-day period for the completion of FISC review of the Petition in this case. See § 1881a(h)(5)(C). That 30-day period ends on [REDACTED] 2014, a deadline that is incompatible, as a practical matter, with the Government's making redactions of the Requested Opinions for disclosure [REDACTED] and

⁷ For the most part, the Requested Opinions pertain to classified material that the Government submitted under seal, as required by 50 U.S.C. § 1881a(g)(1)(A), for ex parte and in camera review under § 1881a(i). In a prior case, the FISC observed that "the Congressional judgment embodied" in a comparable statutory provision for ex parte review of procedures suggested that the FISC "should not lightly override the government's opposition to the release of" a classified FISC opinion containing classified information that "directly relates to what the government [previously] submitted for ex parte and in camera review." [REDACTED] Order issued on [REDACTED] 2008, at 2 n.2. The same logic is applicable here.

⁸ Moreover, the detailed statutory provisions regarding FISC proceedings under Section 702 do not provide for [REDACTED] disclosure of opinions arising from the Court's ex parte review of Section 702 certifications and procedures. Section 702 makes clear that, in the ordinary course, the FISC will have reviewed and approved a certification and accompanying procedures prior to the issuance of a directive pursuant to that certification. See 50 U.S.C. § 1881a(a), (g)(1)(A), (h)(1), (i)(3). If Congress had thought access to such prior FISC opinions were necessary for the recipient of a directive to challenge its lawfulness, it could have provided for such access.

consideration of whatever additional argument such counsel would make after reviewing the Requested Opinions.⁹

C. Due Process

In its Motion for Disclosure [REDACTED]

presents no argument and cites no authority for its suggestion that due process requires the requested disclosure. Motion for Disclosure at 1-2. The weight of authority indicates otherwise. For example, with respect to challenges to the lawfulness of electronic surveillance brought by an aggrieved person,¹⁰ the district court is required to review the application, order, and other materials relating to the electronic surveillance in camera and ex parte if “the Attorney General files an affidavit under oath that disclosure . . . would harm the national security.” 50 U.S.C. § 1806(f). Such materials bear directly on any claim that a surveillance was unlawful; nevertheless, disclosure may only occur – even a partial disclosure “under appropriate security procedures and protective orders” – “where such disclosure is necessary to make an accurate

⁹ The Court may extend that 30-day period “as necessary for good cause and in a manner consistent with national security,” § 1881a(j)(2), but [REDACTED] not shown good cause to delay the proceeding to accommodate the requested disclosure. Moreover, [REDACTED]

[REDACTED] it is doubtful that delaying resolution of the lawfulness of the Directives would be consistent with national security.

¹⁰ “Aggrieved person” is defined as “a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” 50 U.S.C. § 1801(k).

determination of the legality of the surveillance,” when the court has found that the surveillance was unlawful or “to the extent that due process requires discovery or disclosure.” § 1806(f), (g). Courts have found non-disclosure of surveillance materials under these provisions to comport with due process, see, e.g., United States v. El-Mezain, 664 F.3d 467, 567-68 (5th Cir. 2011); United States v. Abu-Jihaad, 630 F.3d 102, 129 (2d Cir. 2010); United States v. Damrah, 412 F.3d 618, 623-24 (6th Cir. 2005), even when the attorneys seeking access have security clearances. See United States v. Ott, 827 F.2d 473, 476-77 (9th Cir. 1987). [REDACTED] presented no reason to reach a different conclusion here.

Beyond what is compelled by the Due Process Clause, the Court is satisfied that withholding the Requested Opinions does not violate common-sense fairness. As stated above, each quotation or reference to the Requested Opinions in the Government’s Reply fairly represents what those opinions say on the discrete point addressed. And the Government properly adduced each of those points in reply to [REDACTED] Response. In these circumstances, the Court would decline to compel disclosure of the Requested Opinions as a matter of discretion, assuming for the sake of argument that indeed the Court would have discretion to compel disclosure in a proper case.

//
//
//
//

* * *

[REDACTED] Motion for Disclosure was DENIED.¹¹
ISSUED this [REDACTED] 2014, [REDACTED]


ROSEMARY M. COLLYER
Judge, United States Foreign
Intelligence Surveillance Court

¹¹ Because the Court finds no basis to conclude that the Government is improperly withholding the Requested Decisions, [REDACTED] “to ask the government to show cause why these decisions should not be provided” and to “strike any portions of pleadings that refer to materials that have not been provided [REDACTED] in appropriately redacted form,” see Motion for Disclosure at 1 n.2, is also denied.

Production of Tangible Things" ("Application" or "the instant Application"), which was submitted to the Court on June 19, 2014, by the Federal Bureau of Investigation ("FBI"). The Application requested the issuance of orders pursuant to 50 U.S.C. §1861, as amended (also known as Section 215 of the USA PATRIOT Act), requiring the ongoing daily production to the National Security Agency ("NSA") of certain telephone call detail records in bulk ("bulk telephony metadata").

On August 29, 2013, Judge Claire V. Eagan of this Court issued an Amended Memorandum Opinion in Docket Number BR 13-109, offering sound reasons for authorizing an application for orders requiring the production of bulk telephony metadata ("August 29 Opinion"). On September 17, 2013, following a declassification review by the Executive Branch, the Court published its redacted August 29 Opinion and the Primary Order issued in Docket Number BR 13-109. On October 11, 2013, Judge Mary A. McLaughlin of this Court granted the FBI's application to renew the authorities approved in Docket Number BR 13-109, issued a Memorandum adopting Judge Eagan's statutory and constitutional analyses, and provided additional analysis on whether the production of bulk telephony metadata violates the Fourth Amendment ("October 11 Opinion"). Both judges of this Court held that the compelled production of such records does not constitute a search under the Fourth Amendment. Judge

McLaughlin further found that the Supreme Court's decision in United v. Jones, __ U.S. __, 132 S. Ct. 945 (2012) neither mandates nor supports a different conclusion.

Following a declassification review by the Executive Branch, the Court published the October 11 Opinion and the Primary Order issued in Docket Number BR 13-158 in redacted form a week later on October 18, 2013. Since the date of Judge McLaughlin's re-authorization of the bulk telephony metadata collection in Docket Number BR 13-158, the government has sought on three occasions renewed authority for this collection. The Court has approved those applications in Docket Numbers BR 14-01 (on January 3, 2014), BR 14-67 (on March 28, 2014), and the instant Application.

In approving the instant Application, I fully agree with and adopt the constitutional and statutory analyses contained in the August 29 Opinion and the October 11 Memorandum. In particular, with respect to the constitutional analysis, I concur with Judges Eagan and McLaughlin that under the controlling precedent of *Smith v. Maryland*, 442 U.S. 735 (1979), the production of call detail records in this matter does not constitute a search under the Fourth Amendment. With respect to the statutory requirements for the issuance of orders for the collection of bulk telephony metadata, I adopt the analysis put forth by Judge Eagan in her August 29 Opinion, and in particular, I note her discussion on the issue of relevance:

~~TOP SECRET//SI//NOFORN~~

The government must demonstrate "facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." 50 U.S.C. 1861(b)(2)(A). The fact that international terrorist operatives are using telephone communications, and that it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, is sufficient to meet the low statutory hurdle set out in Section 215 to obtain a production of records. Furthermore, it is important to remember that the relevance finding is only one part of a whole protective statutory scheme. Within the whole of this particular statutory scheme, the low relevance standard is counter-balanced by significant post-production minimization procedures that must accompany such an authorization and an available mechanism for an adversarial challenge in this Court by the record holder. [. . .] Without the minimization procedures set out in detail in this Court's Primary Order, for example, no Orders for production would issue from this Court. See Primary Ord. at 4-17. Taken together, the Section 215 provisions are designed to permit the government wide latitude to seek the information it needs to meet its national security responsibilities, but only in combination with specific procedures for the protection of U.S. person information that are tailored to the production and with an opportunity for the authorization to be challenged. The Application before this Court fits comfortably within this statutory framework.

August 29 Opinion at 22-23.

Since the issuance of the August 29 Opinion and October 11 Memorandum, there have been changes to the minimization procedures applied to the bulk telephony metadata collection. These were requested by the government and approved by this Court. Moreover, the legality of the bulk telephony metadata collection has been challenged in litigation throughout the country and considered by four U.S. District

~~TOP SECRET//SI//NOFORN~~

Court judges. Lastly, on December 18, 2013, in an order entered in BR 13-158, Judge McLaughlin granted leave to the Center for National Security Studies ("the Center") to file an *amicus curiae* brief on why 50 U.S.C. §1861 does not authorize the collection of telephony metadata records in bulk. The Center filed its *amicus* brief on April 3, 2014, after the most recent authorization of this collection in Docket Number BR 14-67. Prior to making a decision to grant the instant Application, I considered each of these developments, which I briefly note below.

Changes to Minimization Procedures

Pursuant to 50 U.S.C. §1861(g), the bulk telephony metadata collected pursuant to orders granting the instant Application, as well as all predecessor applications, are subject to minimization procedures. The statutory requirements for minimization procedures under 50 U.S.C. §1861(g) are discussed in the August 29 Opinion. August 29 Opinion at 11. On February 5, 2014, the Court granted the government's Motion for Amendment to Primary Order in Docket Number BR 14-01, which amended the minimization procedures required by the Primary Order in that case in two significant respects. First, the amended procedures preclude the government (except in emergency circumstances) from querying the bulk telephony metadata without first having

obtained, by motion, a determination from this Court that reasonable, articulable suspicion (RAS) exists to believe that the selection term (e.g., a telephone number) to be used for querying is associated with an international terrorist organization named in the Primary Order requiring the production of the bulk telephony metadata.¹ Second, the amended procedures require that queries of the bulk telephony metadata be limited so as to identify only that metadata found within two "hops" of an approved selection term.² The government has requested, and the Court has approved, the same limitations in orders accompanying the two subsequent applications for this collection filed with this Court (i.e., Docket Number BR 14-67 and the instant Application).

On February 25, 2014, the government filed a Motion for Second Amendment to Primary Order in Docket Number BR 14-01, through which it sought further to modify the minimization procedures ("February 25 Motion"). Specifically, the government sought relief from the requirement that it destroy bulk telephony metadata after five

¹ Previously, the minimization procedures allowed for this RAS determination to be made by one of a limited set of high-ranking NSA personnel.

² The first "hop" would include metadata associated with the set of numbers directly in contact with the approved selection term, and the second "hop" would include metadata associated with the set of numbers directly in contact with the first "hop" numbers. Previously, the minimization procedures allowed the government to query the bulk telephony metadata to identify metadata within three "hops" of an approved selection term.

years, based on the government's common law preservation obligations in pending civil litigation. In seeking relief from the five-year destruction requirement, the government proposed a number of additional restrictions on access to and use of the data, all designed to ensure that collected metadata that was more than five years old could only be used for the relevant civil litigation purposes. Although this Court initially denied the February 25 Motion without prejudice, the Court granted a second motion for the same relief on March 12, 2014 ("March 12 Order and Opinion"), that the government sought in order to comply with a preservation order that had been issued by the U.S. District Court for the Northern District of California after this Court's denial of the February 25 Motion. The March 12 Order and Opinion required that the bulk telephony metadata otherwise required to be destroyed under the five year limitation on retention be preserved and/or stored "[p]ending resolution of the preservation issues raised . . . before the United States District Court for the Northern District of California[.]" March 12 Opinion and Order at 6. The March 12 Order and Opinion prohibited NSA intelligence analysts from accessing or using such data for any purpose; permitted NSA personnel to access the data only for the purpose of ensuring continued compliance with the government's preservation obligations; and prohibited any further accesses of BR metadata for civil litigation purposes without prior written notice to this Court. *Id.*

~~TOP SECRET//SI//NOFORN~~

at 6-7. Finally, the March 12 Opinion and Order required the government promptly to notify this Court of any additional material developments in civil litigation pertaining to the BR metadata, including the resolution of the preservation issues in the proceedings in the Northern District of California. *Id.* at 7. The preservation issues raised in the Northern District of California have not yet been resolved. As a result, the government has requested and the Court has approved the same exemption from the five year limitation on retention, subject to the same restrictions on access and use, in Docket Number BR 14-67 and the instant Application.

Prior to deciding whether to re-authorize the bulk telephony metadata collection through the appended Primary Order, I considered with care the stated changes to the minimization procedures. As described, the first set of changes approved in the February 5 Order provide enhanced protections for the bulk telephony metadata. While the March 12 Opinion and Order allows the government to retain bulk telephony metadata beyond five years, it allows the government to do so for the sole purpose of meeting preservation obligations in civil litigation pending against it.

~~TOP SECRET//SI//NOFORN~~

U.S. District Court Cases

In recent months, the legality of the bulk telephony metadata collection has been challenged on both statutory and constitutional grounds in proceedings throughout the country, and four U.S. District Court judges have issued opinions on these challenges.

Smith v. Obama, No. 2:13-CV-257-BLW, 2014 WL 2506421 (D. Idaho June 3, 2014);

A.C.L.U. v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); *Klayman v. Obama*, 957 F. Supp.

2d 1 (D.D.C. 2013); and *U.S. v. Moalin*, No. 10cr4246 JM, 2013 WL 6079518 (S.D. Cal.

November 18, 2013). In three of the four cases in which judges have issued opinions

(i.e., all but the *Klayman* case), they have rejected plaintiffs' challenges to this collection.

In particular, with respect to Fourth Amendment challenges raised by plaintiffs, the

judges in *Smith*, *Clapper* and *Moalin* recognized that the Supreme Court's decision in

Smith v. Maryland is controlling and does not support a finding that the bulk telephony

metadata collection is a violation of the Fourth Amendment.

In *Klayman*, Judge Richard J. Leon of the U.S. District Court for the District of

Columbia alone held that the plaintiffs were likely to succeed on their claim that the

bulk telephony metadata collection was an unreasonable search under the Fourth

Amendment. *Klayman*, 957 F. Supp. 2d at 41. Judge Leon ordered the government to

cease collection of any telephony metadata associated with [the plaintiffs'] personal Verizon accounts" and destroy any such metadata in its possession, but he stayed the order pending appeal. *Id.* at 43.

On January 22, 2014, a recipient of a production order in Docket Number BR 14-01 filed a Petition ("January 22 Petition") pursuant to 50 U.S.C. § 1861(f)(2)(A) and Rule 33 of the Foreign Intelligence Surveillance Court ("FISC") Rules of Procedure, asking this Court "to vacate, modify, or reaffirm" the production order issued to it.³ According to the Petitioner, the Petition arose "entirely from the effect on [the recipient] of Judge Leon's Memorandum [Opinion]," and specifically, that Judge's conclusion that the Supreme Court's decision in *Smith v. Maryland* is "inapplicable to the specific activities mandated by the [Section] 1861 order at issue in the *Klayman* litigation." January 22 Petition at 3-4. Pursuant to the requirements of 50 U.S.C. § 1861(f), Judge Rosemary M. Collyer of this Court issued an Opinion and Order on March 20, 2014 ("March 20 Opinion and Order"), finding that the Petition provided no basis for vacating or

³ Following a declassification review by the Executive Branch, the Court published the January 22 Petition filed in Docket Number BR 14-01 in redacted form on April 25, 2014.

modifying the relevant production order issued in Docket Number BR 14-01.⁴ In her March 20 Opinion and Order, Judge Collyer engaged in an extensive analysis of Judge Leon's opinion in *Klayman*, ultimately disagreeing with his conclusion that *Smith v. Maryland* is inapplicable to the collection of bulk telephony metadata.

In issuing the Primary Order appended hereto which re-authorizes the bulk telephony metadata collection, I have carefully examined the noted U.S. District Court opinions, and I agree with Judge Collyer's analysis and opinion of the *Klayman* holding.

Amicus Curiae Brief

On April 3, 2014, the Center for National Security Studies filed an *amicus curiae* brief explaining why it believes that 50 U.S.C. §1861 does not authorize the collection of bulk telephony metadata. The *amicus* brief made a number of thoughtful points, the merits of which I have analyzed. Notwithstanding the Center's arguments, I find the authority requested by the FBI through the instant Application meets the requirements of the statute, and that the collection of bulk telephony metadata may be authorized under the terms of the statute.

⁴ Following a declassification review by the Executive Branch, the Court published the March 20 Opinion and Order issued in Docket Number BR 14-01 in redacted form on April 25, 2014.

Conclusion

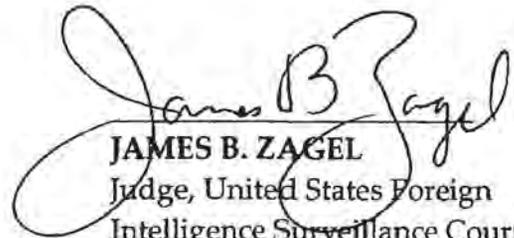
The unauthorized disclosure of the bulk telephony metadata collection more than a year ago led to many written and oral expressions of opinions about the legality of collecting telephony metadata. Congress is well aware that this Court has interpreted the provisions of 50 U.S.C. § 1861 to permit this particular collection, and diverse views about the collection have been expressed by individual members of Congress. In recent months, Congress has contemplated a number of changes to the Foreign Intelligence Surveillance Act, a few of which would specifically prohibit this collection. Congress could enact statutory changes that would prohibit this collection going forward, but under the existing statutory framework, I find that the requested authority for the collection of bulk telephony metadata should be granted. Courts must follow the law as it stands until the Congress or the Supreme Court changes it.

In light of the public interest in this particular collection and the government's declassification of related materials, including substantial portions of Judge Eagan's August 29 Opinion, Judge McLaughlin's October 11 Memorandum, and Judge Collyer's March 20 Opinion and Order, I request pursuant to FISC Rule 62 that this Memorandum Opinion and Accompanying Primary Order also be published, and I

~~TOP SECRET//SI//NOFORN~~

direct such request to the Presiding Judge as required by the Rule.

ENTERED this 19th day of June, 2014.


JAMES B. ZAGEL
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//SI//NOFORN~~



~~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]

[REDACTED]

Docket Number: BR

14 - 9 6

PRIMARY ORDER

A verified application having been made by the Deputy 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

~~TOP SECRET//SI//NOFORN~~

Derived from: Pleadings in the above-captioned docket
Declassify on: 20 June 2039

amended, requiring the 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

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

¹ The Honorable Rosemary M. Collyer issued an Opinion and Order finding that, under *Smith v. Maryland*, 442 U.S. 735 (1979), this bulk production of non-content call detail records does not involve a search or seizure under the Fourth Amendment. See FISC docket no. BR 14-01, Opinion and Order issued on March 20, 2014 (under seal and pending consideration for unsealing, declassification, and release). This authorization relies on that analysis of the Fourth Amendment issue. In addition, the Court has carefully considered opinions issued by Judges Eagan and McLaughlin in docket numbers BR 13-109 and BR 13-158, respectively, as well as the decision in *Smith v. Obama*, No. 2:13-CV-257-BLW, 2014 WL 2506421 (D. Idaho June 3, 2014), *American Civil Liberties Union v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. Dec. 27, 2013), *Klayman v. Obama*, 957 F.Supp.2d 1 (D.D.C. 2013), *U.S. v. Moalin*, No. 10cr4246 JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013), and the Brief of Amicus Curiae for Center for National Security Studies on the Lack of Statutory Authority for this Court's Bulk Telephony Metadata Orders, Misc. 14-01 (FISC filed Apr. 3, 2014), available at <http://www.fisc.uscourts.gov/sites/default/files/Misc%2014-01%20Brief-1.pdf>.

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, and as further explained in the accompanying Memorandum Opinion, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"² created by [REDACTED].

² 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)

B. The Custodian of Records of [REDACTED]

[REDACTED]

[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]

[REDACTED]

[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

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).

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 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.³ 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

³ 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.

authorized personnel who have received appropriate and adequate training.⁴

Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms⁵ 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

⁴ 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.

⁵



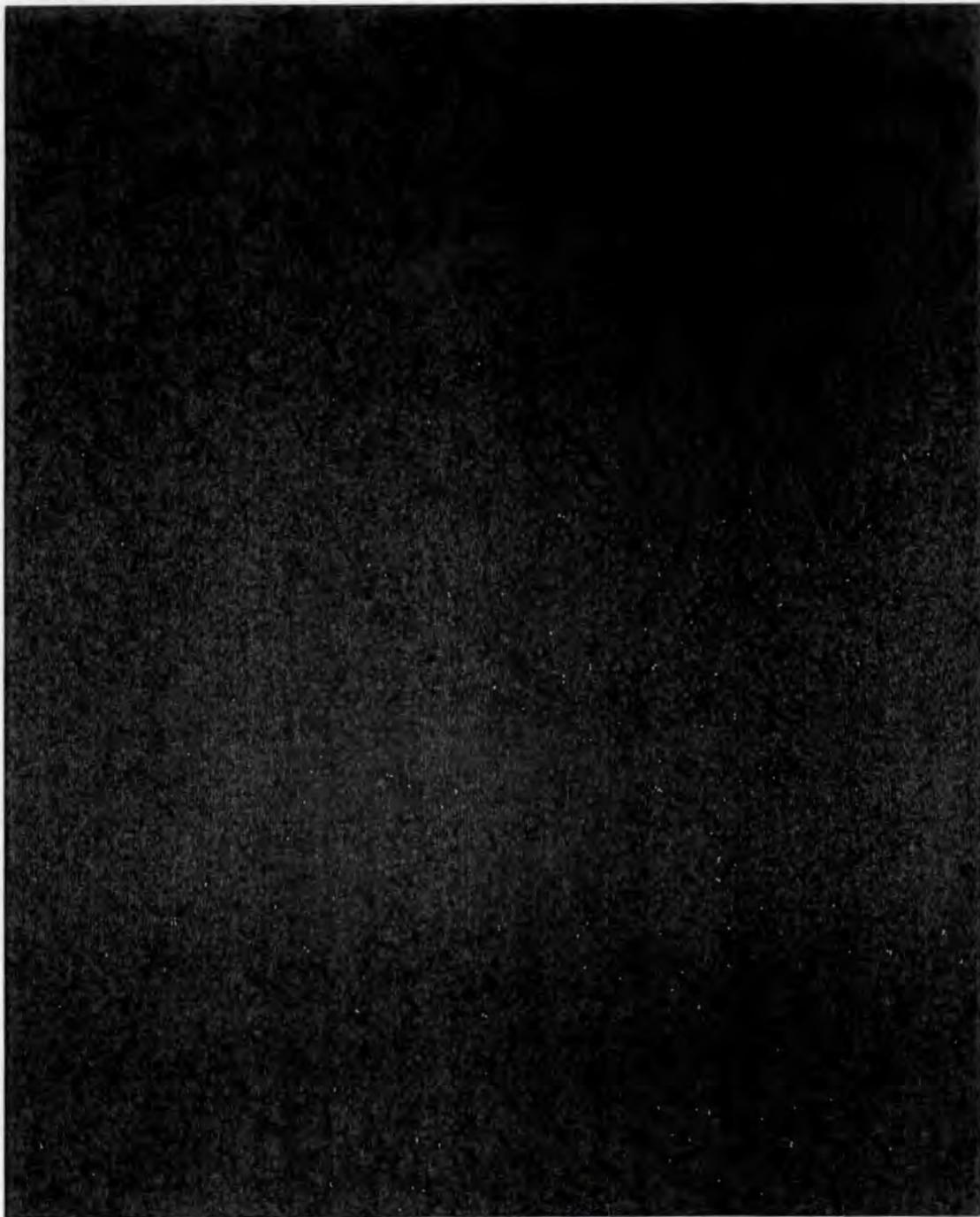
authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. The government may request, by motion and on a case-by-case basis, permission from the Court for NSA⁶ to use specific selection terms that satisfy the reasonable articulable suspicion (RAS) standard⁷ as "seeds" to query the BR metadata

⁶ 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.

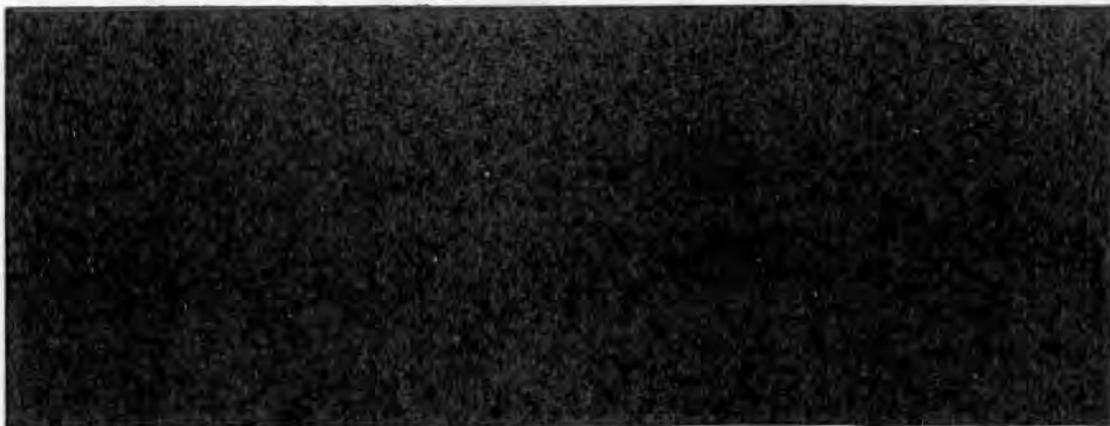
⁷ The reasonable articulable suspicion standard is met when, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [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. In the event the emergency provisions the Court's Primary Order are invoked by the Director or Acting Director, NSA's Office of General Counsel (OGC), in consultation with the Director or Acting Director will first 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.



TOP SECRET//SI//NOFORN

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 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. 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



TOP SECRET//SI//NOFORN

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 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

⁸ In the event the Court denies such motion, the government shall take appropriate remedial steps, including any steps the Court may direct.

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 NSA has implemented technical controls, which preclude any query for intelligence analysis purposes with a non-RAS-approved seed.

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]

[REDACTED] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.^{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

¹¹ This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

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]

[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 receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to this Order, [REDACTED]

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 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)

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."

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.

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 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.

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.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.¹⁷ OGC shall provide NSD/DoJ with copies 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

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.

~~TOP SECRET//SI//NOFORN~~

authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

(vi) 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

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

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 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.

- Remainder of this page intentionally left blank -

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

This authorization regarding [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] expires on the 12th day
of September, 2014, at 5:00 p.m., Eastern Time.

Signed 19 June 2014 16:35 Eastern Time
Date Time


JAMES B. ZAGEL
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//SI//NOFORN~~

[REDACTED]

~~TOP SECRET/COMINT/NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[REDACTED]

Docket Nos. [REDACTED]

OPINION AND ORDER REQUIRING DESTRUCTION OF
INFORMATION OBTAINED BY UNAUTHORIZED ELECTRONIC SURVEILLANCE

For the reasons explained below, the Court is ordering the government to destroy information obtained by unauthorized electronic surveillance that it conducted under color of orders issued in the above-referenced dockets pursuant to the electronic surveillance provisions of the Foreign Intelligence Surveillance Act (FISA), codified as amended at 50 U.S.C. §§ 1801-1812.

I. Background¹

The authorized surveillance target in this case was the [REDACTED].
The unauthorized electronic surveillance involved [REDACTED].

[REDACTED] Compliance notice filed on Aug. 26, 2010, at 1. The duration of unauthorized surveillance [REDACTED] ranged from approximately 15 months to three years and collectively involved over [REDACTED] improperly intercepted communications. *Id.* at 2-8.

Under its standard minimization procedures, NSA was obligated to “monitor the acquisition of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications outside the authorized scope of the surveillance or information concerning United States persons not related to the purpose of the surveillance.” Standard Minimization Procedures for Electronic Surveillance Conducted by the NSA (“SMPs”) § 3(b). The Court has found, and the government has not disputed, that NSA’s failure “to comply with

¹ See Opinion and Order Regarding Fruits of Unauthorized Electronic Surveillance issued on Dec. 10, 2010, at 1-3 (“December 10, 2010 Opinion”) for a discussion of the procedural history of this matter prior to that date. The December 10, 2010 Opinion is incorporated herein by reference.

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

this requirement resulted directly in the unauthorized intercept of [REDACTED] [REDACTED] December 10, 2010 Opinion at 5. Also contributing to the duration and volume of unauthorized surveillance in this case was the government's submission of [REDACTED] applications that falsely stated that [REDACTED]

The government proposed to retain the fruits of this unlawful surveillance, insofar as they reside in an NSA database called [REDACTED]. See Letter filed on Dec. 3, 2010 ("December 3, 2010 Letter"). In support of this proposal, the government argued that the SMPs did not apply to the fruits of unlawful surveillance, but only to interceptions authorized pursuant to the Court's orders. December 3, 2010 Letter at 2 n.3. Secondly, it argued that the criminal prohibition codified at 50 U.S.C. § 1809(a)(2) only prohibits use or disclosure of unlawfully obtained information for investigative or analytic purposes. *Id.* at 4-6.

The Court addressed both of these contentions in its December 10, 2010 Opinion. After examining the SMPs and the statutory provisions relating to minimization, the Court rejected the government's contention that the SMPs do not apply to over-collected information.³ December 10, 2010 Opinion at 3-6. The Court also noted that the SMPs appeared to require the destruction of at least some of the over-collected information. *Id.* at 5.

With regard to Section 1809(a)(2), the Court found unpersuasive the government's argument that the unqualified language of this prohibition only encompasses use or disclosure for investigative or analytic purposes. December 10, 2010 Opinion at 6-7. However, the Court recognized a narrower implicit exception from this prohibition for use or disclosure of "the results of unauthorized surveillance [that is] needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future." *Id.* at 8.

Based on the information available at the time of the December 10, 2010 Opinion, the Court could not ascertain whether or to what extent the over-collected information in this case might fall within this implicit exception to Section 1809(a)(2). *Id.* The Court ordered the

² See e.g., Docket No. [REDACTED], Declaration of [REDACTED], NSA, at 3-4 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

³ The Court uses the term "over-collected" to refer to information obtained by unauthorized electronic surveillance.

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

government to make a submission by January 31, 2011, providing additional information and analysis. *Id.* at 8-9. With the benefit of extensions, the government completed this submission on April 8, 2011, after filing an interim update on February 14, 2011. At the request of the government, a hearing was conducted in this matter on May 10, 2011.

II. The Current Status of the Over-Collected Information

Since the December 10, 2010 Opinion, NSA has completed its efforts to locate and purge the information obtained from this unauthorized electronic surveillance from data repositories other than [REDACTED] Verified Factual Update filed on Feb. 14, 2011 (“Verified Factual Update”), at 4-5. Information from [REDACTED] records was used in this process. *Id.* at 5. More specifically, NSA reports that it [REDACTED]

[REDACTED] *Id.* at 4-5. NSA assesses that it is “highly unlikely” that information obtained from this unauthorized surveillance exists in any repository other than [REDACTED] *Id.* at 3 n.2.

Within [REDACTED] information from this unauthorized surveillance is retained in [REDACTED] [REDACTED]. Government’s Response submitted on April 8, 2011 (“Government’s Response”) at 6. [REDACTED]

[REDACTED]

[REDACTED]

4 [REDACTED]

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

Each [REDACTED] record corresponding to the over-collected information in this case has been marked as “subject to purge.” Verified Factual Update at 5. The government proposes to retain, use, and disclose the over-collected information in [REDACTED] subject to certain restrictions that are discussed *infra* at page 6.

III. Analysis – Section 1809(a)(2)

Section 1809(a) states without qualification: “A person is guilty of an offense if he intentionally . . . (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized” by statute. The December 10, 2010 Opinion recognized a narrow implicit exception to this prohibition for “actions that are necessary to mitigate or prevent the very harms at which Section 1809(a)(2) is addressed.” December 10, 2010 Opinion at 8 (emphasis in original). The Court observed that this exception “must be carefully circumscribed, so that it does not lead to an unjustified departure from the terms of the statute.” *Id.* The Court indicated that this exception would encompass “use” or “disclosure” in the course of “actions in direct response to unauthorized surveillances” that are “necessary to avoid similar instances of over-collection (e.g., by identifying and remedying a technical malfunction) or to remedy a prior over-collection (e.g., by aiding the identification of over-collected information in various storage systems).” *Id.* at 7. The Court was doubtful that future use or disclosure of the over-collected information in this case could fall within this narrow exception, “now that the over-collection has been conclusively attributed” to “failure to recognize and respond properly to [REDACTED] [REDACTED] and that “apparently all of the [over-collected] information . . . has been purged or marked for purging.” *Id.* at 8.

A. Scope of the Implicit Exception

Because the outcome of this case depends on the scope of this exception, a full explanation of why Section 1809(a)(2) admits only a narrowly focused exception is appropriate. “Federal crimes are defined by Congress, and so long as Congress acts within its constitutional power in enacting a criminal statute,” a court “must give effect to Congress’ expressed intention concerning the scope of conduct prohibited.” United States v. Kozminski, 487 U.S. 931, 939

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

(1988); accord, e.g., United States v. Lanier, 520 U.S. 259, 267 n.6 (1997) (“Federal crimes are defined by Congress, not the courts,” and in construing criminal statutes courts are “oblige[d] . . . to carry out congressional intent as far as the Constitution will admit.”). This generally means that, “in applying criminal laws,” courts “must follow the plain and unambiguous meaning of the statutory language,” United States v. Albertini, 472 U.S. 675, 680 (1985), and bear in mind that it is for Congress to resolve “the pros and cons of whether a statute should sweep broadly or narrowly.” United States v. Rodgers, 466 U.S. 475, 484 (1984).

More specifically, courts should not attempt “to restrict the unqualified language of a [criminal] statute to the particular evil that Congress was trying to remedy – even assuming that it is possible to identify that evil from something other than the text of the statute itself.” Brogan v. United States, 522 U.S. 398, 403 (1998). Thus, even if it were established that Congress enacted Section 1809(a)(2) in order to curb investigative abuses, that provision would still properly apply to non-investigative uses or disclosures. See Albertini, 472 U.S. at 682 (criminal prohibition applies even though enacting Congress “very likely gave little thought” to circumstances in question). The exception recognized in the December 10, 2010 Opinion stands on narrower but firmer ground: that in limited circumstances, prohibiting use or disclosure of the results of unauthorized electronic surveillance would be “so ‘absurd or glaringly unjust’ . . . as to [call into] question whether Congress actually intended what the plain language” of Section 1809(a)(2) “so clearly imports.” Rodgers, 466 U.S. at 484 (quoting Sorrells v. United States, 287 U.S. 435, 450 (1932)); accord Chapman v. United States, 500 U.S. 453, 463-64 (1991); see also United States v. Rutherford, 442 U.S. 544, 552 (1979) (“Exceptions to clearly delineated statutes will be implied only where essential to prevent absurd results or consequences obviously at variance with the policy of the enactment as a whole.”) (internal quotations omitted).

B. Application of the Implicit Exception

In accordance with the narrowness of the exception it had articulated, the Court ordered the government to “specifically explain why [the] particular information” at issue in this case “is now needed to remedy past unauthorized surveillance or prevent similar unauthorized surveillance in the future.” December 10, 2010 Opinion at 8-9 (emphasis added). The government has not done so. At the May 10, 2011 hearing, the government conceded that there were no plausible circumstances in which further use or disclosure of the information obtained by the unauthorized surveillance in this case and now residing in ██████████ would prove necessary to these ends. See also Government’s Response at 9 (“The ██████████ compliance incident resulted from a set of discrete and specific facts [I]t did not result from technological problems and appears to be the result of human error.”).

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

Instead, the government argues that certain restrictions on access to the over-collected information in [REDACTED] will ensure that future use and disclosure will comport with Section 1809(a)(2). The Court disagrees for reasons explained below.⁵

The government reports that all records in [REDACTED] that are marked as subject to purge, including the records containing the over-collected information in this case, are only accessible to a limited number of authorized personnel, termed [REDACTED] Verified Factual Update at 5-6. And, pursuant to a policy adopted after the December 10, 2010 Opinion, “information from unauthorized electronic surveillance in [REDACTED] and marked as subject to purge will be used only when reasonably necessary (1) to remedy or prevent the 1809(a) harms^[6] arising from a particular incident of unauthorized electronic surveillance or (2) to evaluate and, when necessary, adjust NSA’s processes and procedures designed to remedy or prevent the 1809(a) harms.” Government’s Response at 13. As explained above, it is untenable that further use or disclosure of the over-collected information in this case is necessary for the first enumerated purpose.

In the government’s view, actions taken as “reasonably necessary” to the second enumerated purpose would include steps to implement “an enterprise-wide compliance program,” to include third-party audits and assessments, as well as monitoring and assessment of NSA’s internal controls. *Id.* at 14-15. The Court is unpersuaded that uses and disclosures of the over-collected information in this case would comply with Section 1809(a)(2) simply because they are in furtherance of this second purpose. That is not because the Court doubts the importance of an enterprise-wide compliance program in remedying or preventing 1809(a) harms. Rather, it is because there is no reason to believe that further use or disclosure of the specific over-collected information in this case will be needed for such a program to be effective, now that the cause of the unauthorized surveillance has been identified as discrete human error and all of the over-collected information has been purged or marked as subject to purge. After all, in a happier world where NSA had not unlawfully intercepted [REDACTED] under color of the orders in this case, NSA presumably would still have the wherewithal to devise and implement an effective compliance program. There is no reason to think that

⁵ The government also identifies adverse consequences that might follow from a general requirement to destroy over-collected information in [REDACTED]. Because this argument goes to the retention or destruction of over-collected information, rather than its use or disclosure, the Court addresses it in the context of minimization. *See infra* pp. 8-9.

⁶ The government has adopted the term “1809(a) harms” as shorthand for unauthorized electronic surveillance or use or disclosure of the results of such surveillance. *See, e.g.*, Government’s Response at 12-13, 17.

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

information about [REDACTED] is necessary for an effective, real-world compliance program, now that the particular incidents to which it pertains have been addressed.

The most that the government can claim is that, as an undifferentiated class, [REDACTED] records marked as subject to purge are needed for an effective compliance program. See Government's Response at 7-8, 10-11; Declaration of [REDACTED] Director of Compliance, NSA (" [REDACTED] Declaration") at 4 (submitted as Attachment B to the Government's Response). But it does not follow from this premise that use or disclosure of any information within that undifferentiated class would comport with Section 1809(a)(2), so long as it is made in furtherance of a compliance program designed to prevent or remedy 1809(a) harms at a programmatic level. Because the specific over-collected information at issue no longer has any distinctive utility for NSA's compliance efforts, it is neither absurd, nor glaringly unjust, nor obviously at variance with the policy of FISA as a whole, see *supra* p. 5, to conclude that Section 1809(a)(2) prohibits its further use or disclosure, even in the context of external auditing, monitoring of internal controls, or other aspects of an enterprise-wide compliance program.

IV. Analysis – SMPs

The Court's December 10, 2010 Opinion noted that Section 5(a) of the SMPs appears to require the destruction of at least some of the information over-collected in this case, December 10, 2010 Opinion at 5, and directed the government to "[a]ddress in detail . . . how the SMPs apply to the proposed retention and use of information obtained from this unauthorized surveillance." *Id.* at 8 (emphasis added). In response, the government has stated that the "SMPs do not explicitly address the Government's authority to retain, use, or disclose information from unauthorized electronic surveillance for the purpose of preventing or remedying . . . 1809(a) harms," and that the government "is assessing an appropriate amendment to the SMPs to account" for such situations. Government's Response at 17-18. The Court understands this response to its December 10, 2010 Opinion to concede that the SMPs, as now in effect, do not explicitly permit the retention of the over-collected information in this case.

Apart from this concession, it seems clear that the SMPs explicitly require NSA to destroy most, if not all, of the over-collected information in this case, and would do so even if the information had been lawfully acquired. The SMPs divide communications into two types: foreign communications and domestic communications. "Communications identified as domestic communications shall be promptly destroyed," subject to exceptions that appear inapplicable to this case. SMPs § 5(a). Similarly, foreign communications "of or concerning United States persons" may only be retained under specified circumstances that do not appear to be present in this case, and otherwise "shall be promptly destroyed." *Id.* §§ 3(e), 6(a). One category of communications is not subject to a general destruction requirement: foreign communications that are not of or concerning a U.S. person. *Id.* § 7. Given the definitions of the operative terms and

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

the nature of the unauthorized surveillance in this case, this category would consist of [REDACTED] [REDACTED] communications in which (1) at least one communicant was outside the United States; (2) no communicants were U.S. persons; and (3) no non-public information concerning a U.S. person was divulged. See *id.* § 2(b), (c), (e). Because [REDACTED] [REDACTED], one would expect that only a small percentage of the unlawful intercepts – if any – would satisfy all three conditions.

In any event, the government – notwithstanding the Court’s requiring a detailed discussion of how the SMPs apply to this case – has not addressed the effect of specific provisions or the status of particular types of communications. Instead, it requests the Court to recognize an implicit exception to the destruction requirements of the SMPs, despite the fact that this information was unlawfully acquired. For the reasons stated *supra* at pages 5-7, the Court concludes that further use or disclosure of the over-collected information in this case would not be consistent with Section 1809(a)(2). No lawful benefit can plausibly result from retaining this information, but further violation of law could ensue. Accordingly, the Court declines to find that the over-collected information in this case is subject to an implicit exception from the destruction requirements of the SMPs.

The government also describes various ways in which it might be burdensome or counterproductive to require NSA to purge from [REDACTED] information obtained by unauthorized electronic surveillance. It takes effort to identify information in [REDACTED]. See *Verified Factual Update* at 9-10. NSA anticipates difficulties in determining when records pertaining to a particular unauthorized electronic surveillance are no longer needed and asserts that premature destruction may impede NSA’s compliance efforts in ways not foreseen when a decision to destroy is made. *Government’s Response* at 9-12; [REDACTED] *Declaration* at 7-10. It is feared that NSA personnel may draw erroneous conclusions from the resulting gaps in data. [REDACTED] *Declaration* at 7.

To a considerable extent, these objections are directed at cases not before the Court. The records pertaining to the over-collected information in this case have already been identified and isolated, see *Government’s Response* at 6; *Verified Factual Update* at 9, and there is no difficulty in concluding that this over-collected information is no longer needed to prevent or remedy 1809(a) harms, see *supra* pp. 5-7. This case is therefore distinguishable from those that may require a longer period of technical examination or exploitation to understand and remedy causes of unauthorized surveillance or to identify and segregate over-collected information.

In this case, the government’s objections fall well short of establishing a need to exempt the over-collected information from the destruction requirements of the SMPs. It could be asserted that any requirement to destroy information “on a case-by-case basis . . . might have negative unintended consequences.” [REDACTED] *Declaration* at 10 (emphasis added). Nevertheless,

~~TOP SECRET/COMINT/NOFORN~~

~~TOP SECRET/COMINT/NOFORN~~

the SMPs routinely require NSA personnel to apply retention criteria on a case-by-case basis to information that was lawfully acquired, and promptly destroy information that does not satisfy those criteria. See *supra* pp. 7-8. There is no reason to think that this approach is distinctively unworkable for unlawfully acquired information. Indeed, a case-by-case assessment is most appropriate for over-collected information because, except in narrow circumstances, intentionally using or disclosing such information is a crime.

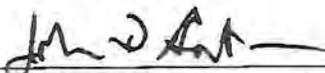
V. Conclusion

Information about these private, non-target communications should have never been acquired. Now that its further use or disclosure cannot reasonably be expected to be lawful, it should be destroyed.

For the reasons stated herein, the government is ORDERED to destroy all information in [REDACTED] that was obtained by the unauthorized electronic surveillance in this case. Although the Court cannot comprehensively identify such information based on the record before it, such information includes, to the extent it exists for each unlawfully intercepted [REDACTED] communication: [REDACTED]

[REDACTED] The government may accomplish this destruction by deleting entire records in [REDACTED] or by deleting all of the fields within records that contain information obtained by the unauthorized electronic surveillance, so long as all information obtained from this unauthorized electronic surveillance and contained in [REDACTED] is in fact destroyed. The government shall submit a written report no later than June 17, 2011, and at monthly intervals thereafter, describing the process by which it is destroying such information, until such time as the destruction process has been completed.

Entered this th 13 day of May, 2011, in Docket Nos. [REDACTED]

for 
FREDERICK J. SCULLIN, JR.
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET/COMINT/NOFORN~~

I, [REDACTED], Deputy Clerk,
FISC, certify that this document
is a true and correct copy of

the original.  Public Release.
January 31, 2011