

**CASE No. 19-16066
(PRIOR APPEALS: NOS. 10-15616, 15-16133)**

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

**CAROLYN JEWEL, TASH HEPTING, ERIK KNUTZEN, YOUNG BOON HICKS (AS EXECUTRIX
OF THE ESTATE OF GREGORY HICKS), AND JOICE WALTON,**

PLAINTIFFS-APPELLANTS,

v.

NATIONAL SECURITY AGENCY, *ET AL.*,

DEFENDANTS-APPELLEES.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF CALIFORNIA, No. 08-CV-04373-JSW
THE HONORABLE JEFFREY S. WHITE, UNITED STATES DISTRICT JUDGE, PRESIDING

**APPELLANTS' EXCERPTS OF RECORD
Vol. 5 of 8, Pages ER 589 to ER 843**

RACHAEL E. MENY
BENJAMIN W. BERKOWITZ
PHILIP J. TASSIN
KEKER, VAN NEST & PETERS LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400

THOMAS E. MOORE III
ROYSE LAW FIRM, PC
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 841-2369

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200

CINDY A. COHN
DAVID GREENE
LEE TIEN
KURT OPSAHL
ANDREW CROCKER
JAMIE L. WILLIAMS
AARON MACKKEY
JAMES S. TYRE
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

Counsel for Plaintiffs-Appellants

APPELLANTS' EXCERPTS OF RECORD**INDEX**

(ECF Numbers are from N.D. Cal. No. 08-CV-04373-JSW.)

VOLUME 1			
ECF No.	Date	Document Description	Page
464	4/25/19	Judgment	ER 001
463	4/25/19	Notice of Filing of Classified Order	ER 002
462	4/25/19	Order Granting Defendants' Motion for Summary Judgment and Denying Plaintiffs' Cross-motion	ER 003
412	8/28/18	Order Regarding Discovery Dispute	ER 029
410	8/17/18	Order Requiring Dispositive Motions Briefing	ER 031
404	6/13/18	Order Denying Plaintiffs' Motion for Access to Classified Discovery Materials and Requiring Additional Briefing	ER 034
356	5/19/17	Minute Order	ER 036
347	3/21/17	Order Granting Joint Request for Case Management Conference	ER 037
340	2/19/16	Order Granting Motion to Lift Stay of Discovery	ER 042
321	2/10/15	Order Denying Plaintiffs' Motion for Partial Summary Judgment and Granting Defendants' Motion for Partial Summary Judgment	ER 046

153	7/23/13	Amended Order	ER 056
VOLUME 2			
ECF No.	Date	Document Description	Page
465	5/20/19	Plaintiffs' Notice of Appeal and Representation Statement	ER 082
432	11/2/18	Declaration of Edward J. Snowden	ER 087
		Exhibit 1/Exhibit A: NSA document "ST 09-0002 Working Draft, Office of The Inspector General, National Security Agency," March 24, 2009 ("NSA Draft OIG Report").	ER 089
431	11/2/18	Declaration of David E. McCraw	ER 146
VOLUME 3			
ECF No.	Date	Document Description	Page
417-2	9/28/18	September 28, 2018 Declaration of Cindy A. Cohn in Opposition to the Government's Motion for Summary Judgment	ER 149

		Exhibit A: Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (January 23, 2014) (“PCLOB Section 215 Report”).	ER 151
VOLUME 4			
ECF No.	Date	Document Description	Page
417-2	9/28/18	September 28, 2018 Declaration of Cindy A. Cohn in Opposition to the Government’s Motion for Summary Judgment	ER 390
		Exhibit B: Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014) (“PCLOB Section 702 Report”).	ER 392
VOLUME 5			
ECF No.	Date	Document Description	Page
417-3	9/28/18	September 28, 2018 Declaration of David A. Greene in Opposition to the Government’s Motion for Summary Judgment (Exhibits D, E, F, G omitted)	ER 589

		Exhibit A: “PR/TT Order” issued by the Foreign Intelligence Surveillance Court compelling the bulk production of Internet metadata by electronic communications service providers.	ER 592
		Exhibit B: October 3, 2011 Order of the Foreign Intelligence Surveillance Court for the interception of Internet content.	ER 710
		Exhibit C: September 20, 2012 Opinion and Order of the Foreign Intelligence Surveillance Court.	ER 796
VOLUME 6			
ECF No.	Date	Document Description	Page
417-4	9/28/18	September 28, 2018 Declaration of Richard R. Wiebe in Opposition to the Government’s Motion for Summary Judgment	ER 844
		Exhibit A: Primary Order in docket BR 10-10 issued by the Foreign Intelligence Surveillance Court compelling the bulk production of telephone call records by multiple telephone companies.	ER 848
		Exhibit B: Excerpt from NSA Inspector General compliance audit report that includes as Appendix C a letter filed with the FISC by the NSA (the “NSA Letter”).	ER 868
		Exhibit C: AT&T’s Transparency Report of January 2016.	ER 908

		Exhibit D: Verizon's Transparency Report for the first half of 2016.	ER 921
		Exhibit E: NSA document published by the New York Times and ProPublica on August 15, 2015.	ER 930
		Exhibit F: Excerpt from George Molczan, <i>A Legal And Law Enforcement Guide To Telephony</i> (2005).	ER 932
		Exhibit G: NSA document published by the New York Times and ProPublica on August 15, 2015.	ER 943
		Exhibit H: Exhibit A to Plaintiffs' Revised First Set of Requests for Admission, served June 19, 2017.	ER 946
		Exhibit I: Exhibit B to Plaintiffs' Revised First Set of Requests for Admission, served June 19, 2017.	ER 953
417-5	9/28/18	Declaration of Phillip Long	ER 955
417-6	9/28/18	Declaration of Dr. Brian Reid	ER 960
417-7	9/28/18	Declaration of Professor Matthew Blaze	ER 979
417-8	9/28/18	Declaration of Ashkan Soltani	ER 993
417-9	9/28/18	Declaration of Carolyn Jewel	ER 999
417-10	9/28/18	Declaration of Tash Hepting	ER 1006
417-11	9/28/18	Declaration of Young Boon Hicks	ER 1012
417-12	9/28/18	Declaration of Erik Knutzen	ER 1014

417-13	9/28/18	Declaration of Joice Walton	ER 1019
262	7/25/14	Declaration of Richard R. Wiebe in Support of Plaintiffs' Motion for Partial Summary Judgment, Exhibit E	ER 1025
89	7/2/12	Declaration of J. Scott Marcus (exhibits omitted)	ER 1031
85	7/2/12	Declaration of Mark Klein	ER 1071
		Exhibit A (redacted version)	ER 1080
		Exhibit B (redacted version)	ER 1085
		Exhibit C (redacted version)	ER 1090
VOLUME 7			
ECF No.	Date	Document Description	Page
1	9/18/08	Complaint	ER 1098
	8/21/19	District Court Docket Sheet in N.D. Cal. No. 08-CV-04373-JSW	ER 1153
VOLUME 8 – PROVISIONALLY UNDER SEAL			
ECF No.	Date	Document Description	Page
84-1	7/2/12	Declaration of James Russell (Exhibit A omitted)	ER 1193

84-2	7/2/12	Declaration of Mark Klein	ER 1206
84-3	7/2/12	Exhibit A (under seal unredacted version)	ER 1216
84-4	7/2/12	Exhibit B (under seal unredacted version)	ER 1260
84-5, 84-6	7/2/12	Exhibit C (under seal unredacted version)	ER 1281

1 CINDY COHN (SBN 145997)
 cindy@eff.org
 2 DAVID GREENE (SBN 160107)
 LEE TIEN (SBN 148216)
 3 KURT OPSAHL (SBN 191303)
 JAMES S. TYRE (SBN 083117)
 4 ANDREW CROCKER (SBN 291596)
 JAMIE L. WILLIAMS (SBN 279046)
 5 ELECTRONIC FRONTIER FOUNDATION
 815 Eddy Street
 6 San Francisco, CA 94109
 Telephone: (415) 436-9333
 7 Fax: (415) 436-9993
 8 RICHARD R. WIEBE (SBN 121156)
 wiebe@pacbell.net
 9 LAW OFFICE OF RICHARD R. WIEBE
 44 Montgomery Street, Suite 650
 10 San Francisco, CA 94104
 Telephone: (415) 433-3200
 11 Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
 rmeny@keker.com
 BENJAMIN W. BERKOWITZ (SBN 244441)
 PHILIP J. TASSIN (SBN 287787)
 KEKER, VAN NEST & PETERS, LLP
 633 Battery Street
 San Francisco, CA 94111
 Telephone: (415) 391-5400
 Fax: (415) 397-7188
 THOMAS E. MOORE III (SBN 115107)
 tmoore@rroyselaw.com
 ROYSE LAW FIRM, PC
 149 Commonwealth Drive, Suite 1001
 Menlo Park, CA 94025
 Telephone: (650) 813-9700
 Fax: (650) 813-9777
 ARAM ANTARAMIAN (SBN 239070)
 antaramian@sonic.net
 LAW OFFICE OF ARAM ANTARAMIAN
 1714 Blake Street
 Berkeley, CA 94703
 Telephone: (510) 289-1626

12 Attorneys for Plaintiffs

13
 14
 15
 16 UNITED STATES DISTRICT COURT
 17 FOR THE NORTHERN DISTRICT OF CALIFORNIA
 18 OAKLAND DIVISION

19)
 20 CAROLYN JEWEL, TASH HEPTING,)
 YOUNG BOON HICKS, as executrix of the)
 21 estate of GREGORY HICKS, ERIK KNUTZEN)
 and JOICE WALTON, on behalf of themselves)
 22 and all others similarly situated,)
)
 23 Plaintiffs,)
)
 24 v.)
)
 25 NATIONAL SECURITY AGENCY, *et al.*,)
)
 26 Defendants.)

CASE NO. 08-CV-4373-JSW

September 28, 2018
Declaration Of
DAVID A. GREENE
In Opposition To The Government's
Motion For Summary Judgment

Courtroom 5, Second Floor
 The Honorable Jeffrey S. White

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I, David A. Greene, do hereby declare:

1. I am a member in good standing of the Bar of the State of California and the bar of this Court. I am counsel to plaintiffs in this action. Except as otherwise stated below, I could and would testify competently to the following.

2. Each exhibit attached hereto is a true and correct copy of the document located at the indicated source.

3. **Exhibit A:** Attached hereto as Exhibit A is a true and correct copy of a “PR/TT” order issued by the Foreign Intelligence Surveillance Court compelling the bulk production of Internet metadata by electronic communications service providers. *Available at* <https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf>.

4. **Exhibit B:** Attached hereto as Exhibit B is a true and correct copy of an order issued by the Foreign Intelligence Surveillance Court for the interception of Internet content on October 3, 2011. *Available at* <https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>.

5. **Exhibit C:** Attached hereto as Exhibit C is a true and correct copy of a September 20, 2012 Opinion and Order of the Foreign Intelligence Surveillance Court, released by the government as a result of FOIA litigation with the ACLU. *Available at* <https://www.aclu.org/foia-document/fisc-opinion-and-order-re-section-1809>.

6. **Exhibit D:** Attached hereto as Exhibit D is a true and correct copy of the Further Observations of the Government of the United Kingdom, submitted to the European Court of Human Rights on December 16, 2016 in *Ten Human Rights Organisations and The United Kingdom* (No. 24960/15) (Eur. Ct. H.R. Dec. 16, 2016). *Available at* <http://privacyinternational.org/sites/default/files/2018-02/2016.12.16%20Government%27s%20further%20obs.pdf>.

7. **Exhibit E:** Attached hereto as Exhibit E is a true and correct copy of the *Report on the Bulk Powers Review*, by David Anderson, Q.C., Independent Reviewer of Terrorism Legislation (August 19, 2016). *Available at*

<https://www.gov.uk/government/publications/investigatory-powers-bill-bulk-powers-review>.

8. **Exhibit F:** Attached hereto as Exhibit F is a true and correct copy of “Privacy and Security: A modern and transparent legal framework,” by the Intelligence and Security Committee of Parliament, Ordered by the House of commons to be printed on 12 March 2015. Available at <https://info.publicintelligence.net/UK-ISC-MassSurveillance.pdf>.

9. **Exhibit G:** Attached hereto as Exhibit E is a true and correct copy of The United Kingdom’s Observations on the Merits, submitted on April 18, 2016 to the European Court of Human Rights on December 16, 2016 in *Ten Human Rights Organisations and The United Kingdom* (No. 24960/15) (Eur. Ct. H.R. Apr. 18, 2016). Available at <http://privacyinternational.org/sites/default/files/2018-02/United%20Kingdom%E2%80%99s%20Observations%20on%20the%20Merits.pdf>.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief.

Executed September 28, 2018.



David A. Greene

EXHIBIT A


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

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).

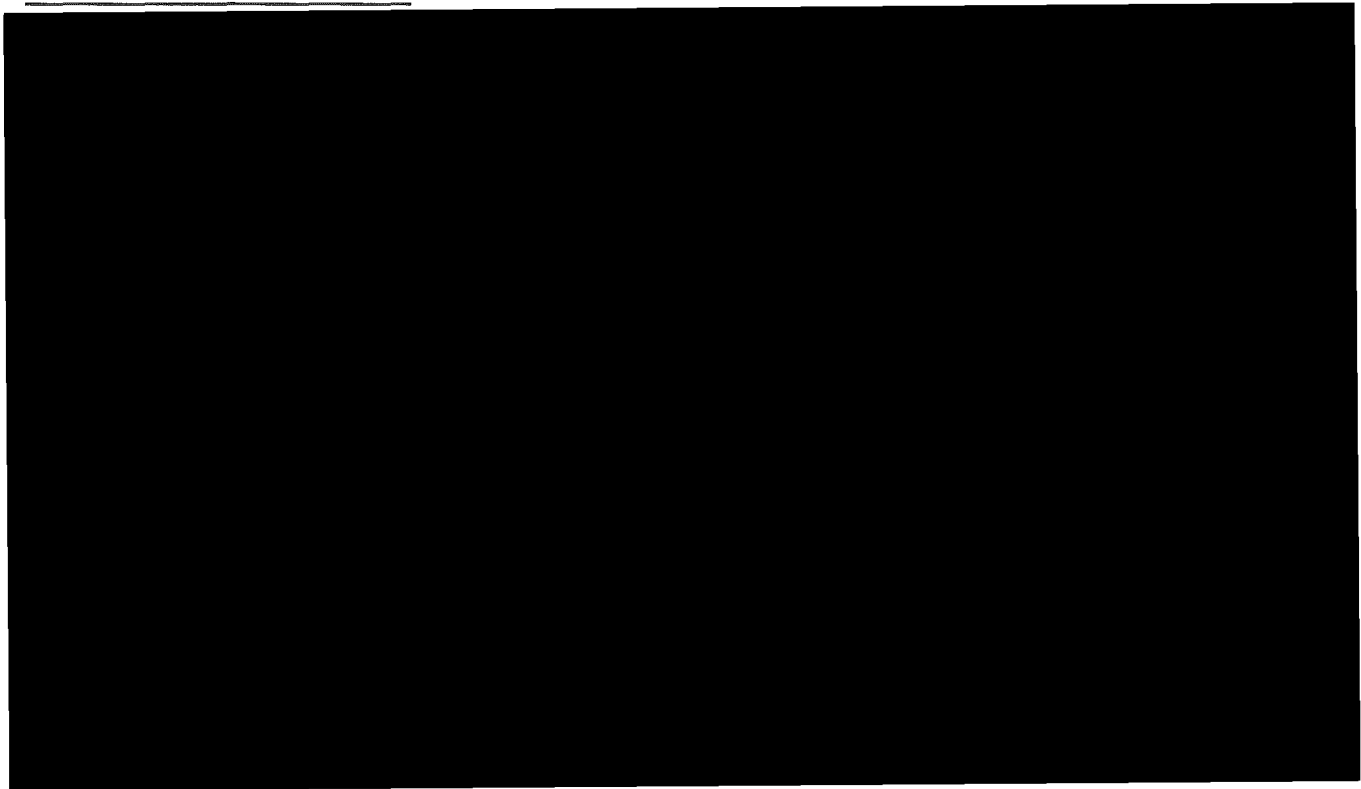
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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

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



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

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

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)

[REDACTED]

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

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

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.

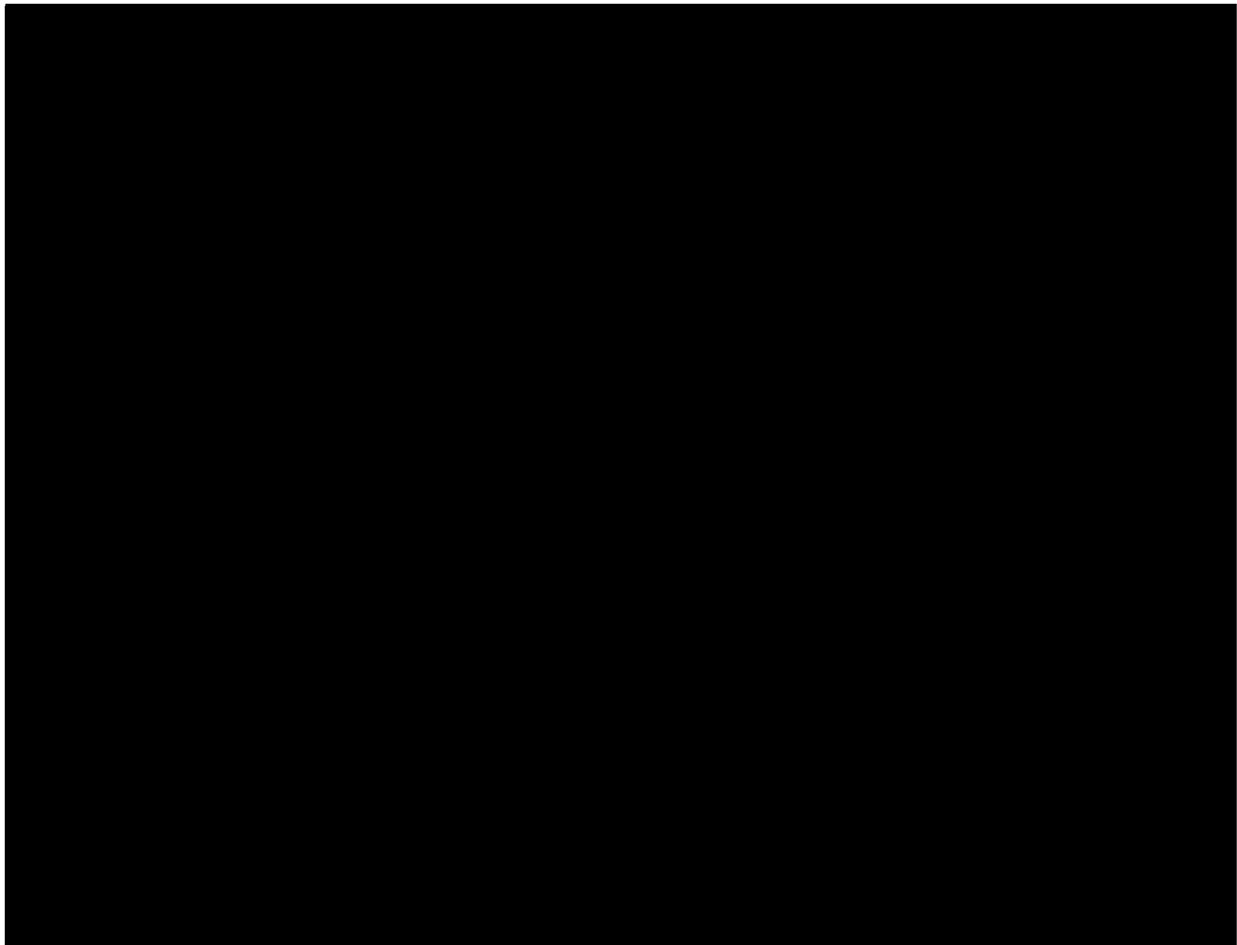
The [REDACTED] Opinion authorized the acquisition of [REDACTED] categories of metadata:

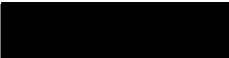
[REDACTED]

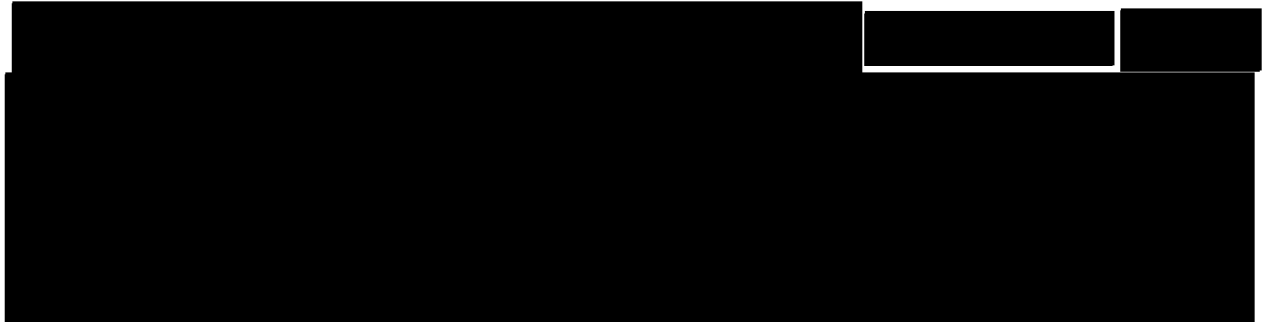
[REDACTED]

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

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



The government proposed to collect these categories of metadata from 

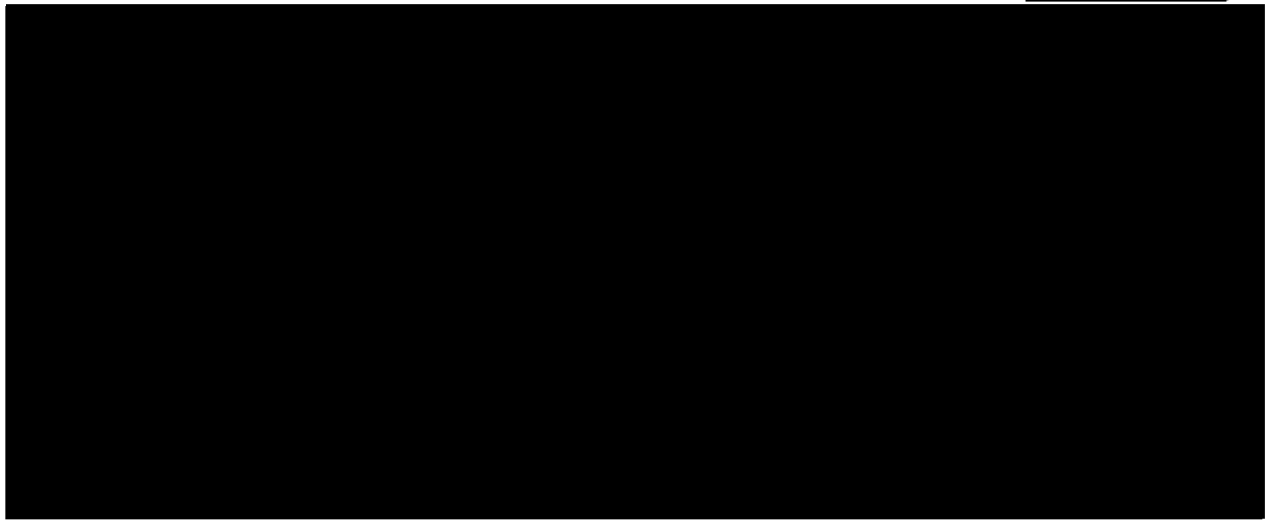


~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



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...)

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

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

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.

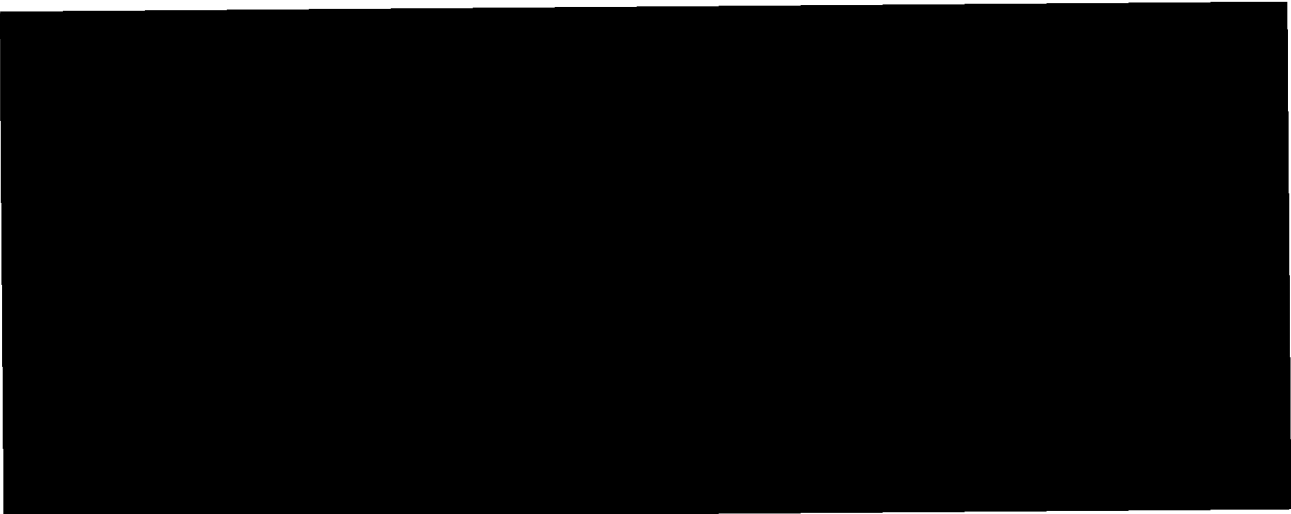
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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

(██████████ 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.



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

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

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.

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

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

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]

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

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

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.

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

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

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.

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

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

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]

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

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

“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.

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

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

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...)

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

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

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]

[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...)

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

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

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.

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

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

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

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

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

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.” ██████████ 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. ██████████ 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* ██████████ Report, Exhibit A, at 18-19.

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

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

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

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*.

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

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

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]

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

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

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.

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

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

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]

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

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

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

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.

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

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

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.

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

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

(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.

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

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

(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]

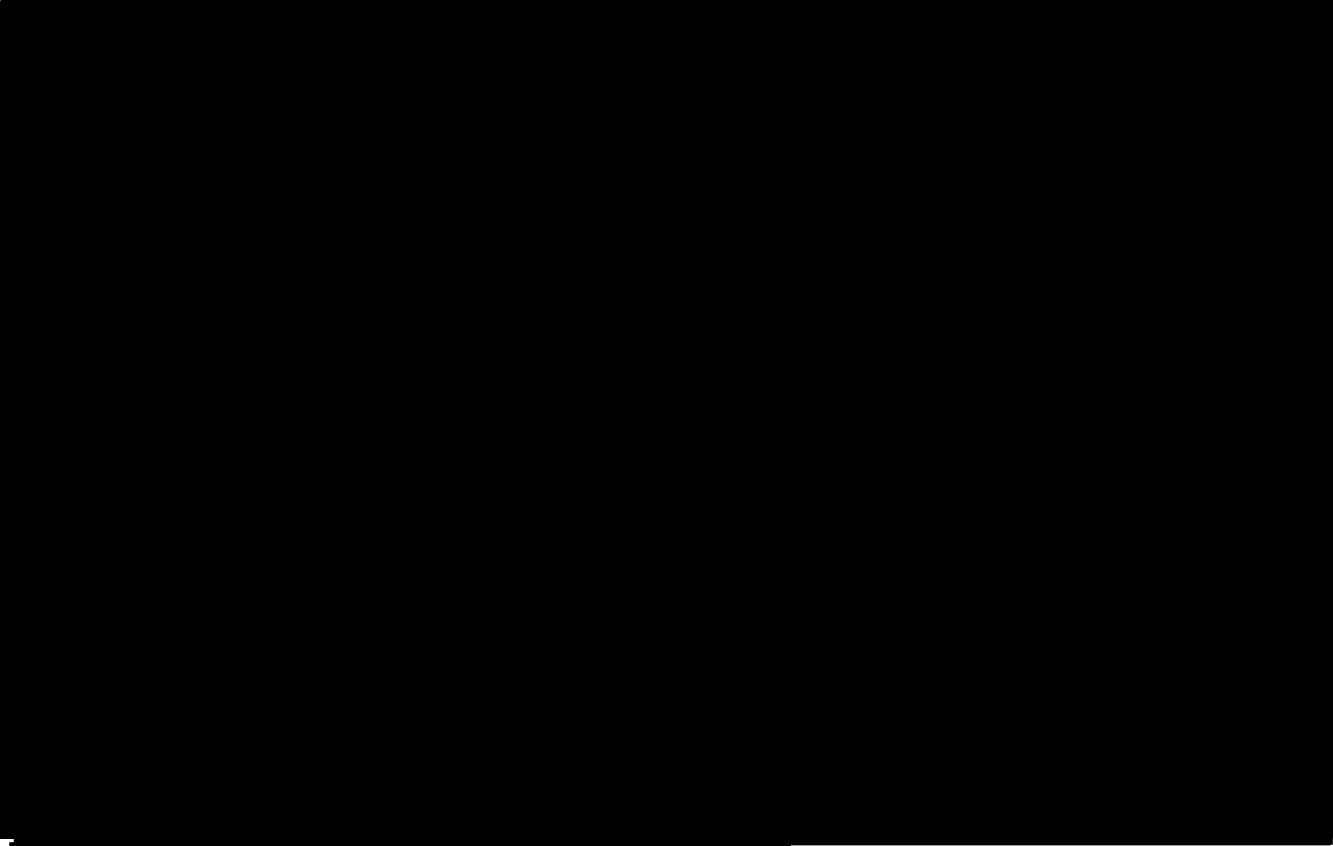
[REDACTED]

[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).

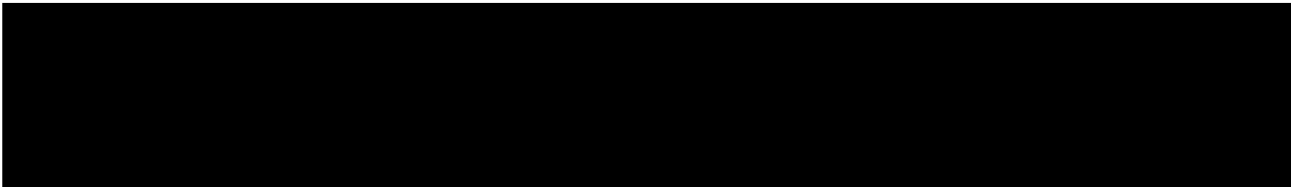
~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN



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



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

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

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]

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).

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

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

resulting from ██████████ 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 ██████████ 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 ██████████ 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.

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

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

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

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

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

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).

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

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

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).

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

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

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.”).

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

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

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

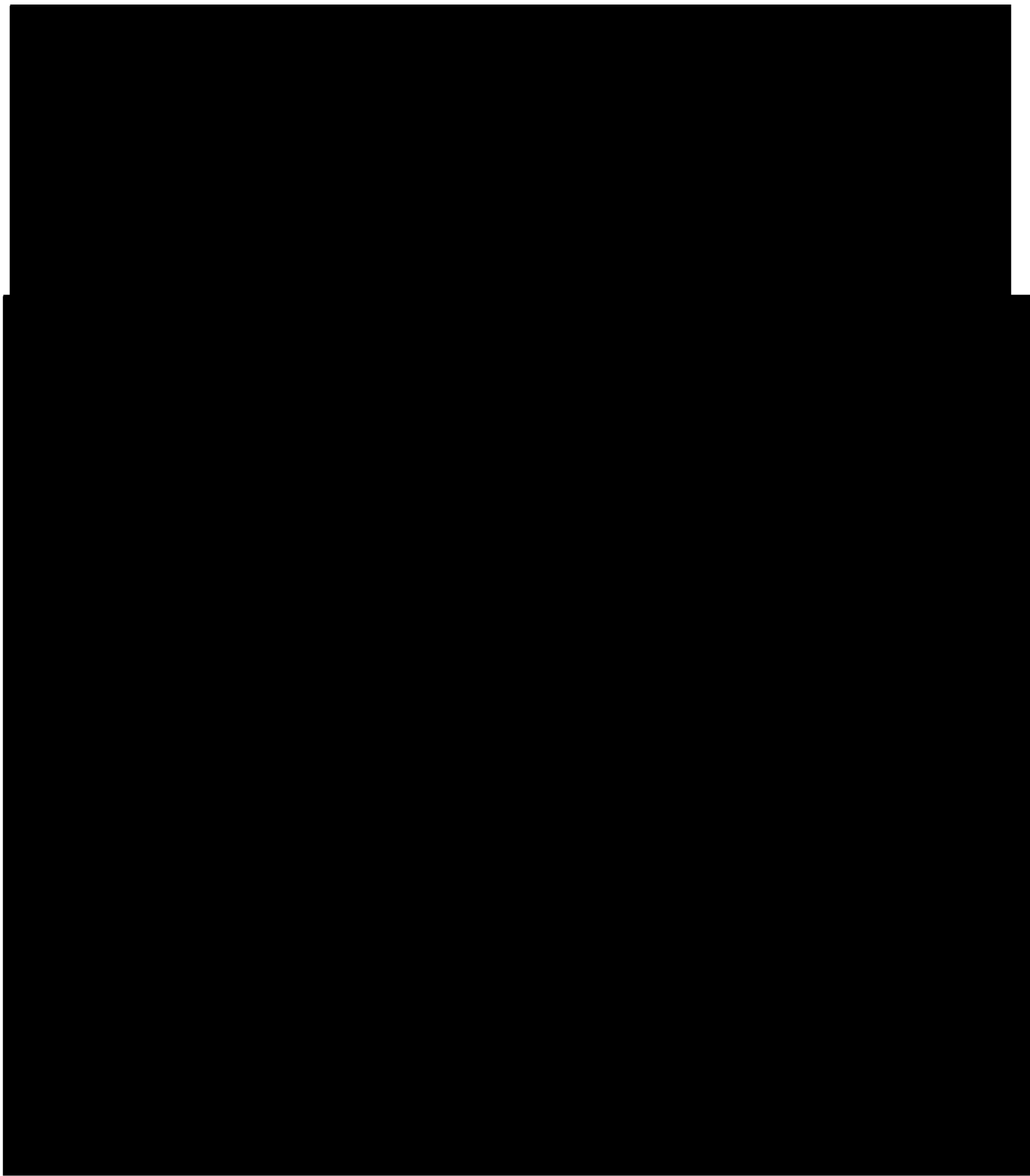
The government requests authority to [REDACTED] categories of

[REDACTED]

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

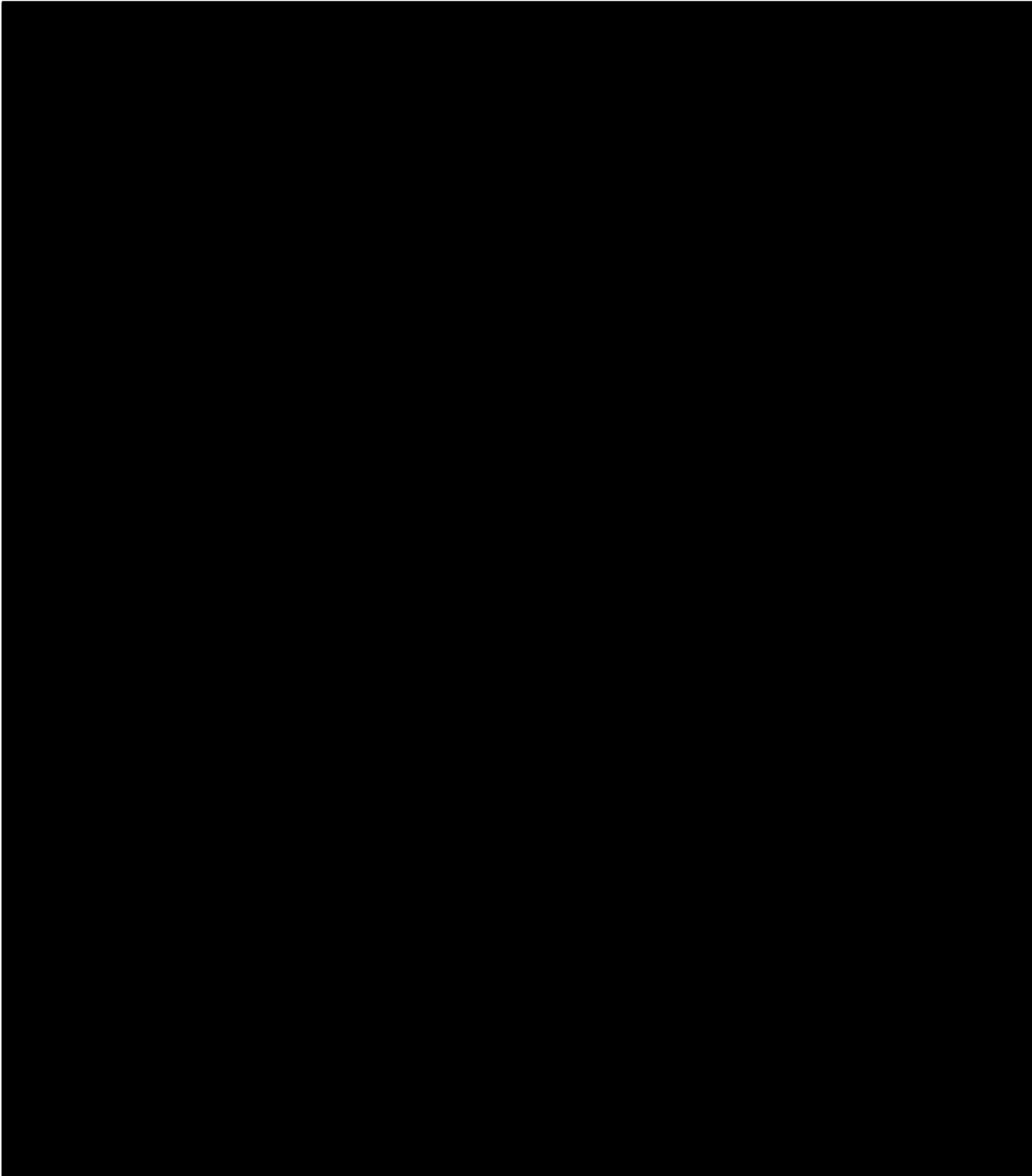
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



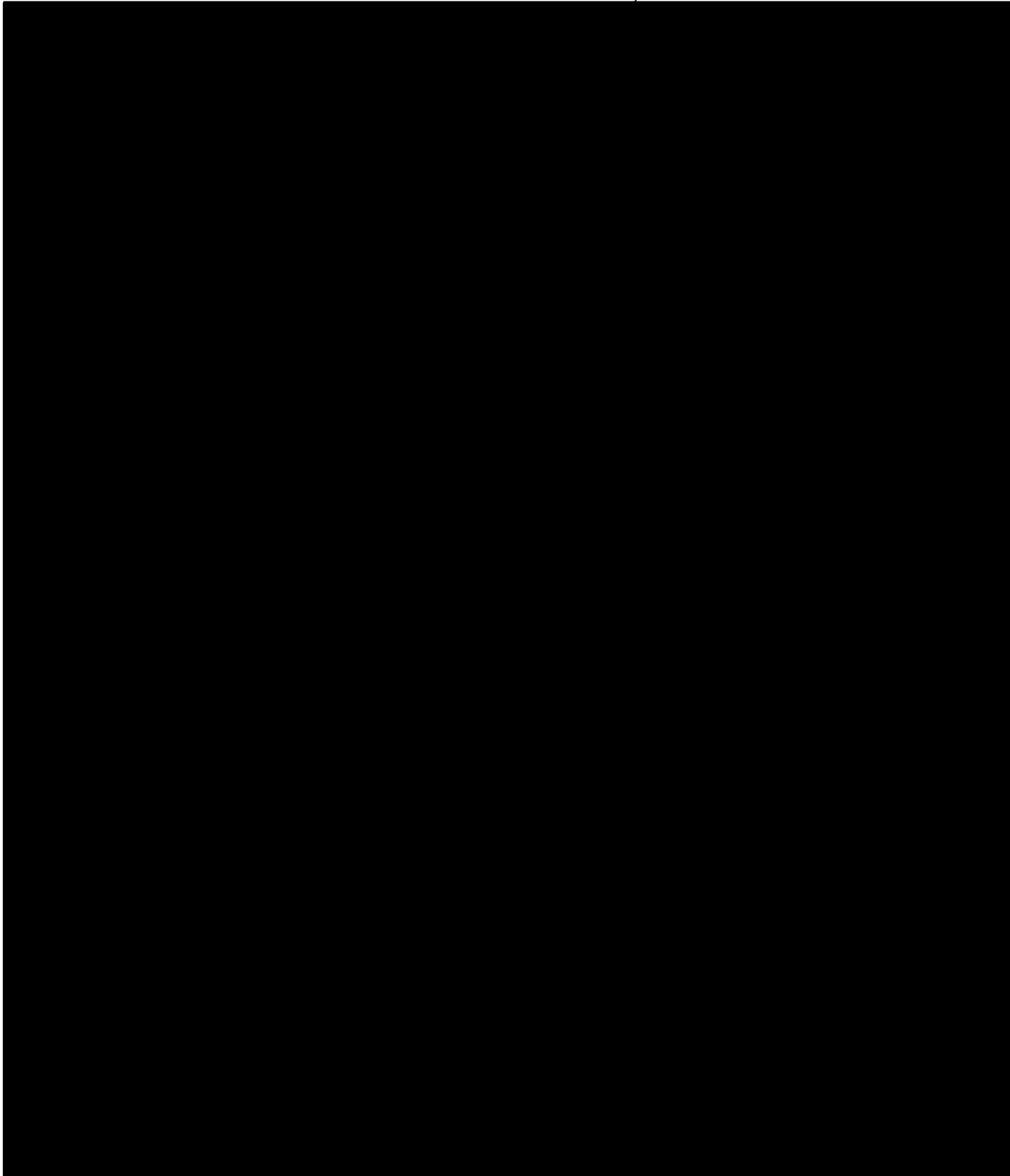
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



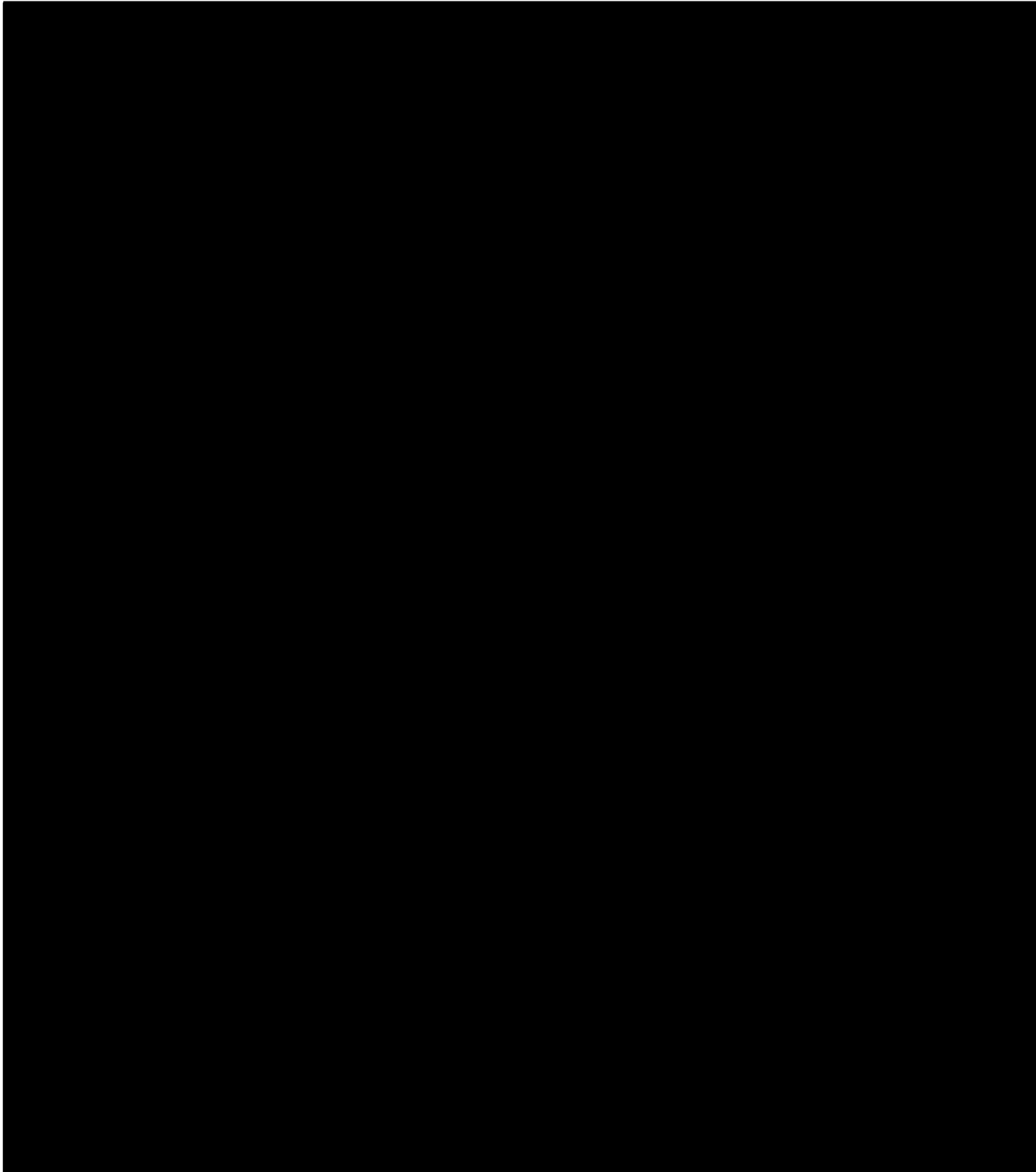
~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN



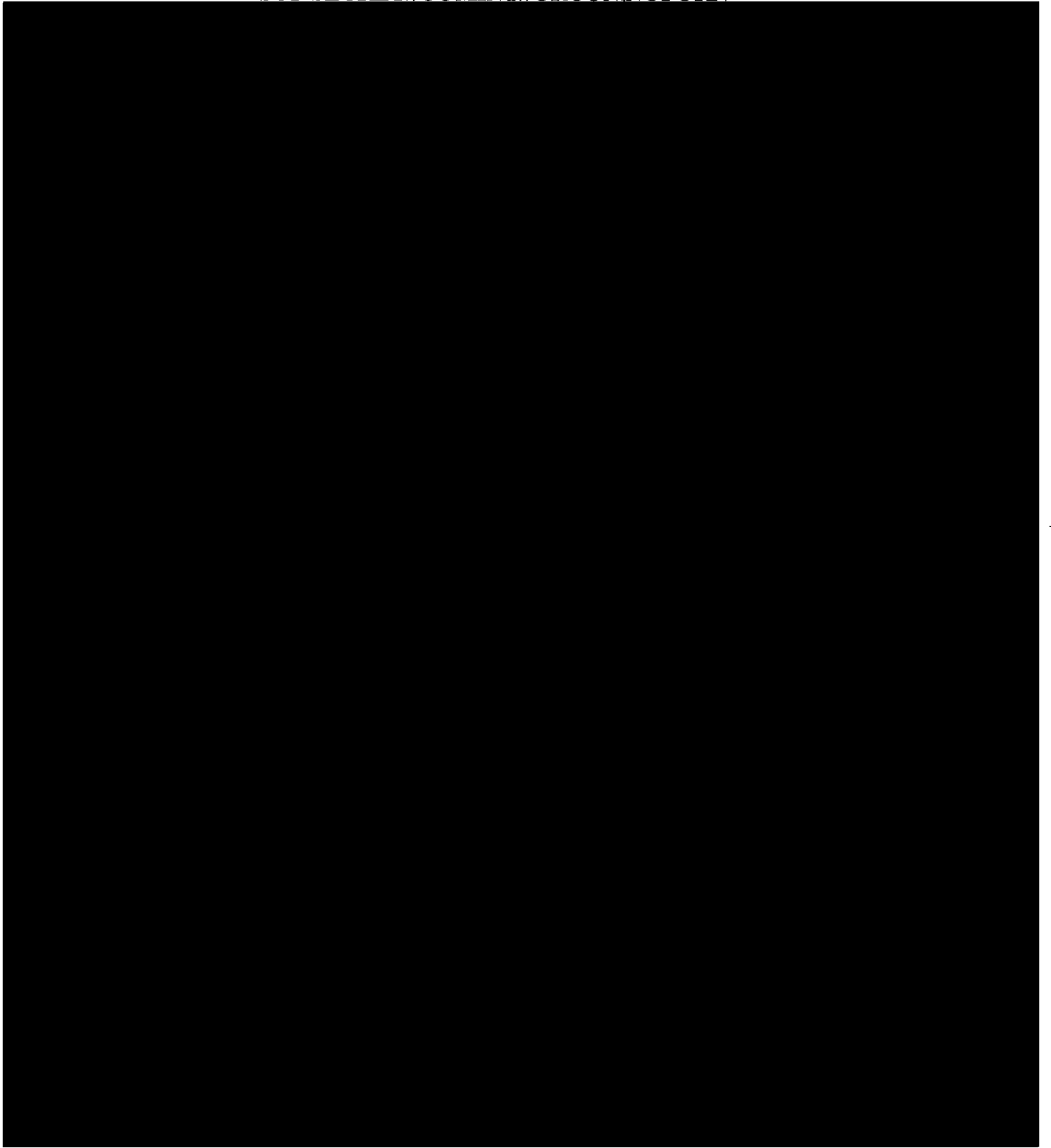
~~**TOP SECRET//COMINT//ORCON,NOFORN**~~

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



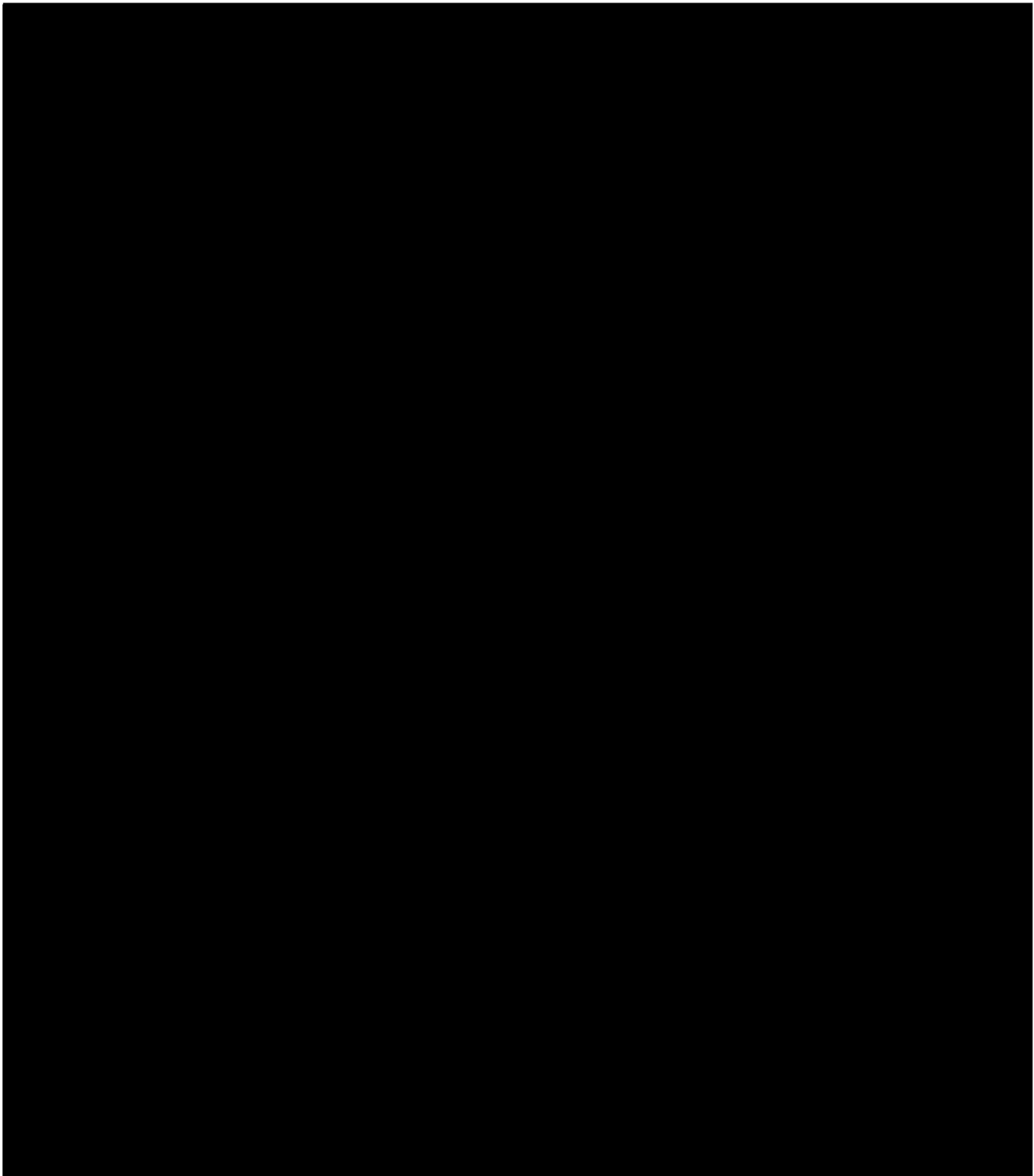
~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN



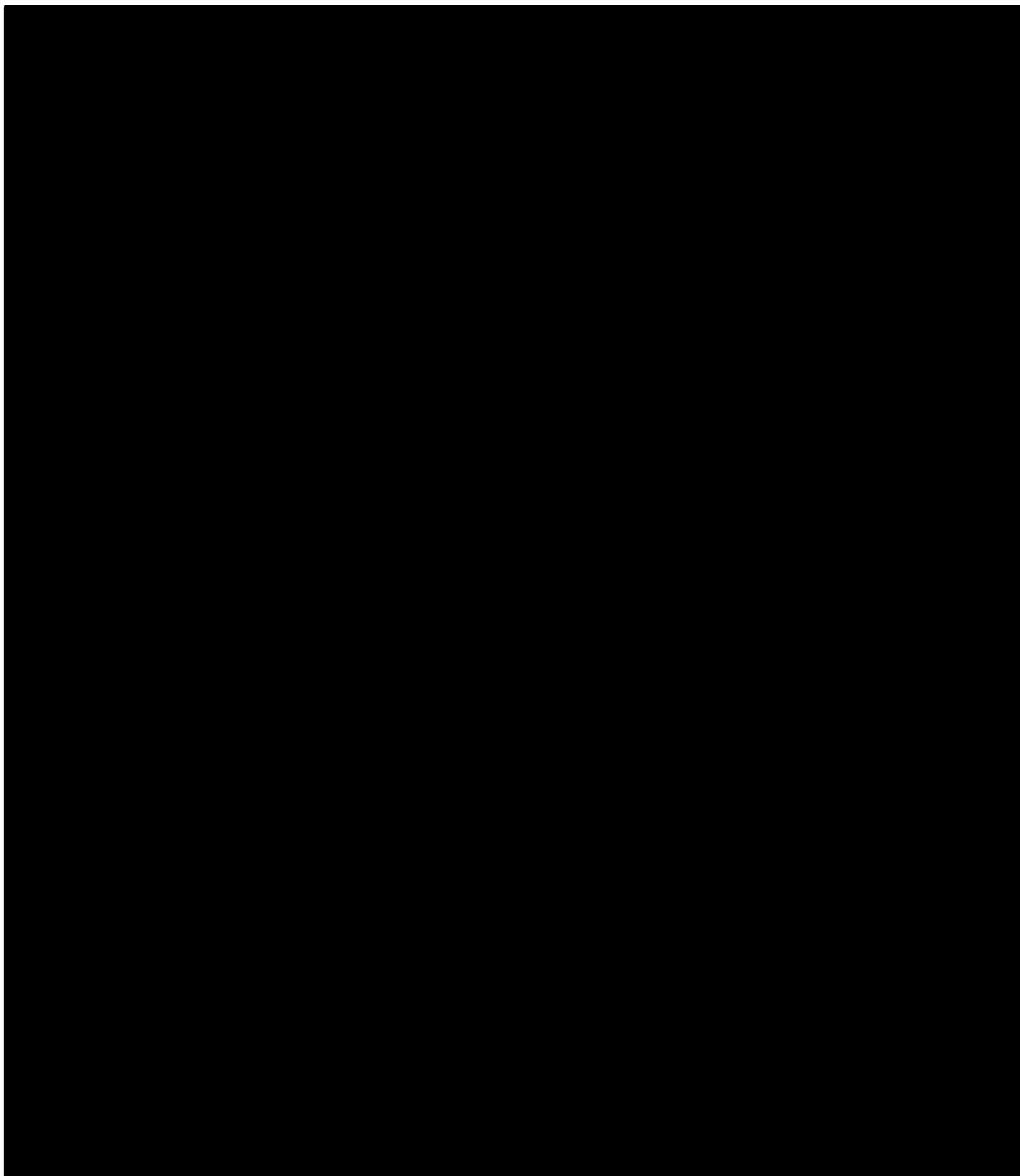
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



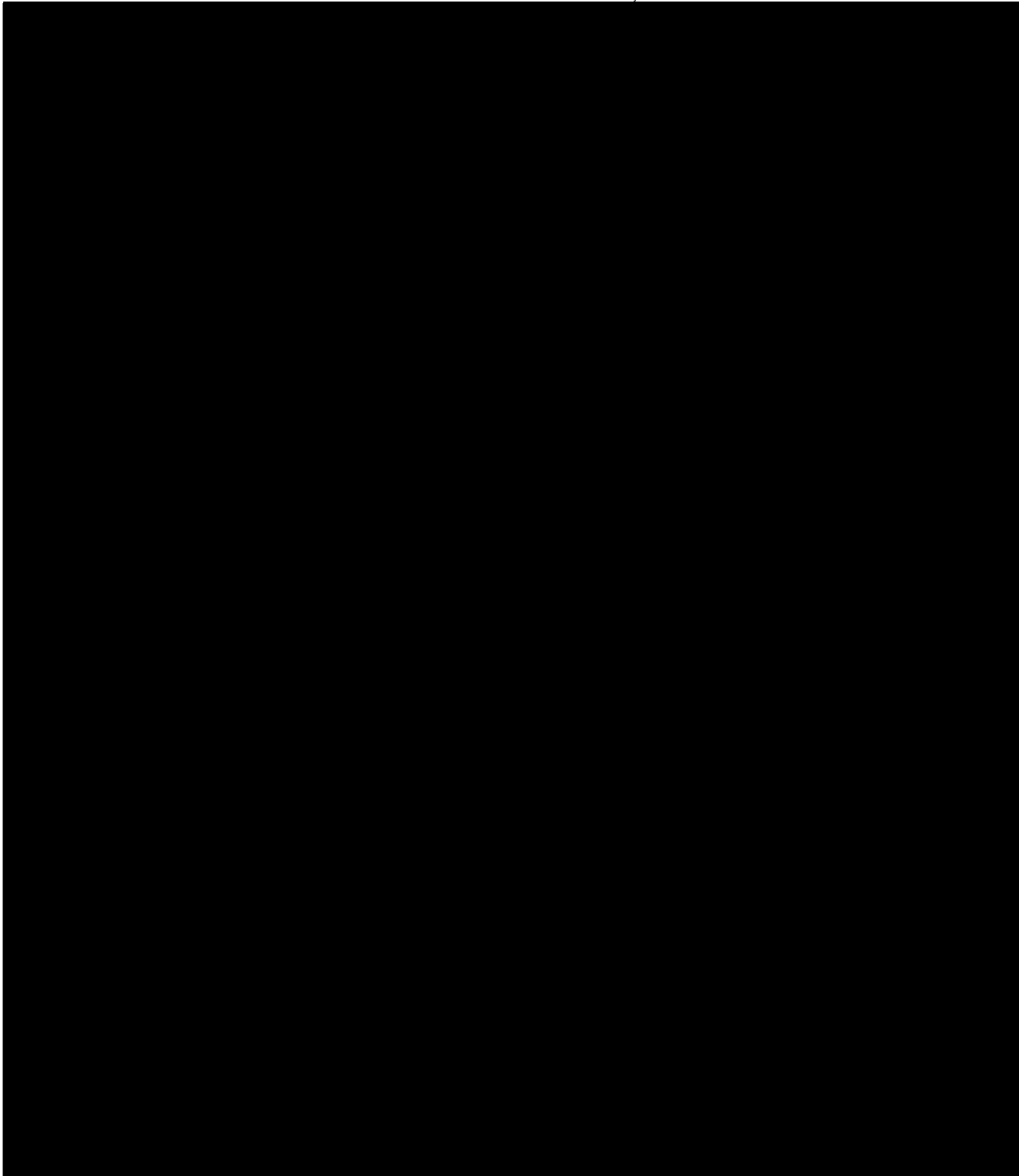
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



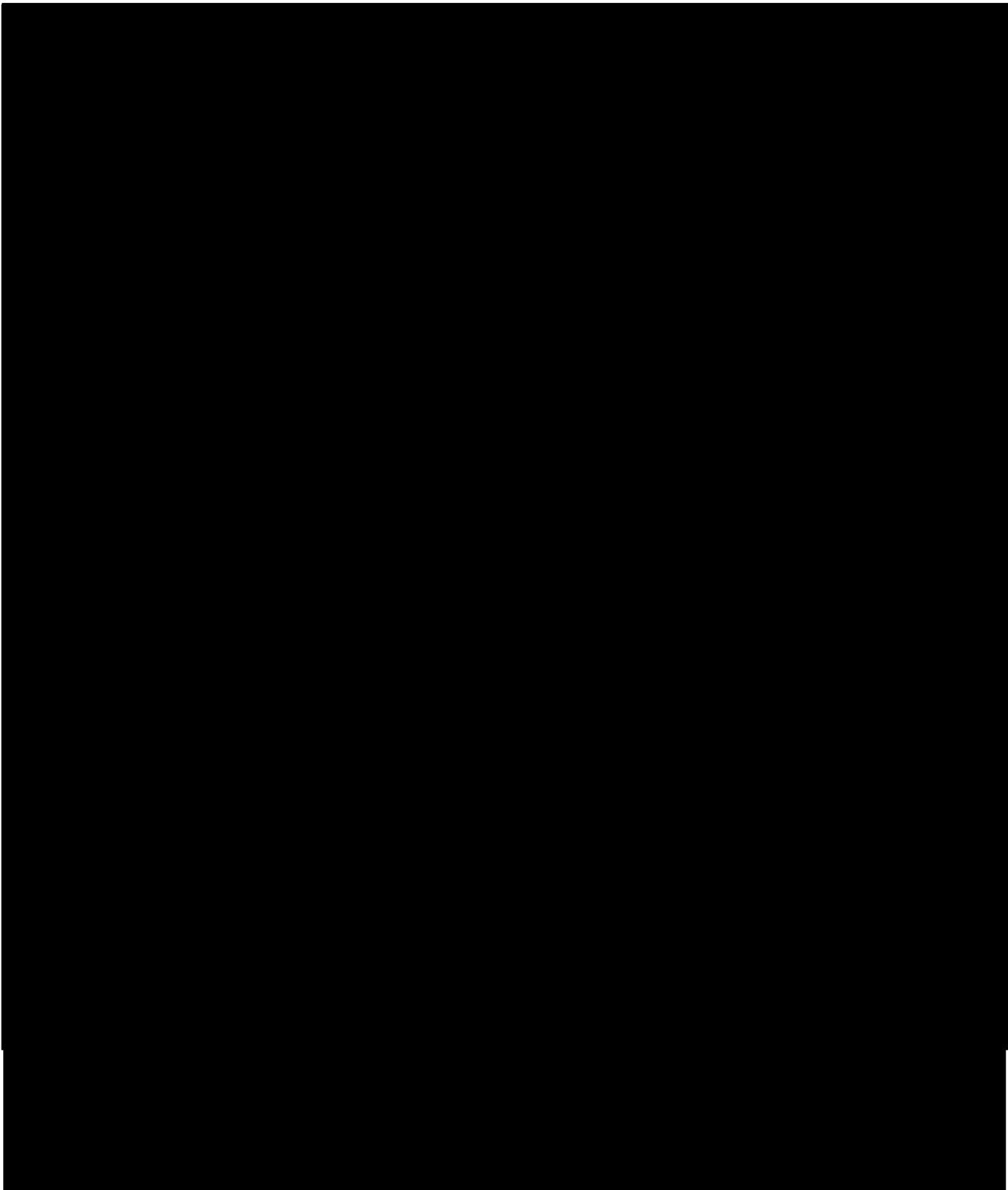
~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN



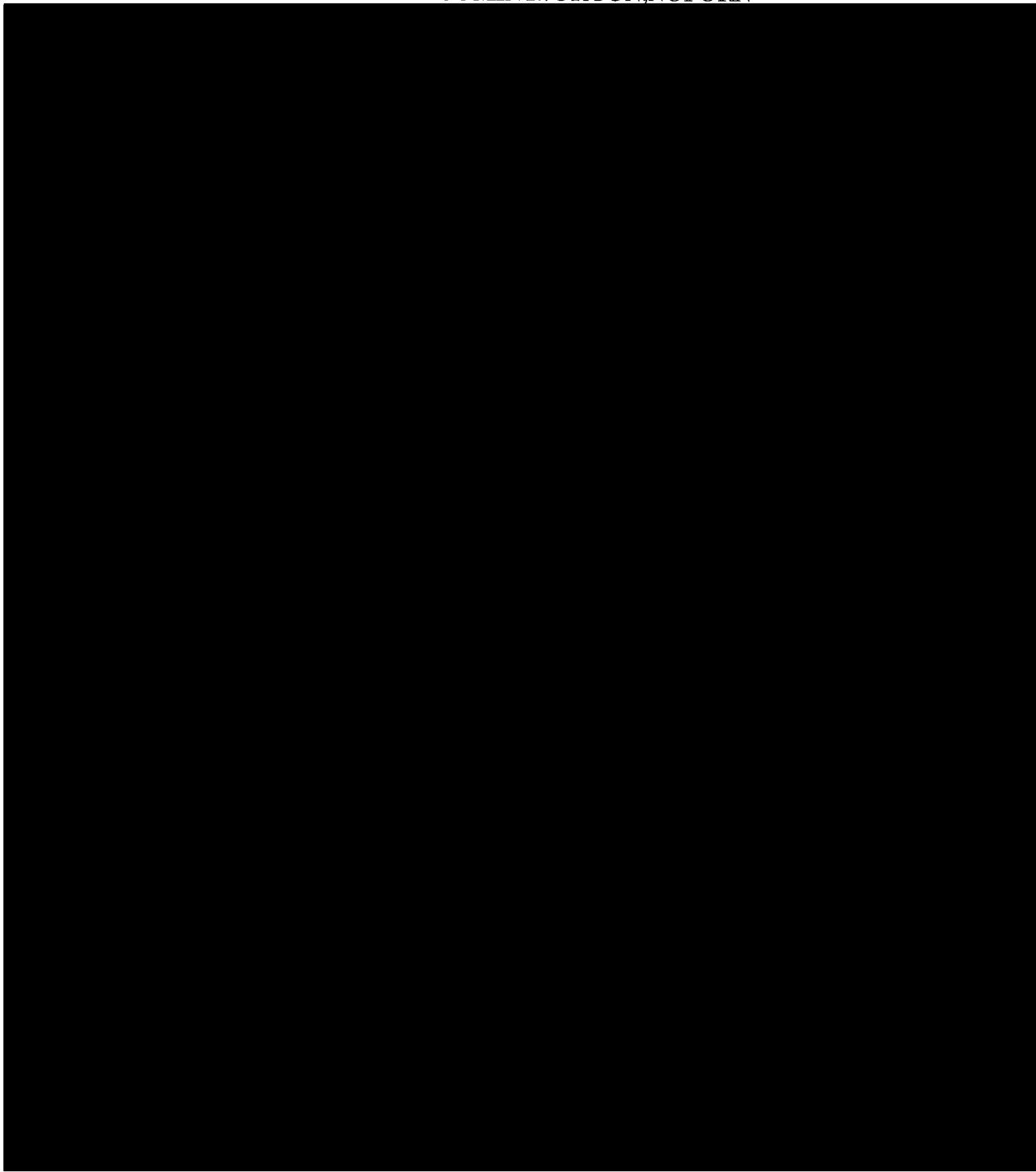
~~**TOP SECRET//COMINT//ORCON,NOFORN**~~

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



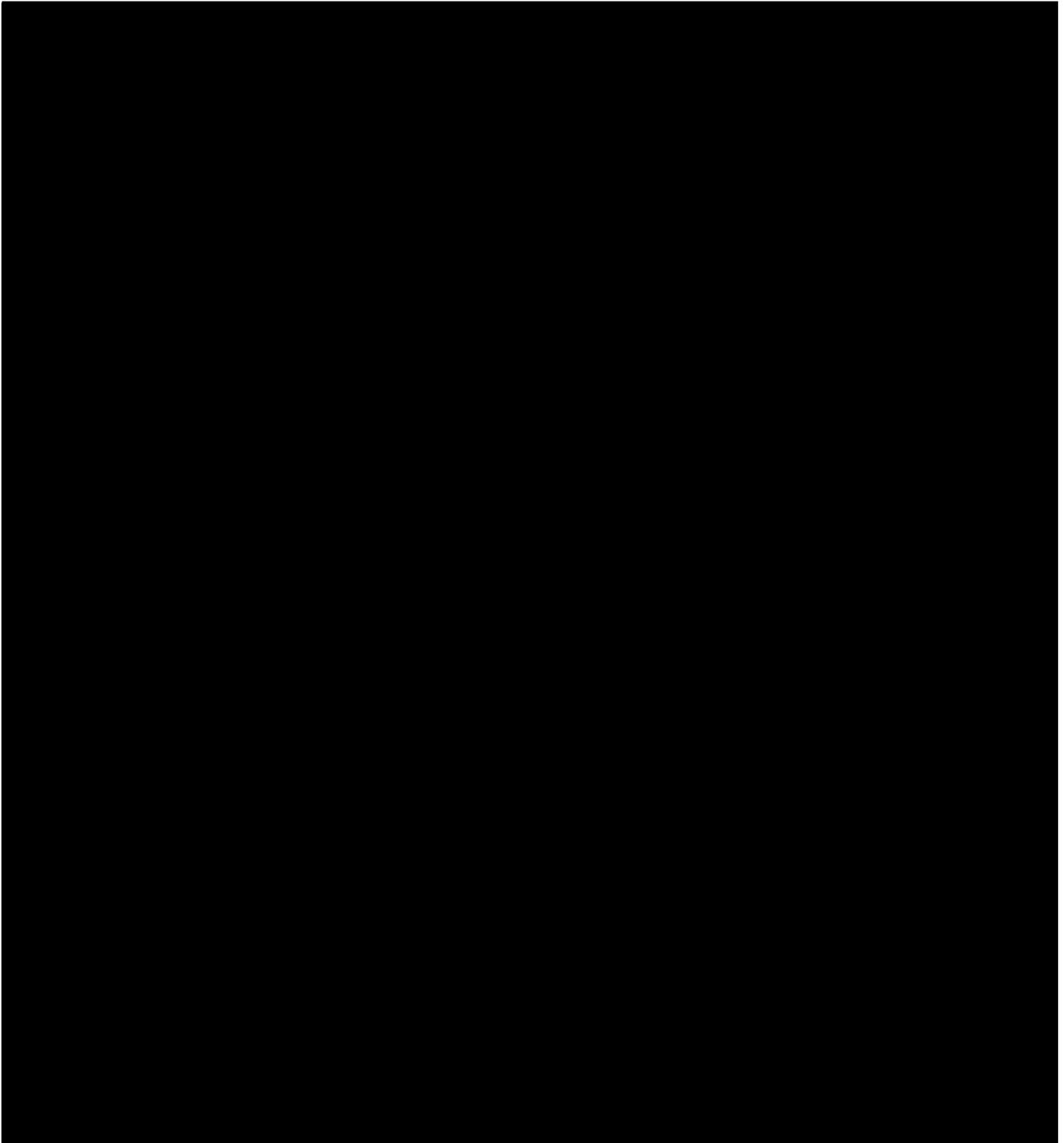
~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN



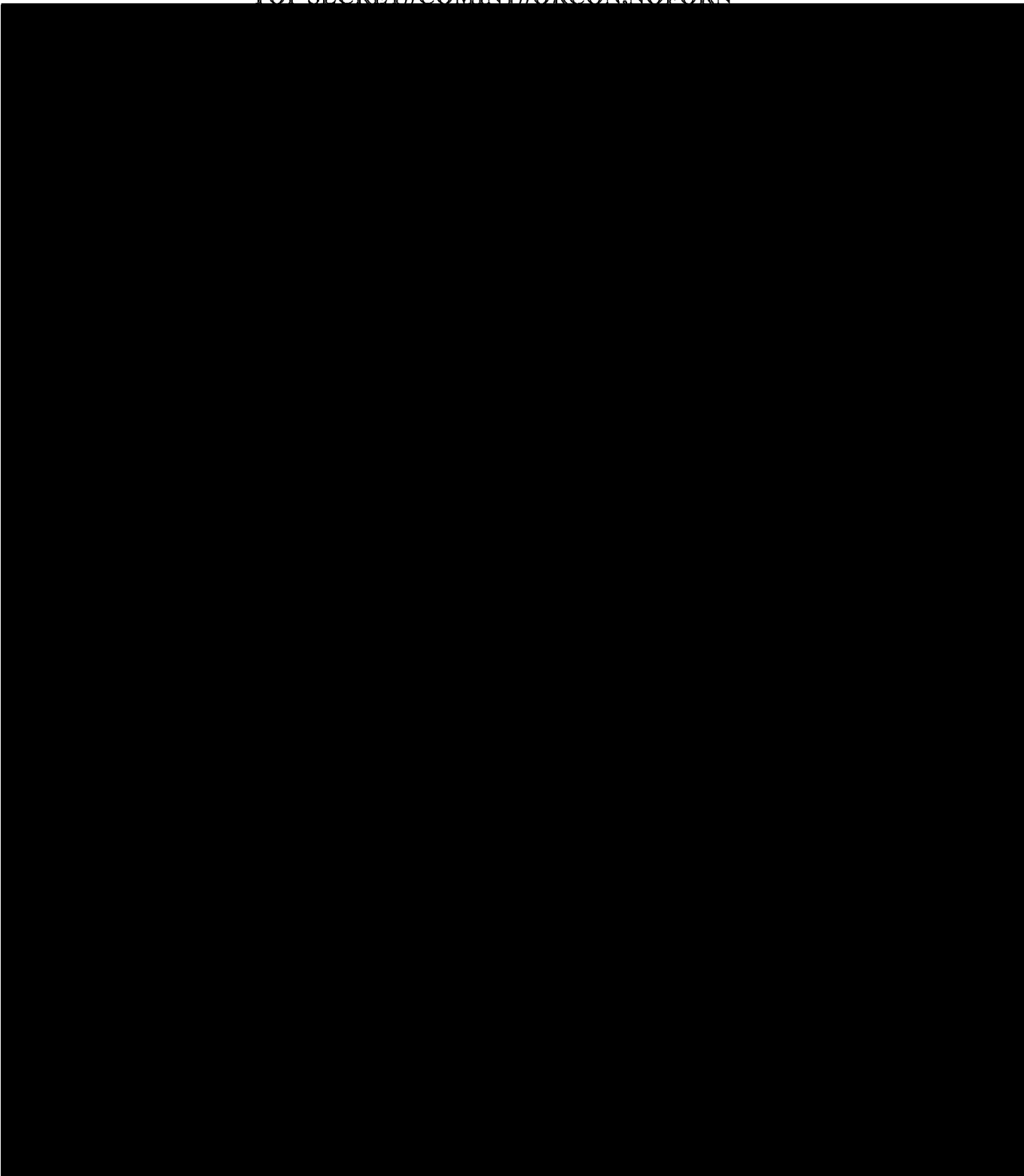
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



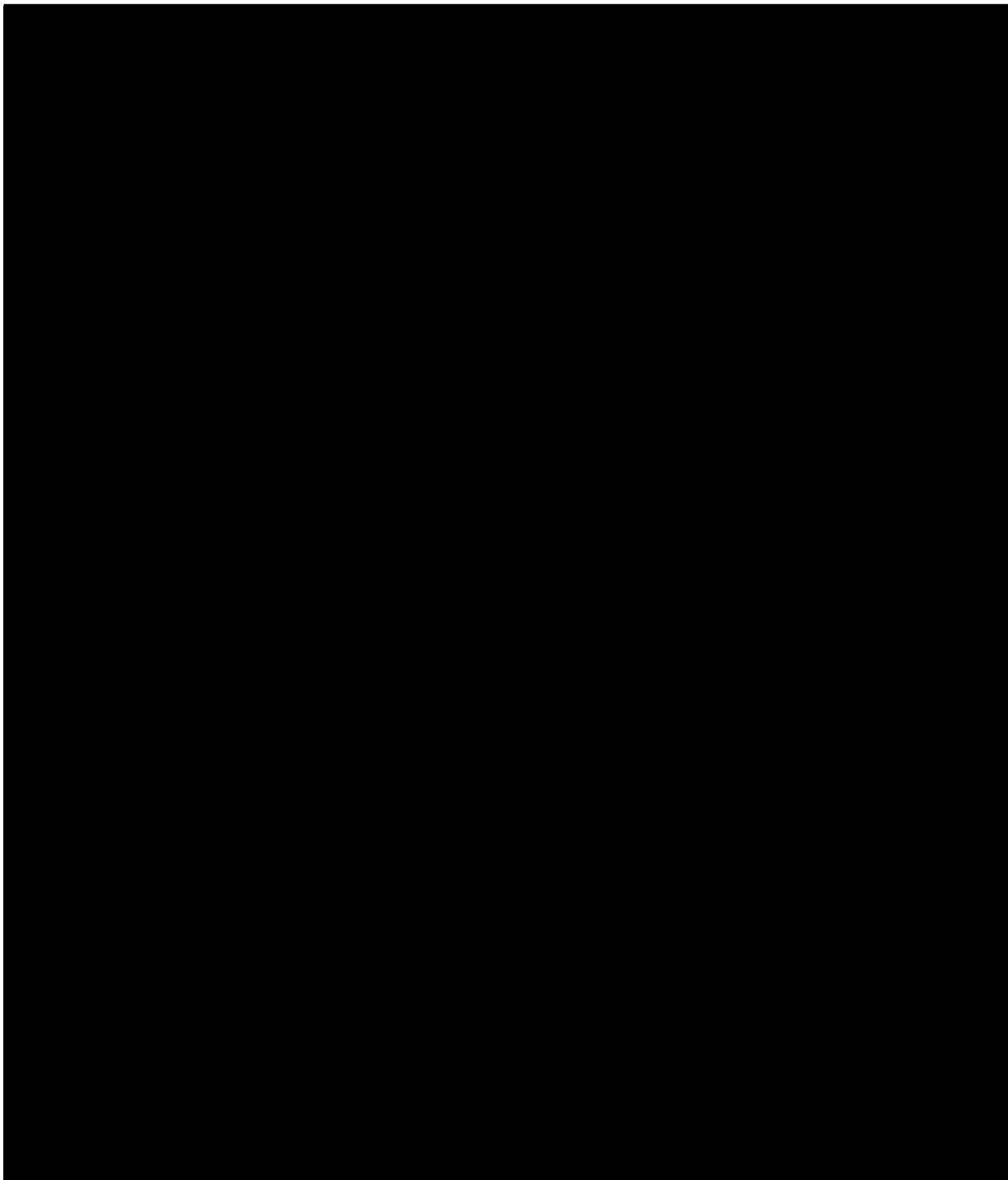
~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN



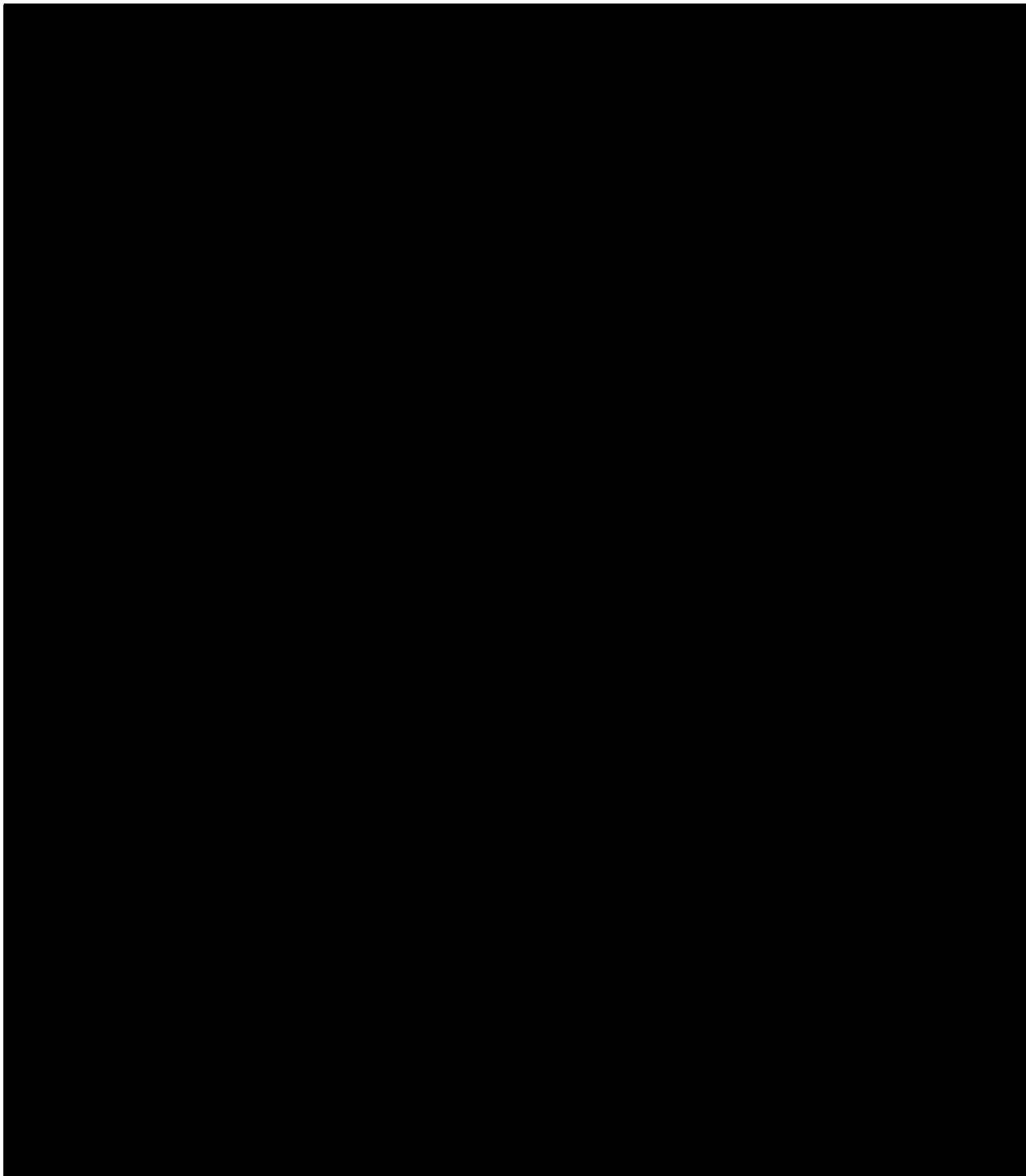
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



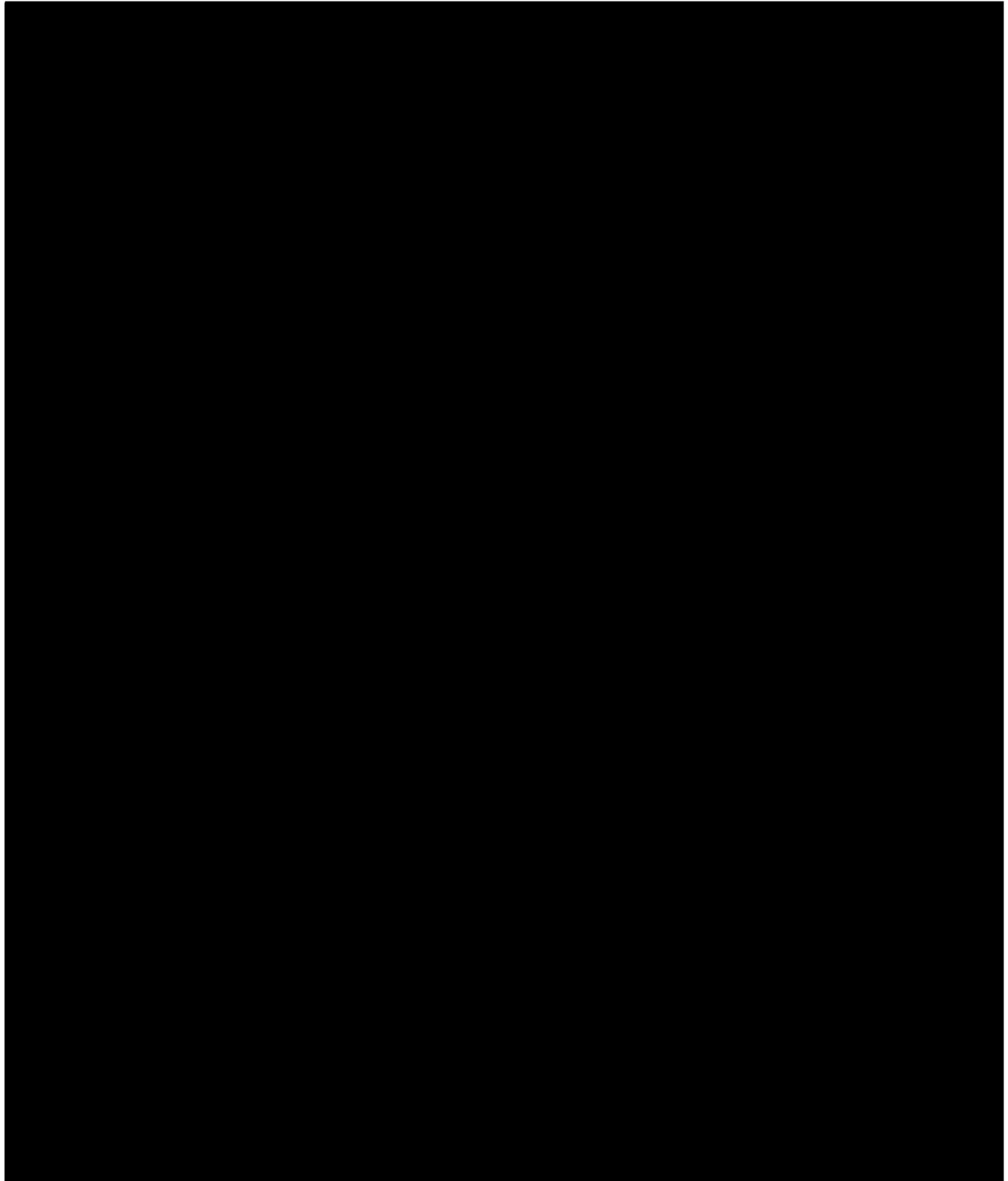
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



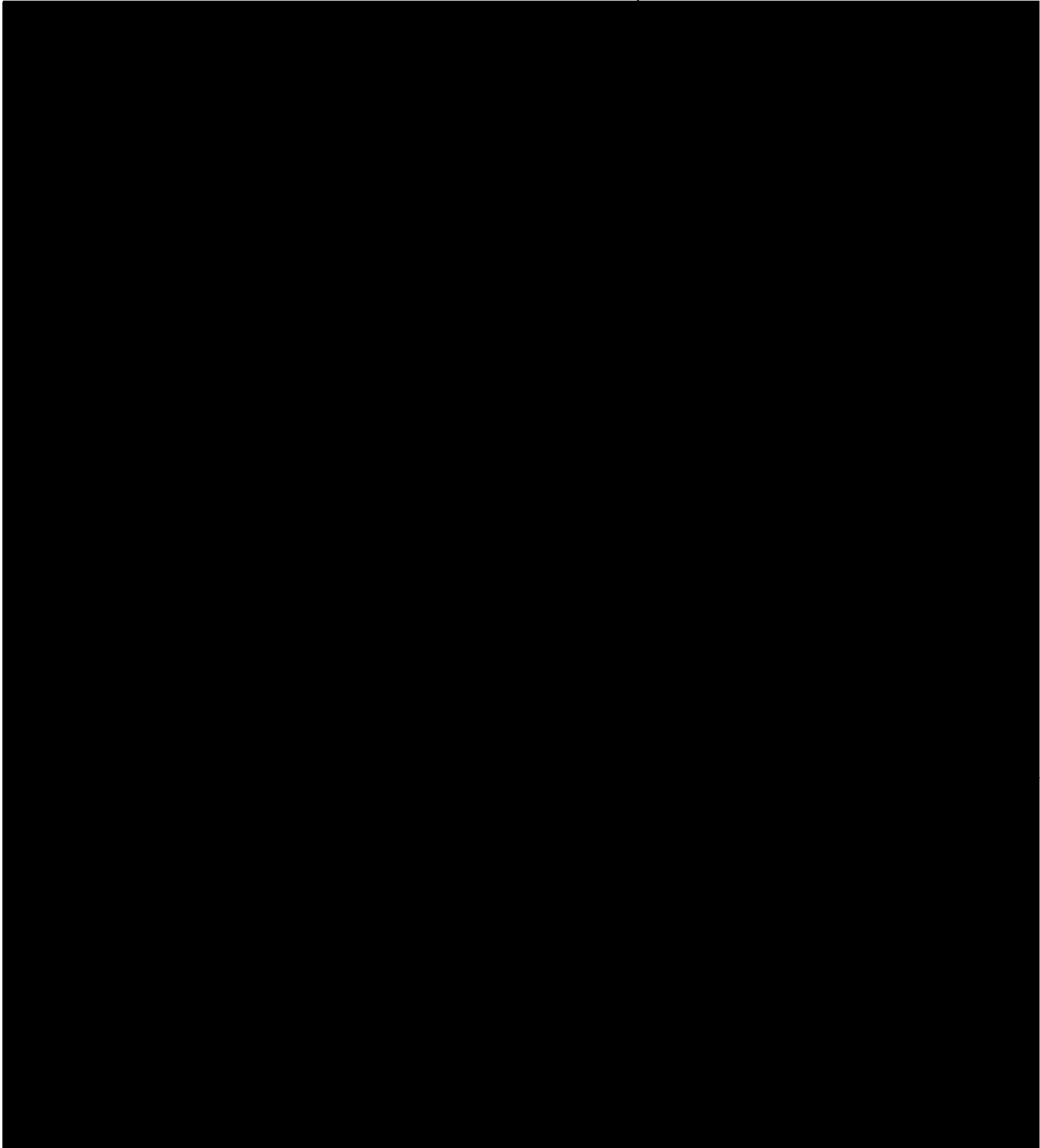
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



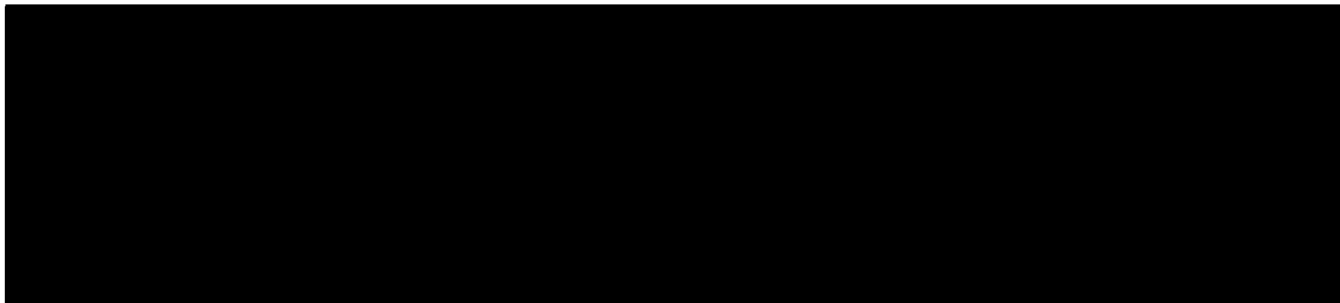
~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN

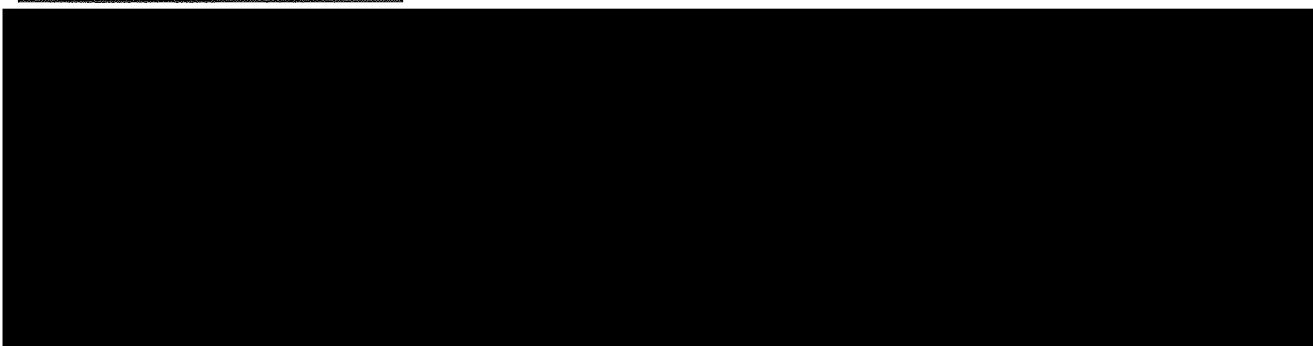


~~**TOP SECRET//COMINT//ORCON,NOFORN**~~

~~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)).

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

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

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:

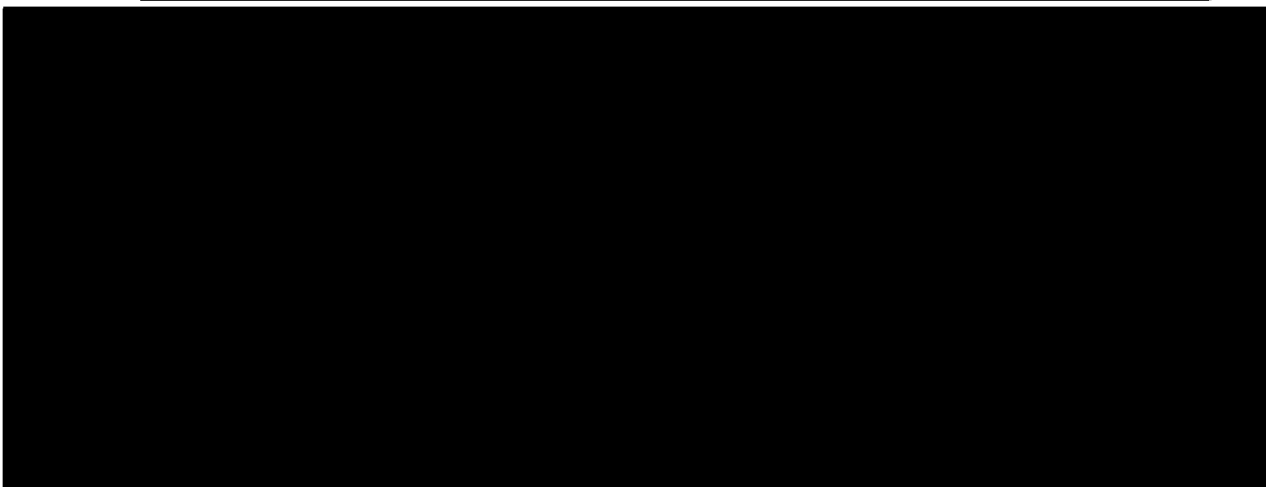
A government agency authorized to install and use a pen register or trap and trace device . . . shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing 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

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

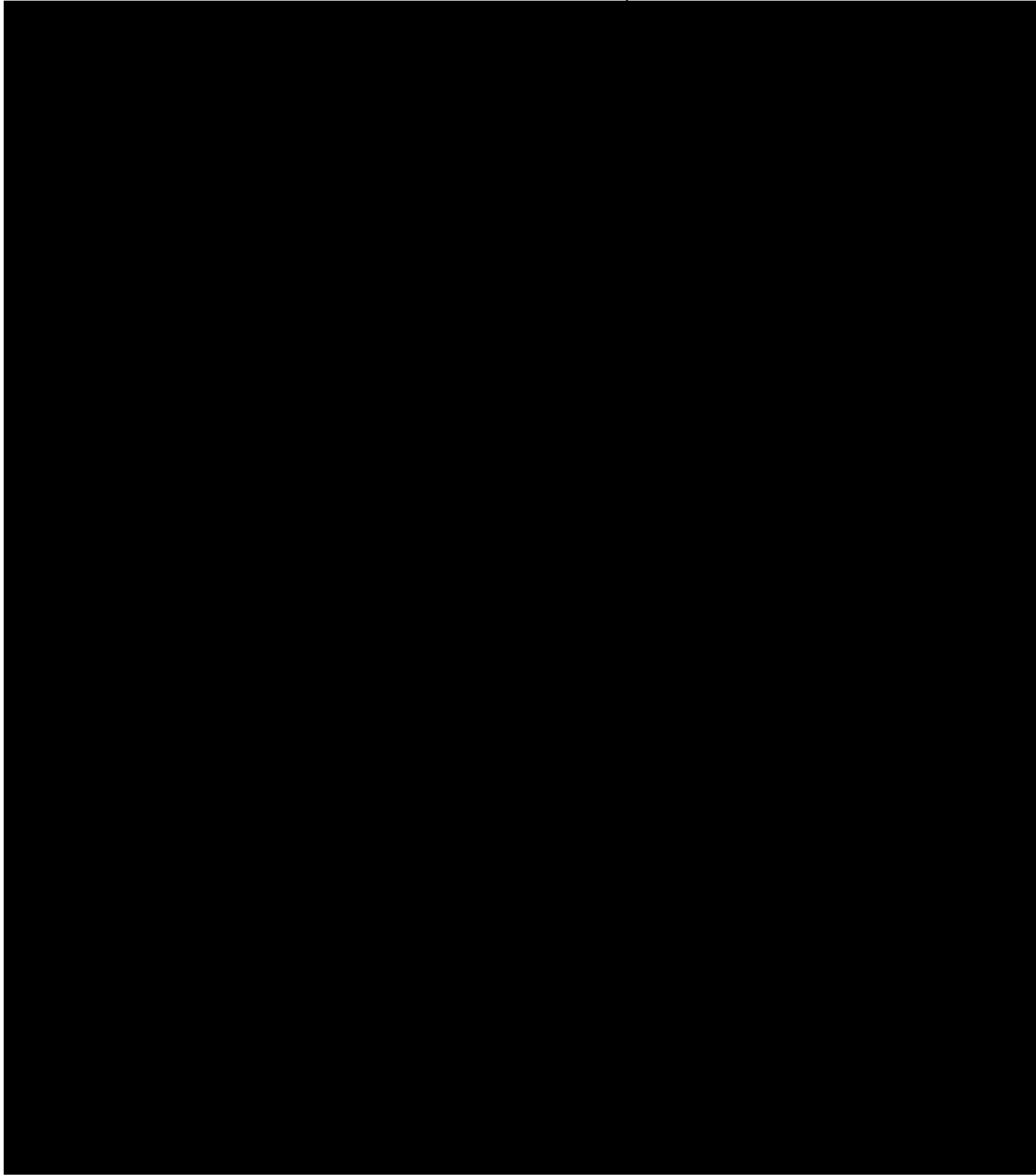
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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~~



~~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.

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

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

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.

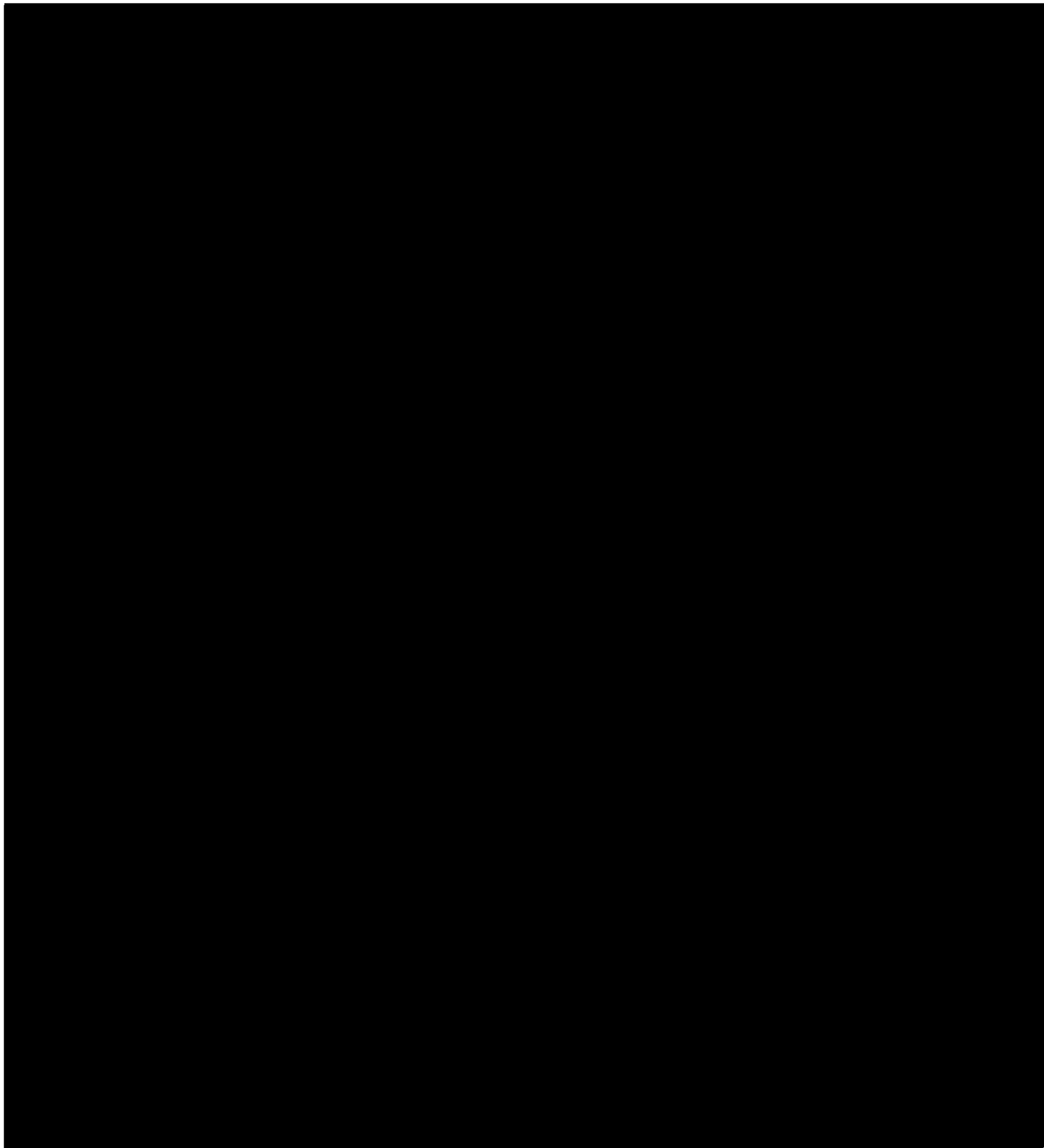
See [REDACTED] Response at 7.



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”).

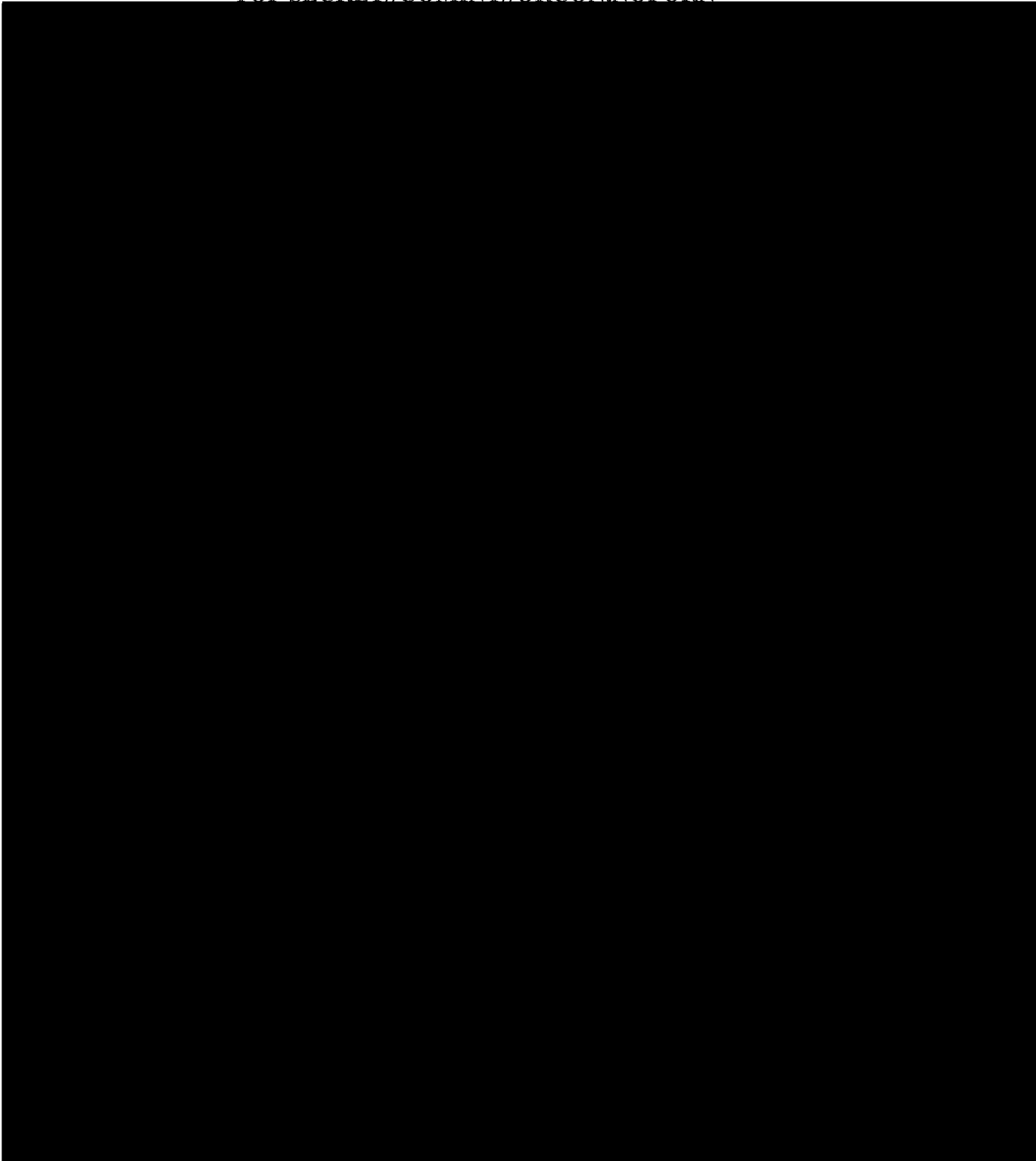
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



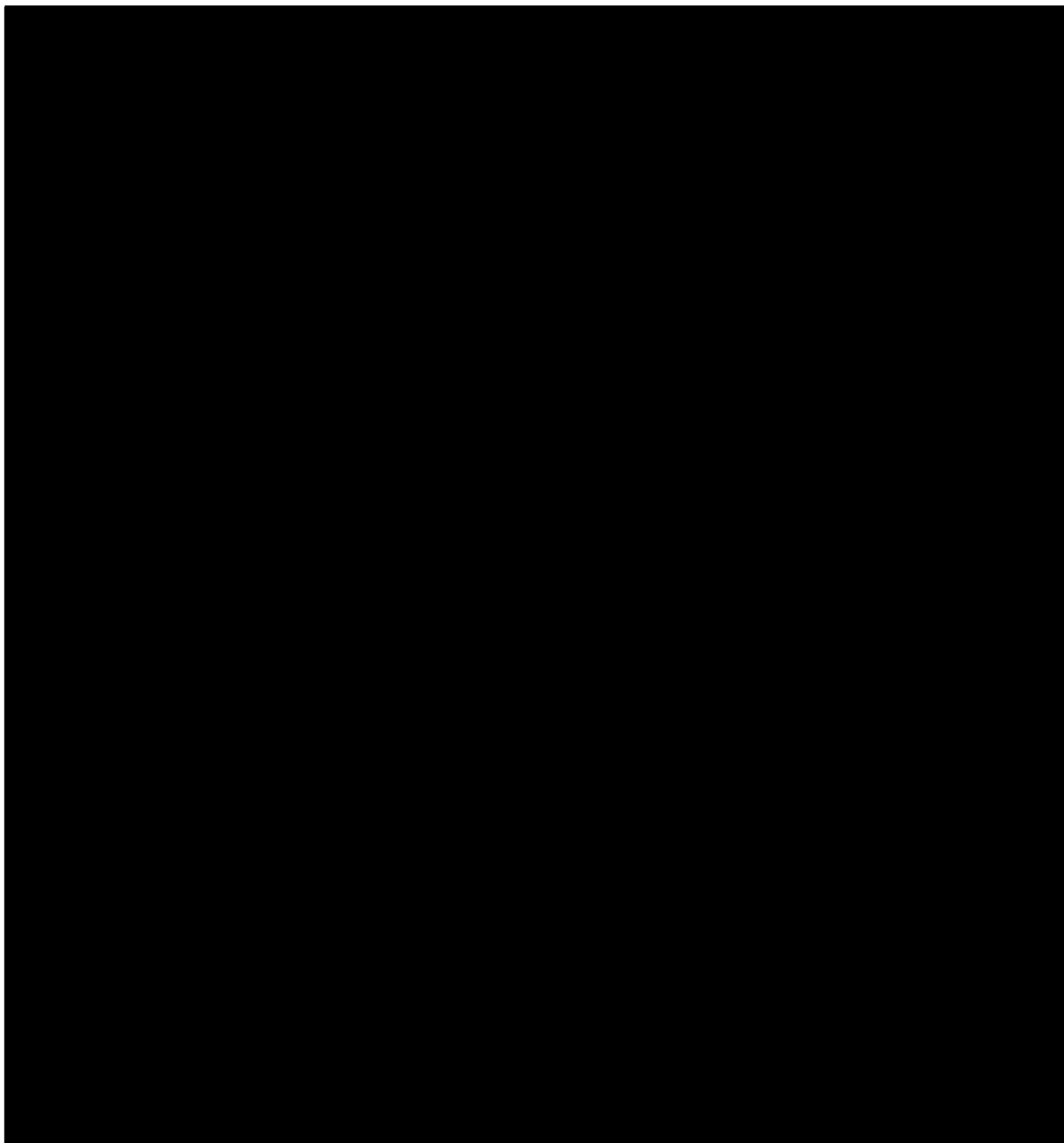
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



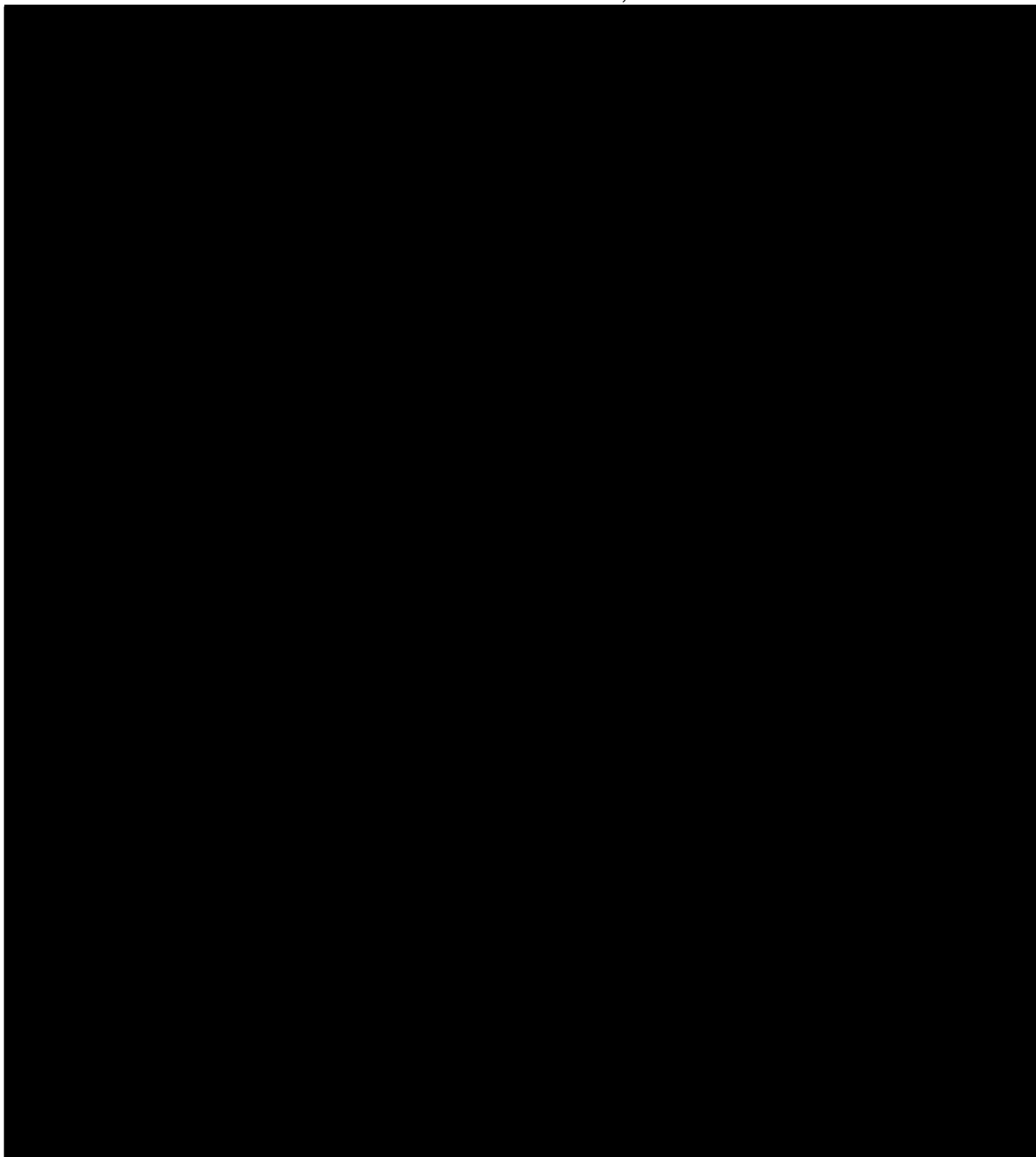
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



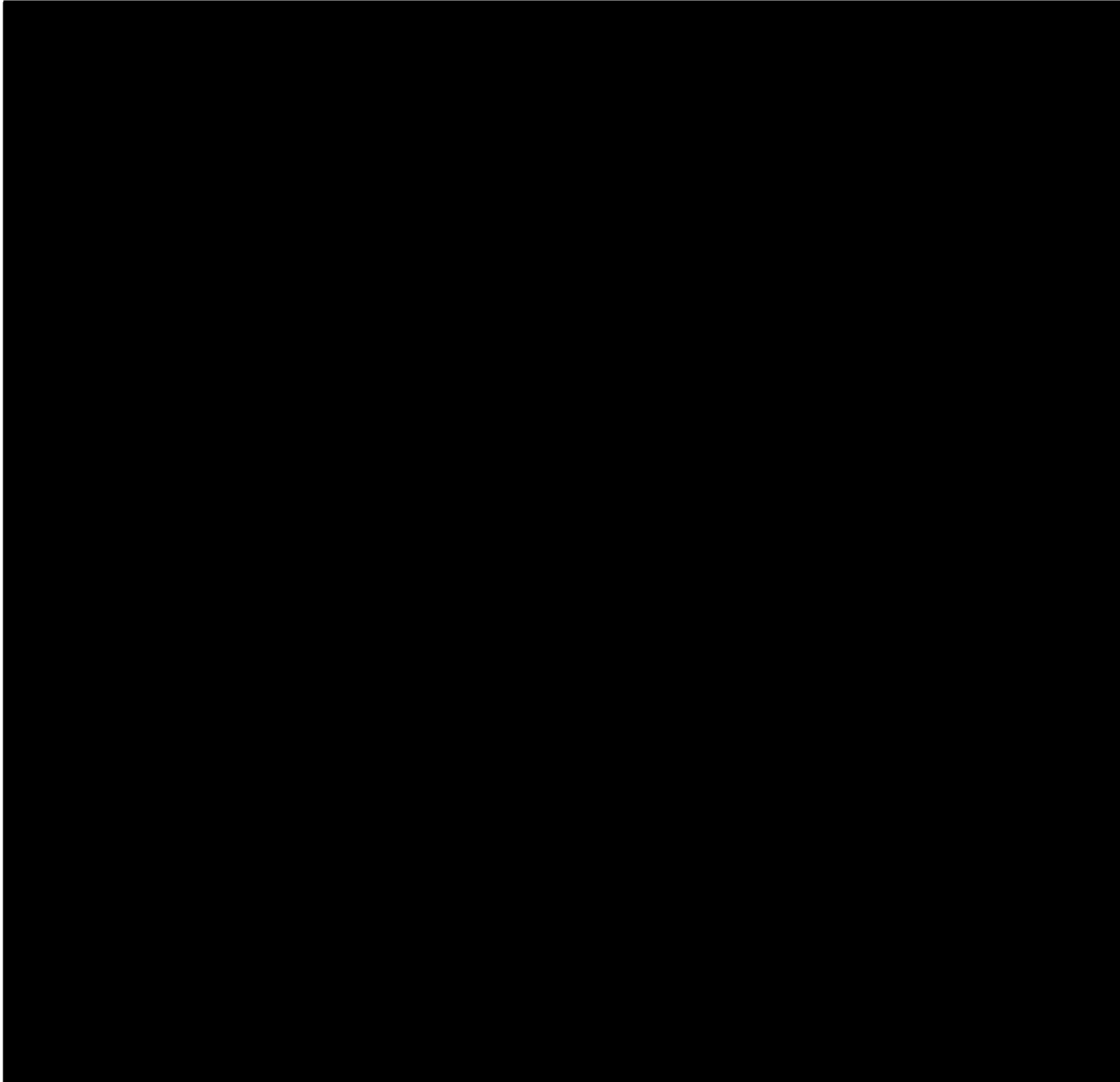
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



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

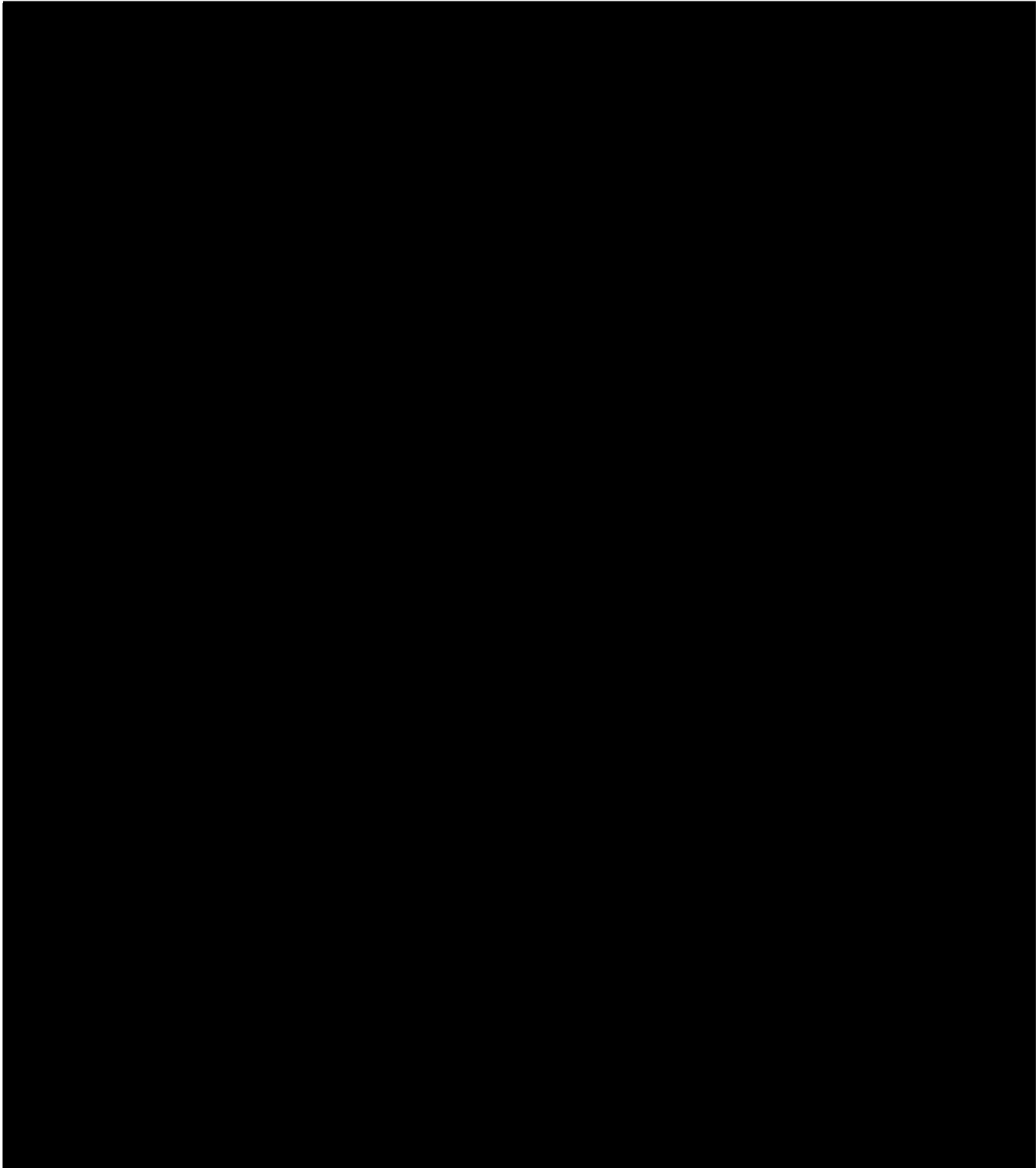
~~TOP SECRET//COMINT//ORCON,NOFORN~~



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).

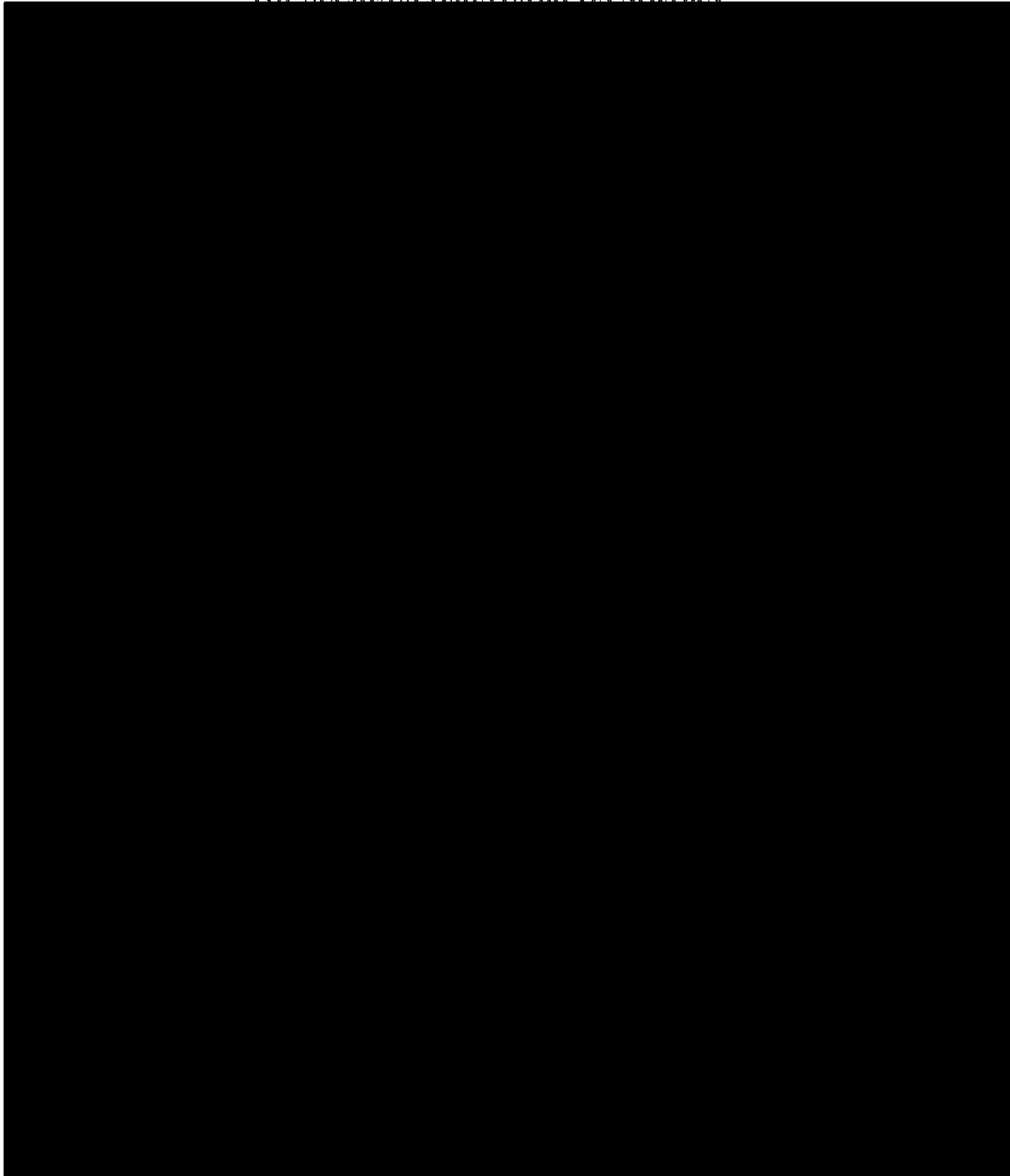
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



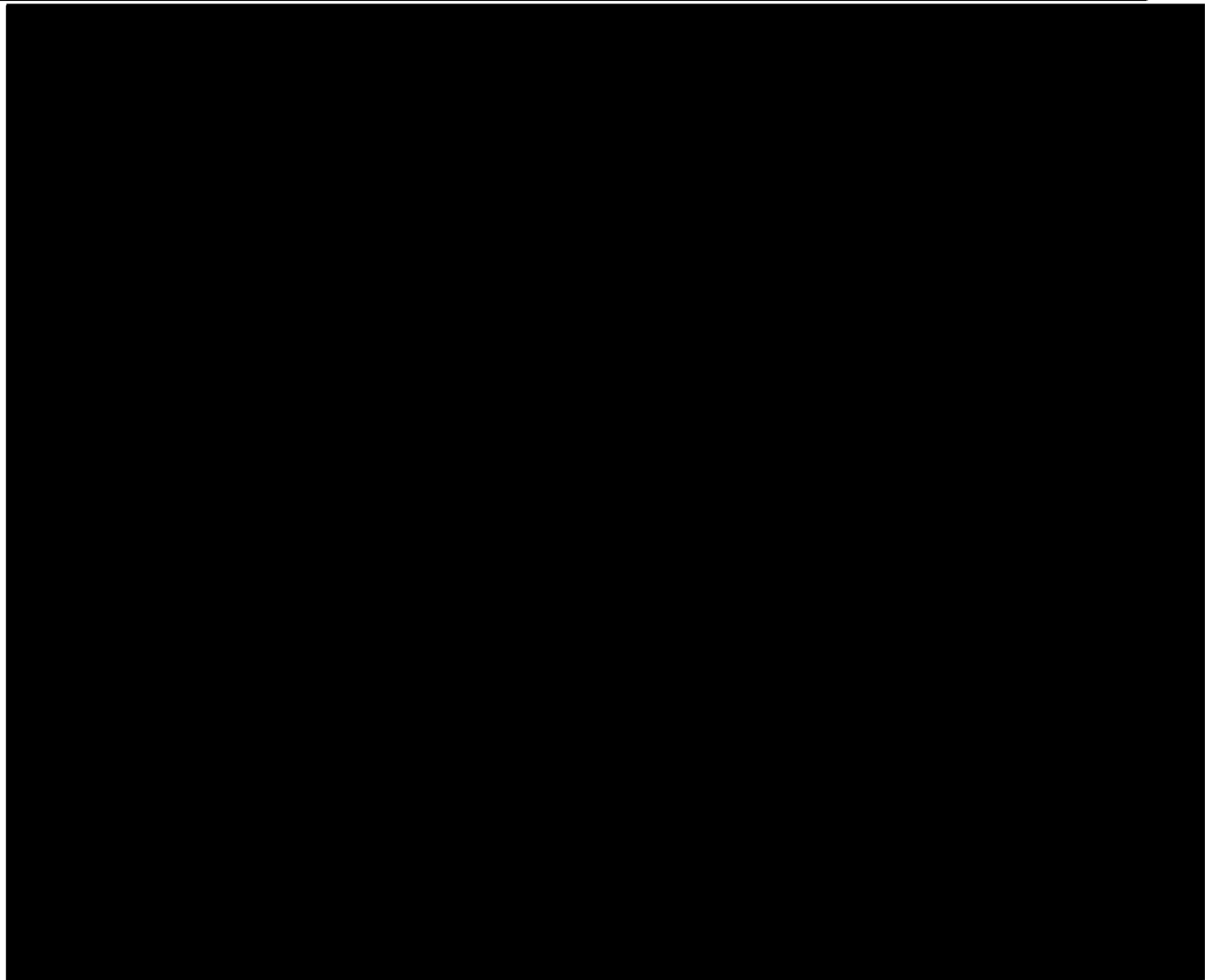
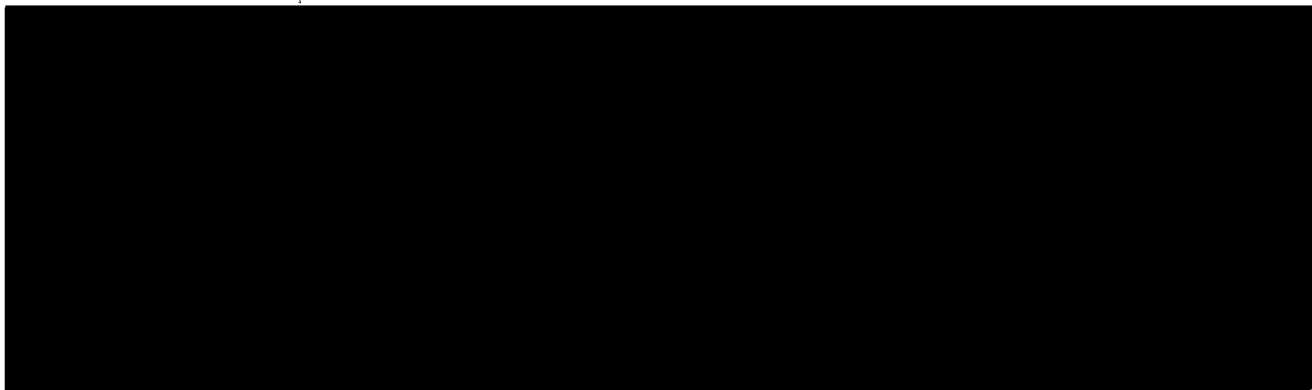
~~TOP SECRET//COMINT//ORCON,NOFORN~~

TOP SECRET//COMINT//ORCON,NOFORN



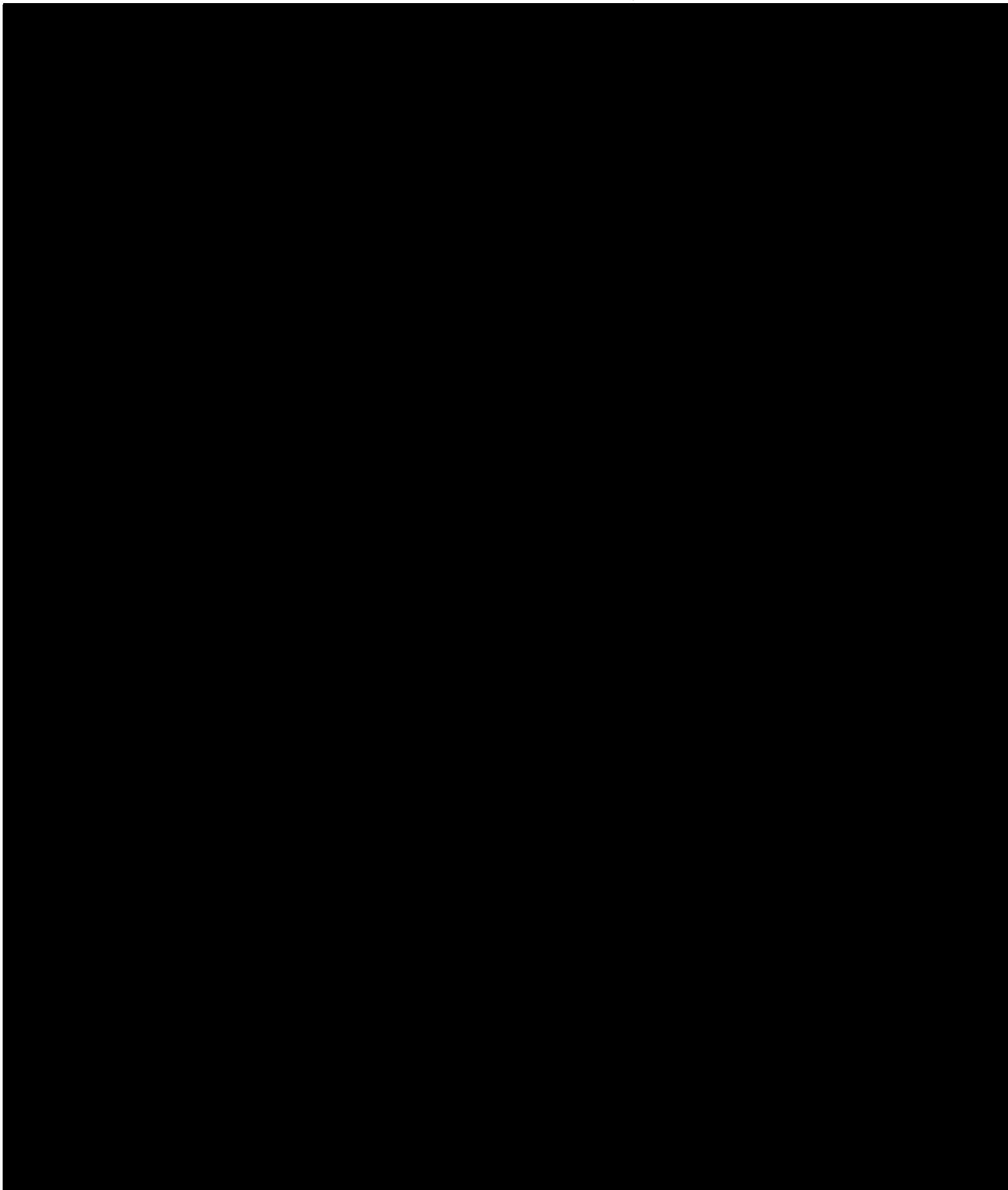
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



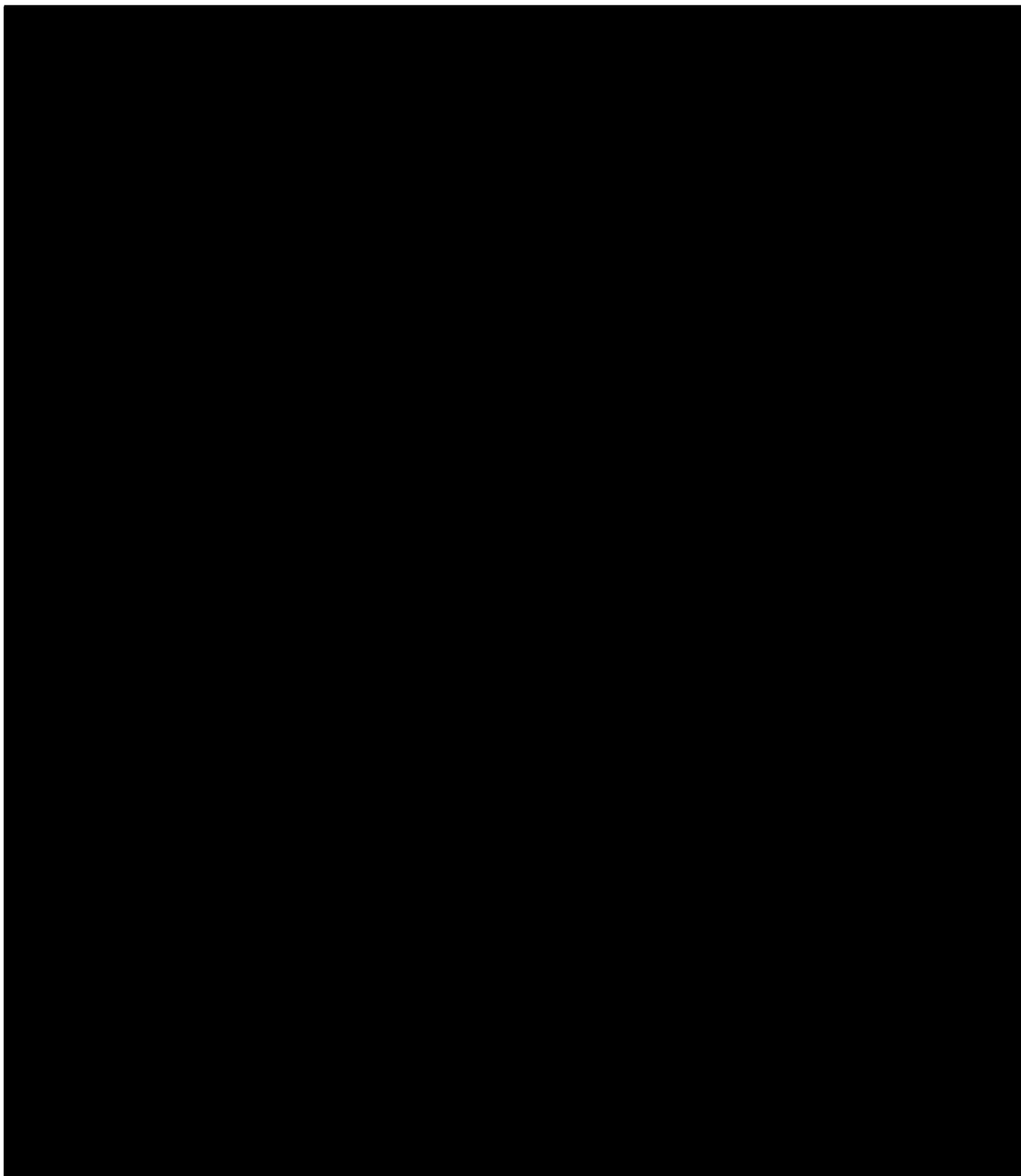
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



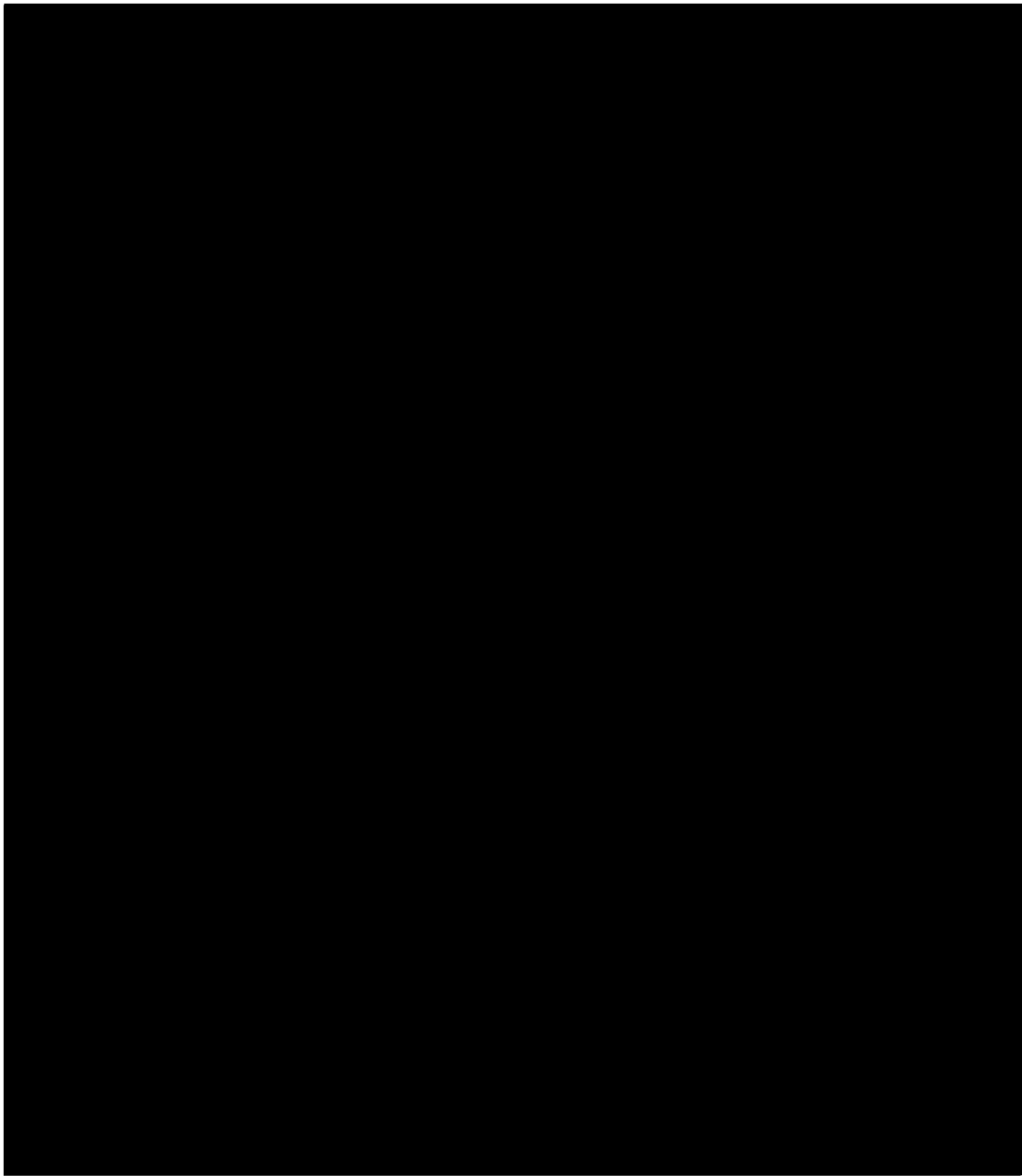
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



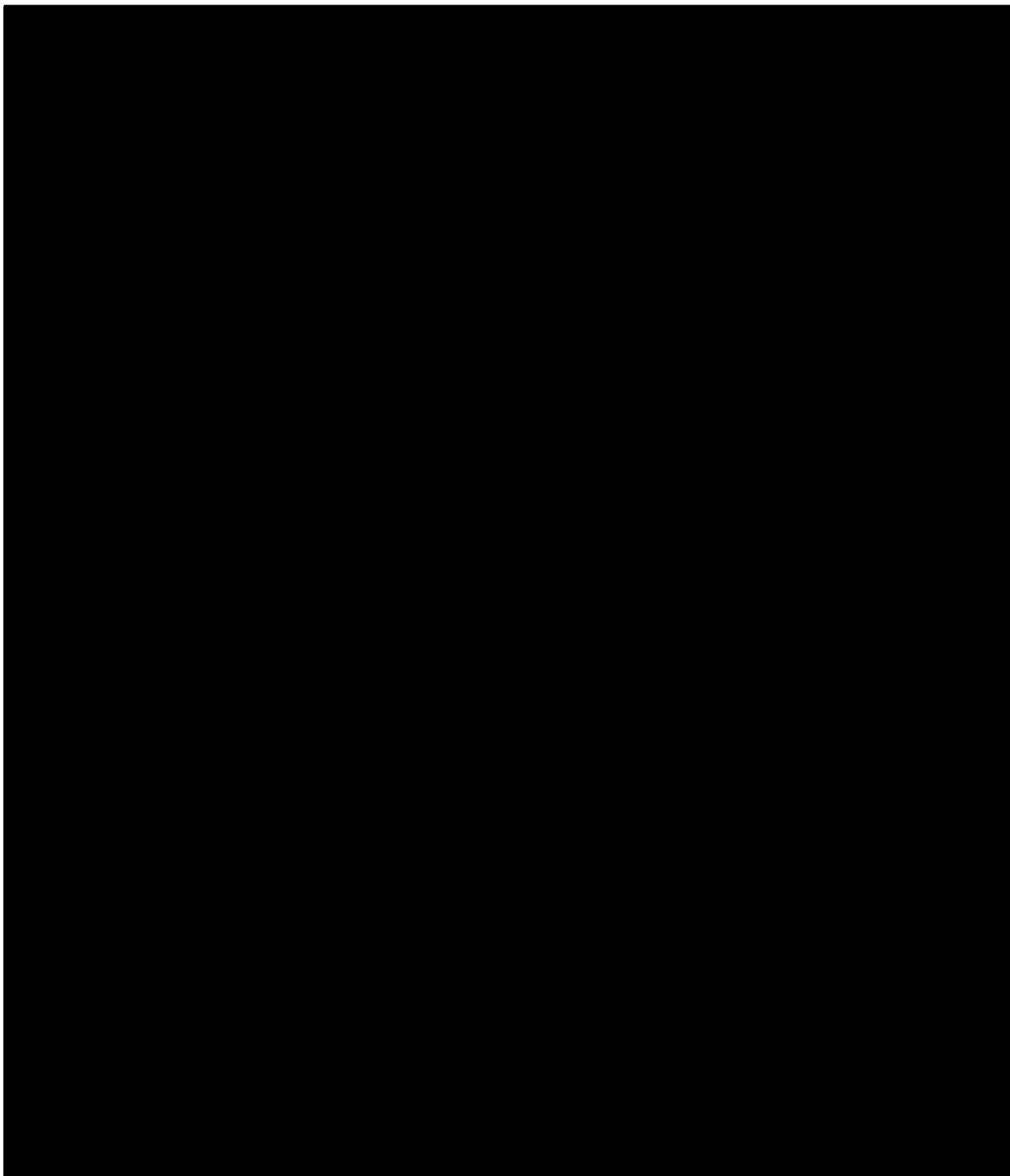
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



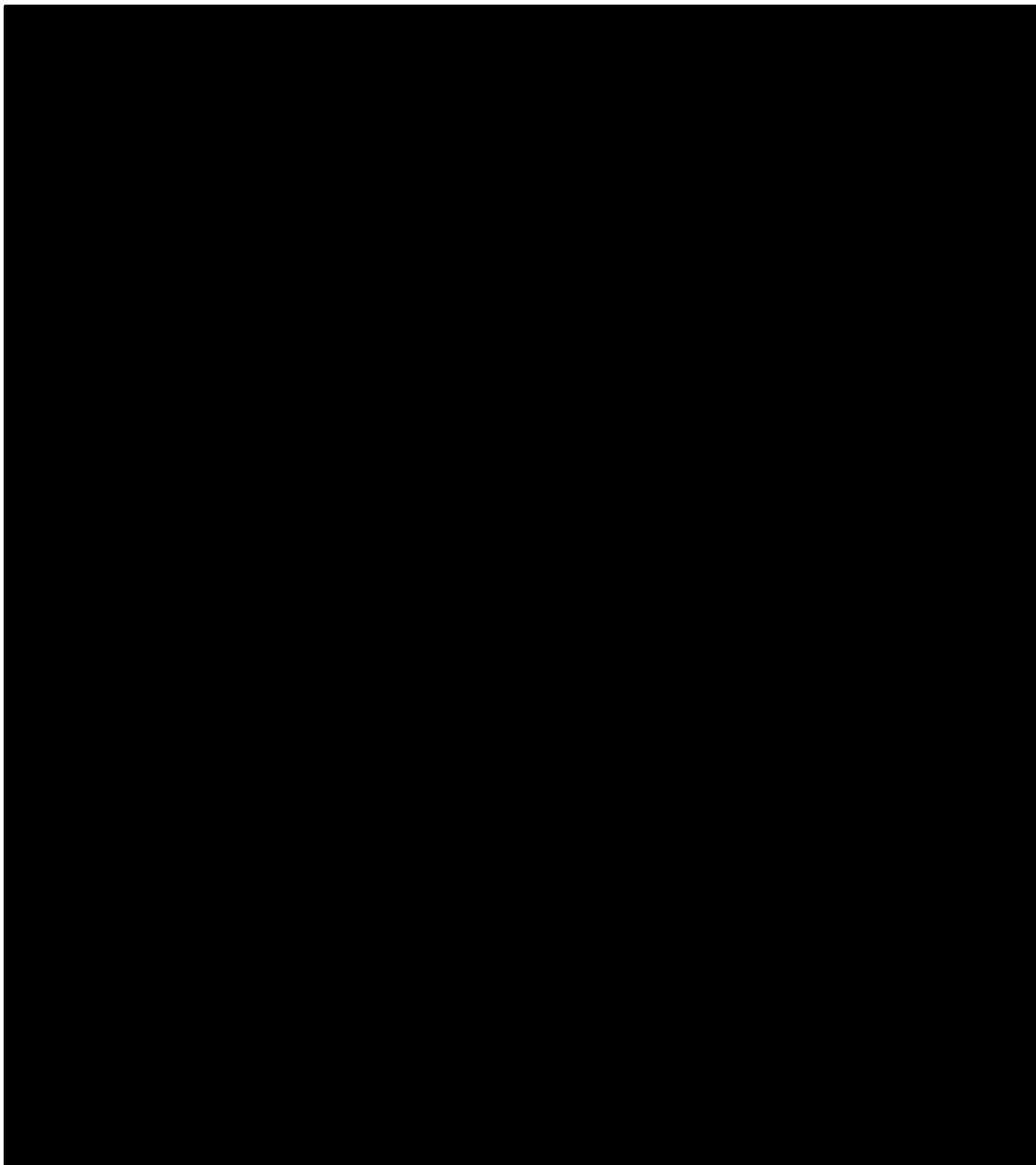
~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~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~~

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]

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

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

– 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]

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

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

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.

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

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

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.

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

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

██████████ 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.

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

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

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]

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

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



C. Specifications of the Order

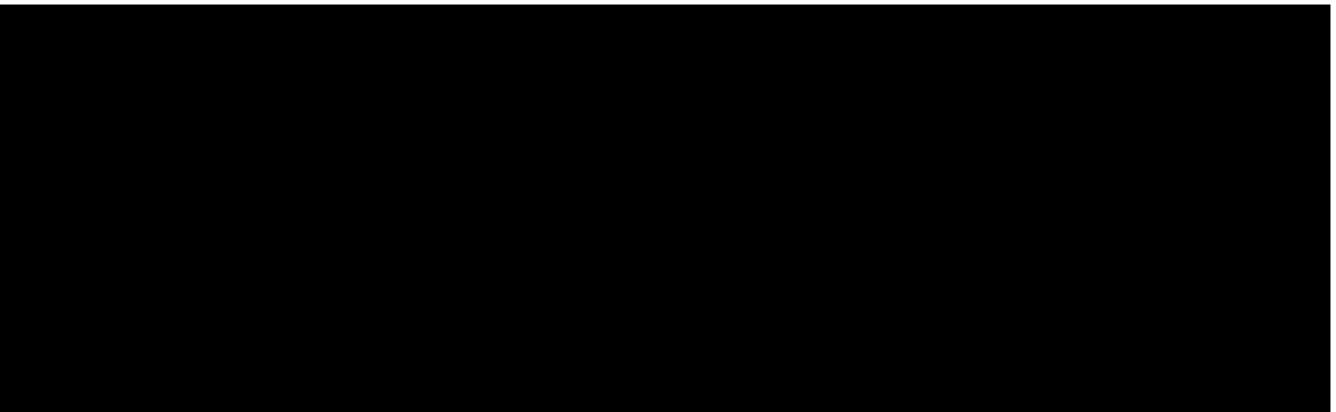
Section 1842(d)(2)(A) requires a PR/TT order to

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

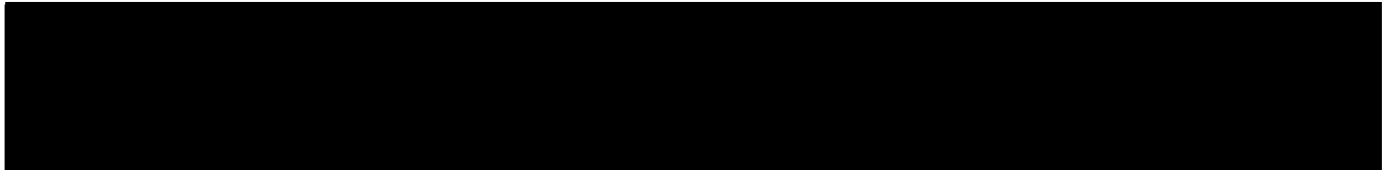
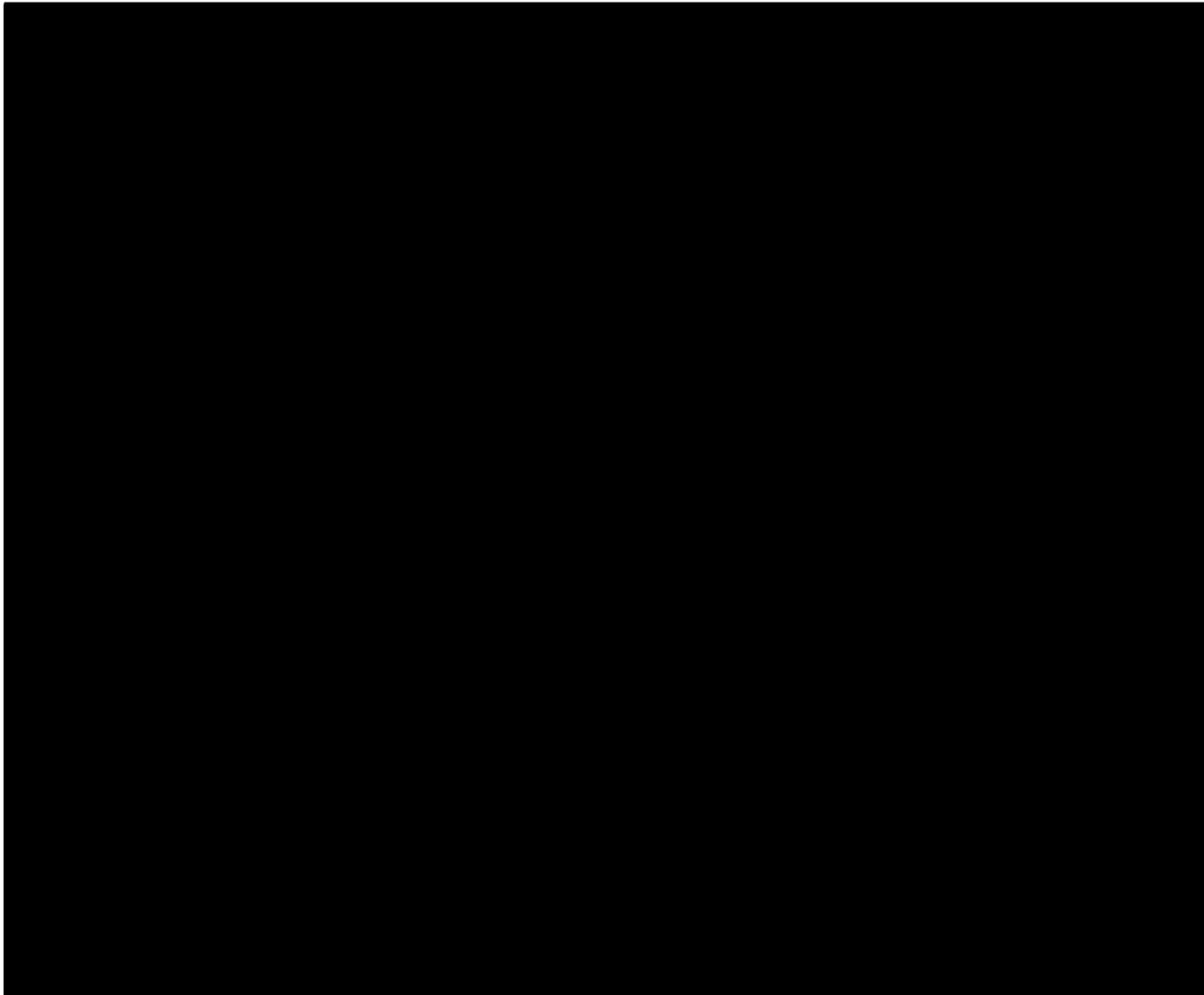
(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.^[65]



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

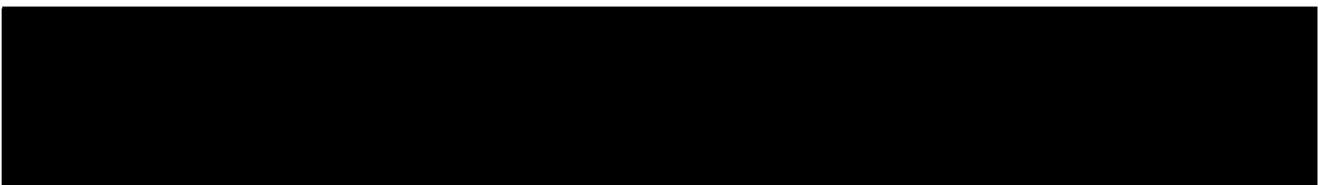
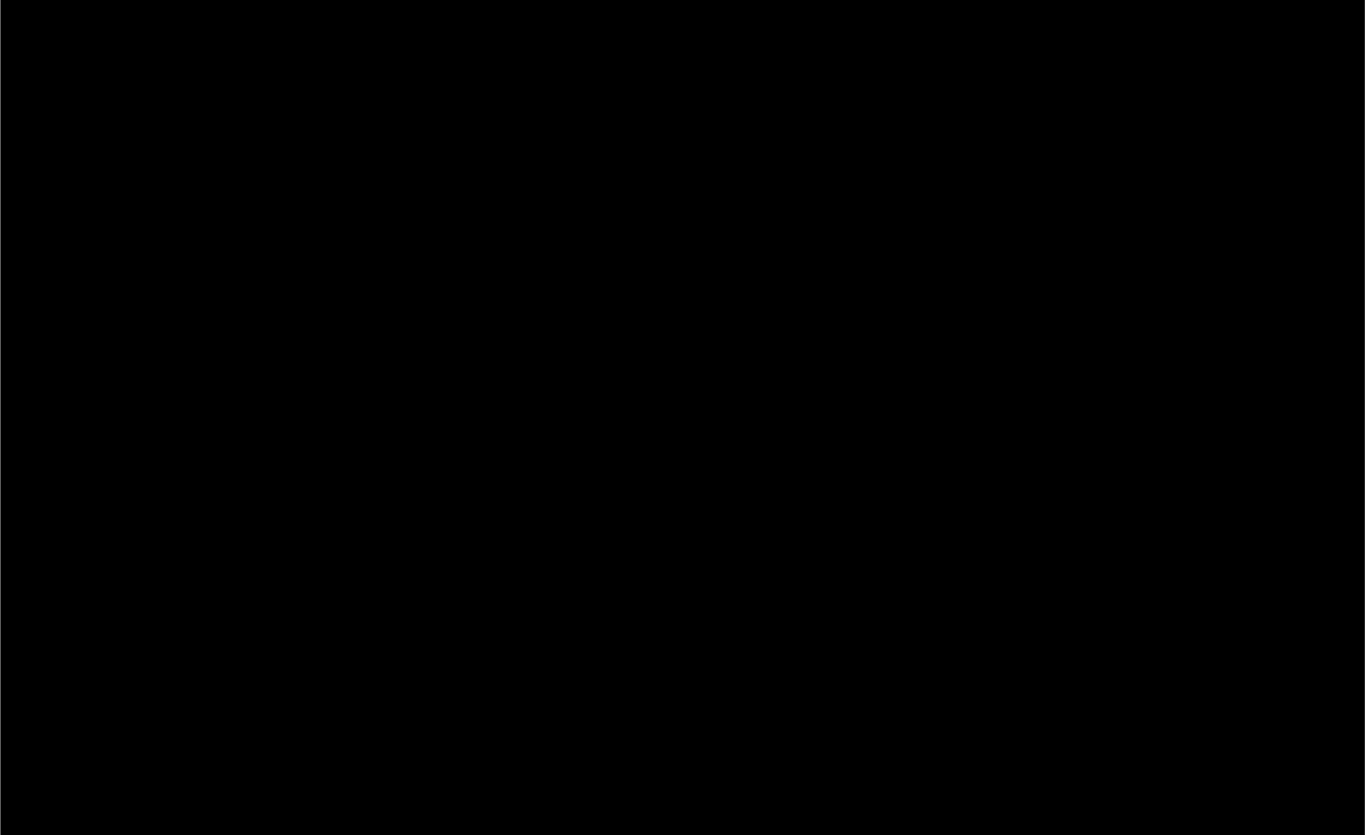
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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.



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

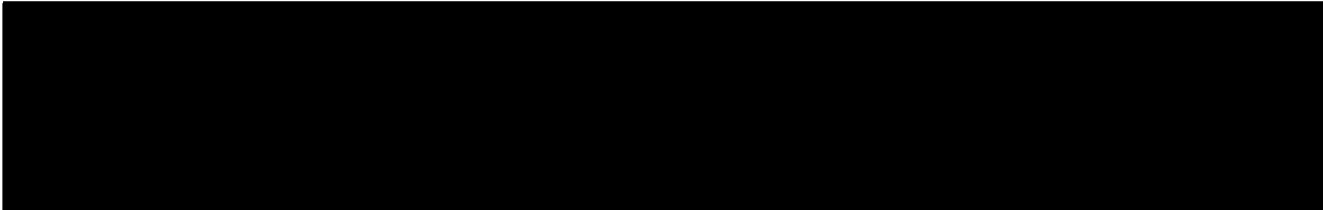
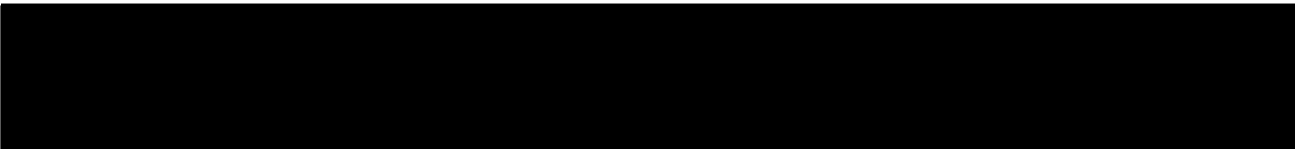
~~TOP SECRET//COMINT//ORCON,NOFORN~~



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

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

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



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

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

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

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/TT Metadata

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

[REDACTED]

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

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

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).

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

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

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

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

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

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...)

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

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

access by appropriately trained and authorized technical personnel was permitted under the [REDACTED] Order. See [REDACTED] 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 [REDACTED] Order. See [REDACTED] Alexander Decl. at 26-27; [REDACTED] 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. [REDACTED] 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)

[REDACTED] through such a query, the NSA technician could share the query results – i.e., the identifier and the fact that it is a [REDACTED] – 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 [REDACTED] Order identified one approving official in addition to the 22 officials listed here. See [REDACTED] Order at 8 (listing the Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate as one of the 23 approving officials).

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

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

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.

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

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

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 ██████████.

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

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

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

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

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

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]. 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.

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

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

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

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

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

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...)

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

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

The government's proposal contains one additional element that was not part of the framework approved by the Court in the ██████████ 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." ██████████ 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)

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

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

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

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.

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

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

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. ██████████

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

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

██████████ 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

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

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

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

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

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

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 ██████████ Application at 16. For the following reasons, the Court will grant the government's request in part and deny it in part.

A. The ██████████ 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 ██████████ it elected not to seek renewal of the authority granted in the ██████████ Order. The government was unable, before the expiration of that authority on ██████████, 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 ██████████ Order at 2-4. Accordingly, as an interim measure, Judge Walton entered an order on ██████████ directing the government not to access the information previously

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

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

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

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

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

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.").

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

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

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

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

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

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).

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

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

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...)”)

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

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

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.

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

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

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,

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

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

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]

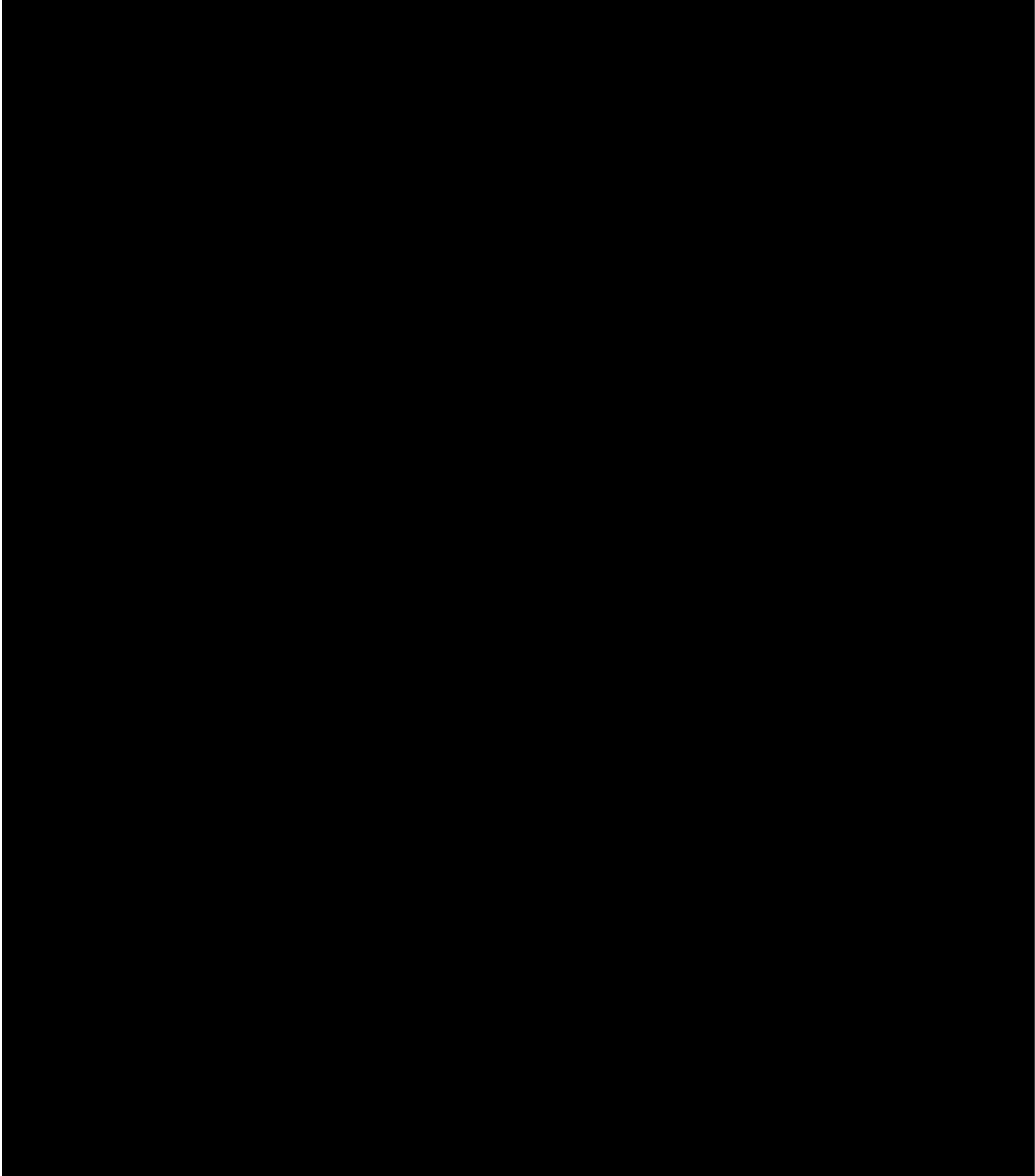
[REDACTED]

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]

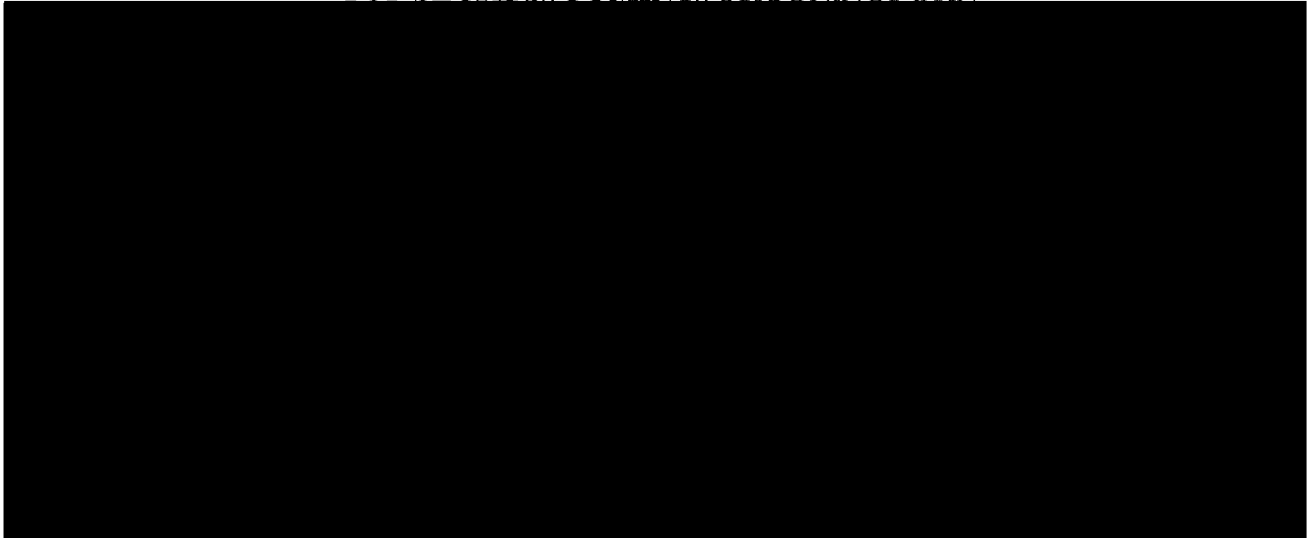
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



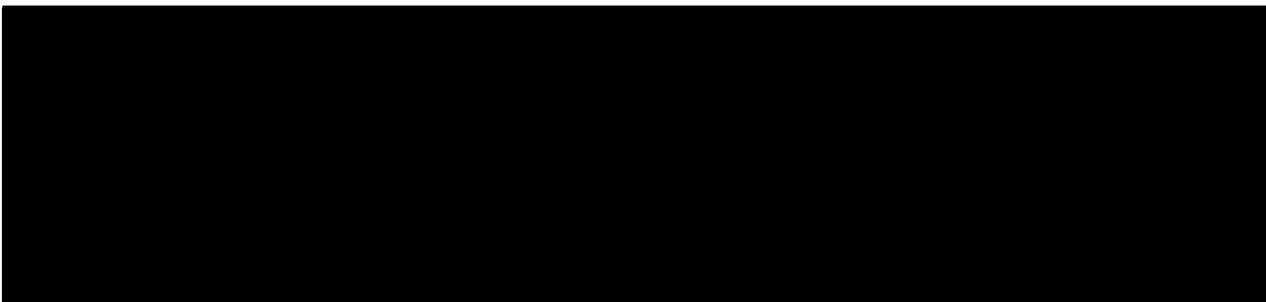
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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



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



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

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

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...)

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

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

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).

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

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

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

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

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

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.

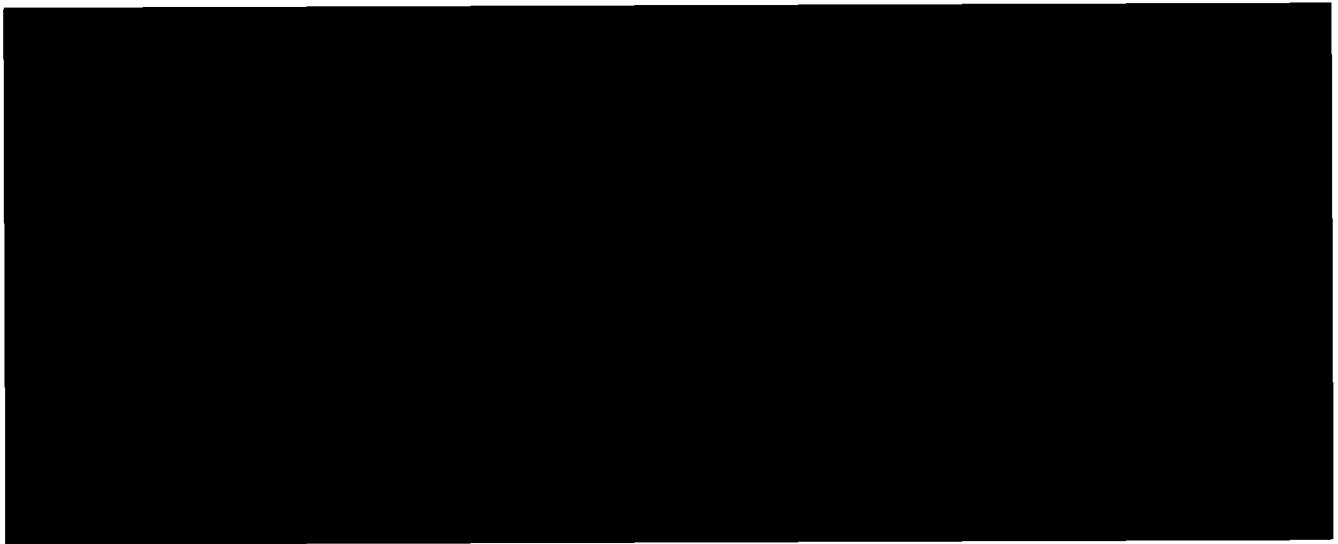
⁸⁸ Contrary to the government’s assertion, the imposition of restrictions on the use and dissemination of the data collected is not “unique” to the bulk PR/TT. Indeed, the Court restricts the government’s use of [REDACTED] See, e.g., Docket No. PR/TT [REDACTED] Primary Order at 4.

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

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

“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



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

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

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...)

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

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

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).

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

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

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

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

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

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.

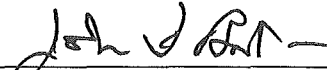
~~TOP SECRET//COMINT//ORCON,NOFORN~~

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

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 _____ E.T.
Date Time



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

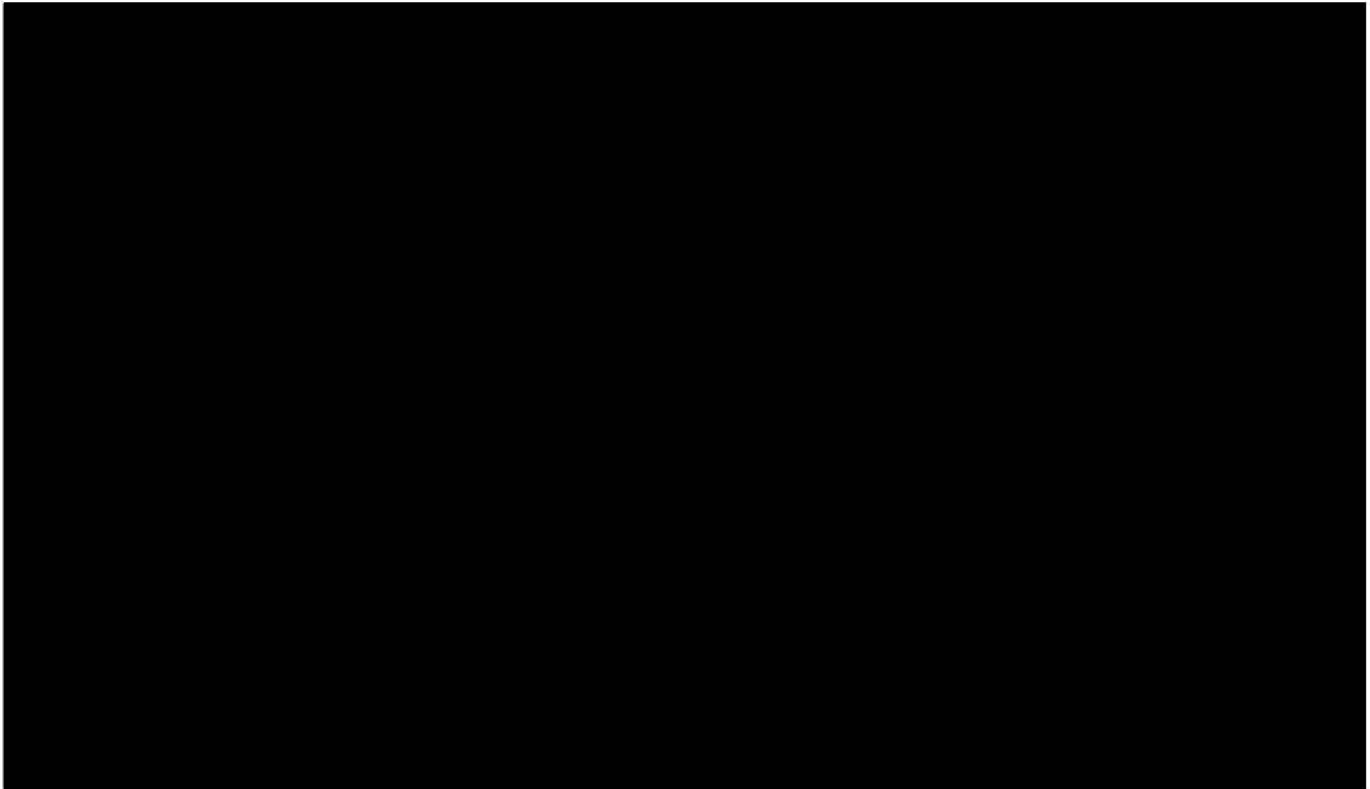
~~TOP SECRET//COMINT//ORCON,NOFORN~~



EXHIBIT B

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

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



MEMORANDUM OPINION

These matters are before the Foreign Intelligence Surveillance Court (“FISC” or “Court”) on: (1) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications

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

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

[REDACTED], which was filed on April 20, 2011; (2) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was filed on April 22, 2011; and (3) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was also filed on April 22, 2011.¹

Through these submissions, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA” or the “Act”), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth below, the government’s requests for approval are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the “upstream collection” of Internet transactions containing multiple communications – is, in some respects, deficient on statutory and constitutional grounds.

¹ For ease of reference, the Court will refer to these three filings collectively as the “April 2011 Submissions.”

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

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

I. BACKGROUND

A. The Certifications and Amendments

The April 2011 Submissions include DNI/AG 702(g) Certification [REDACTED]

[REDACTED], all of which were executed by the Attorney General and the Director of National Intelligence (“DNI”) pursuant to Section 702. [REDACTED] previous certifications have been submitted by the government and approved by the Court pursuant to Section 702. [REDACTED]

[REDACTED] (collectively, the “Prior 702 Dockets”). Each of the April 2011 Submissions also includes supporting affidavits by the Director or Acting 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 NSA and FBI respectively; and three sets of minimization procedures, for use by NSA, FBI, and CIA, respectively.²

Like the acquisitions approved by the Court in the eight Prior 702 Dockets, collection

² The targeting and minimization procedures accompanying Certification [REDACTED] are identical to those accompanying [REDACTED]. As discussed below, the NSA targeting procedures and FBI minimization procedures accompanying Certifications [REDACTED] also are identical to the NSA targeting procedures and FBI minimization procedures that were submitted by the government and approved by the Court for use in connection with Certifications [REDACTED]. The FBI targeting procedures and the NSA and CIA minimization procedures that accompany the April 2011 Submissions differ in several respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications [REDACTED].

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

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

under Certifications [REDACTED] is limited to “the targeting of non-United States persons reasonably believed to be located outside the United States.” Certification [REDACTED]

[REDACTED]

The April 2011 Submissions also include amendments to certifications that have been submitted by the government and approved by the Court in the Prior 702 Dockets. The amendments, which have been authorized by the Attorney General and the DNI, provide that information collected under the certifications in the Prior 702 Dockets will, effective upon the Court’s approval of Certifications [REDACTED], be handled subject to the same

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

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

revised NSA and CIA minimization procedures that have been submitted for use in connection with Certifications [REDACTED]

[REDACTED].

B. The May 2 “Clarification” Letter

On May 2, 2011, the government filed with the Court a letter pursuant to FISC Rule 13(a) titled “Clarification of National Security Agency’s Upstream Collection Pursuant to Section 702 of FISA” (“May 2 Letter”). The May 2 Letter disclosed to the Court for the first time that NSA’s “upstream collection”³ of Internet communications includes the acquisition of entire

“transaction[s]” (b) (1) (A) [REDACTED]

[REDACTED]⁴ According to the May 2 Letter, such transactions may contain data that is wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection. See id. at 2-3. The letter noted that NSA uses [REDACTED] to ensure that “the person from whom it seeks to obtain foreign intelligence information is located overseas,” but suggested that the government might lack confidence in the effectiveness of such measures as applied to Internet transactions. See id. at 3 (citation omitted).

³ The term “upstream collection” refers to NSA’s interception of Internet communications as they transit (b) (1) (A) [REDACTED], rather than to acquisitions directly from Internet service providers such as [REDACTED]. [REDACTED]

⁴ The concept of “Internet transactions” is discussed more fully below. See infra, pages 27-41 and note 23.

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

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

C. The Government's First Motion for Extensions of Time

On May 5, 2011, the government filed a motion seeking to extend until July 22, 2011, the 30-day periods in which the Court must otherwise complete its review of Certifications [REDACTED], and the amendments to the certifications in the Prior 702 Dockets. See Motion for an Order Extending Time Limit Pursuant to 50 U.S.C. § 1881a(j)(2) at 1 (“May Motion”). The period for FISC review of Certification [REDACTED] was then set to expire on May 20, 2011, and the period for review of the other pending certifications and amendments was set to expire on May 22, 2011. Id. at 6.⁵

The government noted in the May Motion that its efforts to address the issues raised in the May 2 Letter were still ongoing and that it intended to “supplement the record . . . in a manner that will aid the Court in its review” of the certifications and amendments and in making the determinations required under Section 702. Id. at 7. According to the May Motion, however, the government would “not be in a position to supplement the record until after the statutory time limits for such review have expired.” Id. The government further asserted that granting the requested extension of time would be consistent with national security, because, by operation of

⁵ 50 U.S.C. § 1881a(i)(1)(B) requires the Court to complete its review of the certification and accompanying targeting and minimization procedures and issue an order under subsection 1881a(i)(3) not later than 30 days after the date on which the certification and procedures are submitted. Pursuant to subsection 1881a(i)(1)(C), the same time limit applies to review of an amended certification or amended procedures. However, 50 U.S.C. § 1881a(j)(2) permits the Court, by order for reasons stated, to extend “as necessary for good cause in a manner consistent with national security,” the time limit for the Court to complete its review and issue an order under Section 1881a(i)(3).

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

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

statute, the government's acquisition of foreign intelligence information under Certifications

██████████ could continue pending completion of the Court's review. See id. at 9-10.

On May 9, 2011, the Court entered orders granting the government's May Motion. Based upon the representations in the motion, the Court found that there was good cause to extend the time limit for its review of the certifications to July 22, 2011, and that the extensions were consistent with national security. May 9, 2011 Orders at 4.

D. The May 9 Briefing Order

Because it appeared to the Court that the acquisitions described in the May 2 Letter exceeded the scope of collection previously disclosed by the government and approved by the Court, and might, in part, fall outside the scope of Section 702, the Court issued a Briefing Order on May 9, 2011 ("Briefing Order"), in which it directed the government to answer a number of questions in writing. Briefing Order at 3-5. On June 1, 2011, the United States filed the "Government's Response to the Court's Briefing Order of May 9, 2011" ("June 1 Submission"). After reviewing the June 1 Submission, the Court, through its staff, directed the government to answer a number of follow-up questions. On June 28, 2011, the government submitted its written responses to the Court's follow-up questions in the "Government's Response to the Court's Follow-Up Questions of June 17, 2011" ("June 28 Submission").

E. The Government's Second Motion for Extensions of Time

The Court met with senior officials of the Department of Justice on July 8, 2011, to

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

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

discuss the information provided by the government in the June 1 and June 28 Submissions. During the meeting, the Court informed the government that it still had serious concerns regarding NSA's acquisition of Internet transactions and, in particular, whether the Court could make the findings necessary to approve the acquisition of such transactions pursuant to Section 702. The Court also noted its willingness to entertain any additional filings that the government might choose to make in an effort to address those concerns.

On July 14, 2011, the government filed a motion seeking additional sixty-day extensions of the periods in which the Court must complete its review of DNI/AG 702(g) Certifications [REDACTED], and the amendments to the certifications in the Prior 702 Dockets. Motion for Orders Extending Time Limits Pursuant to 50 U.S.C. § 1881a(j)(2) ("July Motion").⁶

In its July Motion, the government indicated that it was in the process of compiling additional information regarding the nature and scope of NSA's upstream collection, and that it was "examining whether enhancements to NSA's systems or processes could be made to further ensure that information acquired through NSA's upstream collection is handled in accordance with the requirements of the Act." *Id.* at 8. Because additional time would be needed to supplement the record, however, the government represented that a 60-day extension would be necessary. *Id.* at 8, 11. The government argued that granting the request for an additional extension of time would be consistent with national security, because, by operation of statute, the

⁶ As discussed above, by operation of the Court's order of May 9, 2011, pursuant to 50 U.S.C. § 1881a(j)(2), the Court was required to complete its review of, and issue orders under 50 U.S.C. § 1881a(i)(3) concerning, DNI/AG 702(g) Certifications [REDACTED] and the amendments to the certifications in the Prior 702 Dockets, by July 22, 2011. *Id.* at 6.

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

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

government's acquisition of foreign intelligence information under Certifications [REDACTED]

[REDACTED] could continue pending completion of the Court's review. *Id.* at 9-10.

On July 14, 2011, the Court entered orders granting the government's motion. Based upon the representations in the motion, the Court found that there was good cause to extend the time limit for its review of the certifications to September 20, 2011, and that the extensions were consistent with national security. July 14, 2011 Orders at 4.

F. The August 16 and August 30 Submissions

On August 16, 2011, the government filed a supplement to the June 1 and June 28 Submissions ("August 16 Submission"). In the August 16 Submission, the government described the results of "a manual review by [NSA] of a statistically representative sample of the nature and scope of the Internet communications acquired through NSA's . . . Section 702 upstream collection during a six-month period." Notice of Filing of Aug. 16 Submission at 2. Following a meeting between the Court staff and representatives of the Department of Justice on August 22, 2011, the government submitted a further filing on August 30, 2011 ("August 30 Submission").

G. The Hearing and the Government's Final Written Submission

Following review of the August 30 Submission, the Court held a hearing on September 7, 2011, to ask additional questions of NSA and the Department of Justice regarding the government's statistical analysis and the implications of that analysis. The government made its

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

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

final written submissions on September 9, 2011, and September 13, 2011 (“September 9 Submission” and “September 13 Submission,” respectively).

H. The Final Extension of Time

On September 14, 2011, the Court entered orders further extending the deadline for its completion of the review of the certifications and amendments filed as part of the April Submissions. The Court explained that “[g]iven the complexity of the issues presented in these matters coupled with the Court’s need to fully analyze the supplemental information provided by the government in recent filings, the last of which was submitted to the Court on September 13, 2011, the Court will not be able to complete its review of, and issue orders . . . concerning [the certifications and amendments] by September 20, 2011.” [REDACTED]

[REDACTED] The Court further explained that although it had originally intended to extend the deadline by only one week, the government had advised the Court that “for technical reasons, such a brief extension would compromise the government’s ability to ensure a seamless transition from one Certification to the next.” [REDACTED]

[REDACTED] Accordingly, the Court extended the deadline to October 10, 2011. [REDACTED]

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

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

II. REVIEW OF CERTIFICATIONS [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 of Certifications [REDACTED] confirms that:

- (1) the certifications have been made under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see Certification [REDACTED];
- (2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see Certification [REDACTED];
- (3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures⁷ and minimization procedures;⁸
- (4) each of the certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);⁹ and
- (5) each of the certifications includes an effective date for the authorization in compliance

⁷ See April 2011 Submissions, NSA Targeting Procedures and FBI Targeting Procedures (attached to Certifications [REDACTED]).

⁸ See April 2011 Submissions, NSA Minimization Procedures, FBI Minimization Procedures, and CIA Minimization Procedures (attached to Certifications [REDACTED]).

⁹ See April 2011 Submissions, Affidavits of John C. Inglis, Acting Director, NSA (attached to Certifications [REDACTED]); Affidavit of Gen. Keith B. Alexander, U.S. Army, Director, NSA (attached to Certification [REDACTED]); Affidavits of Robert S. Mueller, III, Director, FBI (attached to Certifications [REDACTED]); Affidavits of Leon E. Panetta, Director, CIA [REDACTED].

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

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

with 50 U.S.C. § 1881a(g)(2)(D), see Certification [REDACTED]
[REDACTED].¹⁰

The Court therefore finds that Certification [REDACTED]

[REDACTED] contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

III. REVIEW OF THE AMENDMENTS TO THE CERTIFICATIONS IN THE PRIOR DOCKETS.

Under the judicial review procedures that apply to amendments by virtue of Section 1881a(i)(1)(C), the Court must review each of the amended certifications “to determine whether the certification contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court has previously determined that the certifications in each of the Prior 702 Dockets, as originally submitted to the Court and previously amended, contained all the required elements.¹¹ Like the prior certifications and amendments, the amendments now before the Court were executed under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), and submitted to the Court within the time allowed under 50 U.S.C. § 1881a(i)(1)(C). See

¹⁰ 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).

¹¹ [REDACTED]

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

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

Certification [REDACTED]¹² Pursuant to Section 1881a(g)(2)(A)(ii), the latest amendments include the attestations of the Attorney General and the DNI that the accompanying NSA and CIA minimization procedures meet the statutory definition of minimization procedures, are consistent with the requirements of the Fourth Amendment, and will be submitted to the Court for approval. Certification [REDACTED]. The latest amendments also include effective dates that comply with 50 U.S.C. § 1881a(g)(2)(D) and § 1881a(i)(1).

Certification [REDACTED] All other aspects of the certifications in the Prior 702 Dockets – including the further attestations made therein in accordance with § 1881a(g)(2)(A), the NSA targeting procedures and FBI minimization procedures submitted therewith in accordance with § 1881a(g)(2)(B),¹³ and the affidavits executed in support thereof in accordance with § 1881a(g)(2)(C) – are unaltered by the latest amendments.

In light of the foregoing, the Court finds that the certifications in the Prior 702 Dockets, as amended, each contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

¹² The amendments to the certifications in the Prior 702 Dockets were approved by the Attorney General on April 11, 2011, and by the DNI on April 13, 2011. See Certification [REDACTED]

¹³ Of course, targeting under the certifications filed in the Prior 702 Dockets will no longer be permitted following the Court's issuance of an order on Certifications [REDACTED]

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

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

IV. 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). See 50 U.S.C. § 1881a(i)(2)(B) and (C); see also 50 U.S.C. § 1881a(i)(1)(C) (providing that amended procedures must be reviewed under the same standard). 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 [50 U.S.C. §§] 1801(h) or 1821(4)” Most notably, that definition requires “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 or physical search], 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.” 50 U.S.C. §§ 1801(h) & 1821(4). Finally, the Court must determine whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A).

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

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

A. The Effect of the Government's Disclosures Regarding NSA's Acquisition of Internet Transactions on the Court's Review of the Targeting and Minimization Procedures

The Court's review of the targeting and minimization procedures submitted with the April 2011 Submissions is complicated by the government's recent revelation that NSA's acquisition of Internet communications through its upstream collection under Section 702 is accomplished by acquiring Internet "transactions," which may contain a single, discrete communication, or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities. June 1 Submission at 1-2. That revelation fundamentally alters the Court's understanding of the scope of the collection conducted pursuant to Section 702 and requires careful reexamination of many of the assessments and presumptions underlying its prior approvals.

In the first Section 702 docket, [REDACTED], the government disclosed that its Section 702 collection would include both telephone and Internet communications. According to the government, the acquisition of telephonic communications would be limited to "to/from" communications – *i.e.*, communications to or from a tasked facility. The government explained, however, that the Internet communications acquired would include both to/from communications and "about" communications – *i.e.*, communications containing a reference to the name of the tasked account. See [REDACTED]. Based upon the government's descriptions of the proposed collection, the Court understood that the acquisition of Internet communications under Section 702 would be limited to discrete "to/from" communications between or among individual account users and to "about"

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

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

communications falling within [REDACTED] specific categories that had been first described to the Court in prior proceedings. [REDACTED]

[REDACTED] Declaration of Director of NSA at 20-22. The Court's analysis and ultimate approval of the targeting and minimization procedures in Docket No. [REDACTED], and in the other [REDACTED] Prior 702 Dockets, depended upon the government's representations regarding the scope of the collection. In conducting its review and granting those approvals, the Court did not take into account NSA's acquisition of Internet transactions, which now materially and fundamentally alters the statutory and constitutional analysis.¹⁴

¹⁴ The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.

In March, 2009, the Court concluded that its authorization of NSA's bulk acquisition of telephone call detail records from [REDACTED] in the so-called "big business records" matter "ha[d] been premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." Docket No. BR 08-13, March 2, 2009 Order at 10-11. Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying. The Court concluded that this requirement had been "so frequently and systemically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively." *Id.*

Shortly thereafter, the government made a similar disclosure regarding NSA's bulk acquisition of metadata regarding Internet communications in the so-called "big pen register" matter. In [REDACTED] the government reported that, from the time of the initial Court authorization in 2004, NSA had been continually collecting various forms of data falling outside the scope of the Court's orders, and that "[v]irtually every PR/TT record' generated by this program included some data that had not been authorized for collection." Docket No. PR/TT [REDACTED] Mem. Op. at 20-21. This long-running and systemic overcollection had

(continued...)

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

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

The government's submissions make clear not only that NSA has been acquiring Internet transactions since before the Court's approval of the first Section 702 certification in 2008,¹⁵ but also that NSA seeks to continue the collection of Internet transactions. Because NSA's acquisition of Internet transactions presents difficult questions, the Court will conduct its review in two stages. Consistent with the approach it has followed in past reviews of Section 702 certifications and amendments, the Court will first consider the targeting and minimization procedures as applied to the acquisition of communications other than Internet transactions – *i.e.*, to the discrete communications between or among the users of telephone and Internet communications facilities that are to or from a facility tasked for collection.¹⁶ The Court will

¹⁴(...continued)

occurred despite the government's repeated assurances over the course of nearly [REDACTED] years that [REDACTED] authorizations granted by docket number PR/TT [REDACTED] and previous docket numbers only collect, or collected, authorized metadata." *Id.* at 20. The overcollection was not detected by NSA until after an "end-to-end review" of the PR/TT metadata program that had been completed by the agency on August 11, 2009. *Id.*

¹⁵ The government's revelations regarding the scope of NSA's upstream collection implicate 50 U.S.C. § 1809(a), which makes it a crime (1) to "engage[] in electronic surveillance under color of law except as authorized" by statute or (2) to "disclose[] or use[] 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. *See* [REDACTED] (concluding that Section 1809(a)(2) precluded the Court from approving the government's proposed use of, among other things, certain data acquired by NSA without statutory authority through its "upstream collection"). The Court will address Section 1809(a) and related issues in a separate order.

¹⁶ As noted, the Court previously authorized the acquisition of [REDACTED] categories of "about" communications. The Court now understands that all "about" communications are acquired by means of NSA's acquisition of Internet transactions through its upstream collection. *See* June 1 Submission at 1-2, *see also* Sept. 7, 2011 Hearing Tr. at 76. Accordingly, the Court considers the
(continued...)

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

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

then assess the effect of the recent disclosures regarding NSA's collection of Internet transactions on its ability to make the findings necessary to approve the certifications and the NSA targeting and minimization procedures.¹⁷

B. The Unmodified Procedures

The government represents that the NSA targeting procedures and the FBI minimization procedures filed with the April 2011 Submissions are identical to the corresponding procedures that were submitted to the Court in Docket Nos. [REDACTED].¹⁸

The Court has reviewed each of these sets of procedures and confirmed that is the case. In fact, the NSA targeting procedures and FBI minimization procedures now before the Court are copies

¹⁶(...continued)

[REDACTED] categories of "about" communications to be a subset of the Internet transactions that NSA acquires. The Court's discussion of the manner in which the government proposes to apply its targeting and minimization procedures to Internet transactions generally also applies to the [REDACTED] categories of "about" communications. See *infra*, pages 41-79.

¹⁷ The FBI and the CIA do not receive unminimized communications that have been acquired through NSA's upstream collection of Internet communications. Sept. 7, 2011 Hearing Tr. at 61-62. Accordingly, the discussion of Internet transactions that appears below does not affect the Court's conclusions that the FBI targeting procedures, the CIA minimization procedures, and the FBI minimization procedures meet the statutory and constitutional requirements.

¹⁸ See Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [REDACTED]; Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [REDACTED]; Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [REDACTED].

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

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

of the procedures that were initially filed on July 29, 2009, in Docket No. [REDACTED]¹⁹ The Court found in those prior dockets that the targeting and minimization procedures were consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.

See Docket No. [REDACTED]

[REDACTED] The Court is prepared to renew its past findings that the NSA targeting procedures (as applied to forms of to/from communications that have previously been described to the Court) and the FBI minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.²⁰

C. The Amended Procedures

As noted above, the FBI targeting procedures and the NSA and CIA minimization procedures submitted with the April 2011 Submissions differ in a number of respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications [REDACTED]. For the reasons that follow, the Court finds that, as applied to the previously authorized collection of discrete communications to or from a tasked facility, the amended FBI targeting procedures and the amended NSA and CIA

¹⁹ Copies of those same procedures were also submitted in Docket Nos. [REDACTED]

²⁰ The Court notes that the FBI minimization procedures are not “set forth in a clear and self-contained manner, without resort to cross-referencing,” as required by FISC Rule 12, which became effective on November 1, 2010. The Court expects that future submissions by the government will comport with this requirement.

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

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

minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.

1. The Amended FBI Targeting Procedures

The government has made three changes to the FBI targeting procedures, all of which involve Section I.4. That provision requires the FBI, [REDACTED]

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

The new language proposed by the government would allow the FBI to [REDACTED]

[REDACTED]

[REDACTED] The government has advised the Court that this change was prompted by the fact that [REDACTED]

[REDACTED] Nevertheless, the current procedures require the FBI to [REDACTED]. The change is intended to eliminate the requirement of [REDACTED].

The second change, reflected in subparagraph (a) of Section I.4, would allow the FBI, under certain circumstances, to [REDACTED]

[REDACTED]

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

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

[REDACTED]

The above-described changes to the FBI targeting procedures pose no obstacle to a finding by the Court that the FBI targeting procedures are “reasonably designed” to “ensure that any acquisition authorized . . . 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.” 50 U.S.C. § 1881a(d)(1). [REDACTED]

[REDACTED]

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

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

[REDACTED]

[REDACTED]

Furthermore, as the Court has previously noted, before the FBI targeting procedures are applied, NSA will have followed its own targeting procedures in determining that the user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States. See Docket No. [REDACTED]. The FBI targeting procedures apply in addition to the NSA targeting procedures, [REDACTED] [REDACTED] Id. The Court has previously found that the NSA targeting procedures proposed for use in connection with Certifications [REDACTED] are reasonably designed to ensure that the users of tasked selectors are non-United States persons reasonably believed to be located outside the United States and also consistent with the Fourth Amendment. See Docket No. [REDACTED] [REDACTED]. It therefore follows that the amended FBI targeting procedures, which provide additional assurance that the users of tasked accounts are non-United States persons located outside the United States, also pass muster.

2. The Amended NSA Minimization Procedures

The most significant change to the NSA minimization procedures regards the rules for querying the data that NSA acquires pursuant to Section 702. The procedures previously approved by the Court effectively impose a wholesale bar on queries using United States-Person identifiers. The government has broadened Section 3(b)(5) to allow NSA to query the vast majority of its Section 702 collection using United States-Person identifiers, subject to approval

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

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

pursuant to internal NSA procedures and oversight by the Department of Justice.²¹ Like all other NSA queries of the Section 702 collection, queries using United States-person identifiers would be limited to those reasonably likely to yield foreign intelligence information. NSA Minimization Procedures § 3(b)(5). The Department of Justice and the Office of the DNI would be required to conduct oversight regarding NSA's use of United States-person identifiers in such queries. See id.

This relaxation of the querying rules does not alter the Court's prior conclusion that NSA minimization procedures meet the statutory definition of minimization procedures. The Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act ("FBI SMPs") contain an analogous provision allowing queries of unminimized FISA-acquired information using identifiers – including United States-person identifiers – when such queries are designed to yield foreign intelligence information. See FBI SMPs § III.D. In granting hundreds of applications for electronic surveillance or physical search since 2008, including applications targeting United States persons and persons in the United States, the Court has found that the FBI SMPs meet the definitions of minimization procedures at 50 U.S.C. §§ 1801(h) and 1821(4). It follows that the substantially-similar

²¹ The government is still in the process of developing its internal procedures and will not permit NSA analysts to begin using United States-person identifiers as selection terms until those procedures are completed. June 28 Submission at 4 n.3. In addition, the government has clarified that United States-person identifiers will not be used to query the fruits of NSA's upstream collection. Aug. 30 Submission at 11. NSA's upstream collection acquires approximately 9% of the total Internet communications acquired by NSA under Section 702. Aug. 16 Submission at 2.

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

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

querying provision found at Section 3(b)(5) of the amended NSA minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons.

A second change to the NSA minimization procedures is the addition of language specifying that the five-year retention period for communications that are not subject to earlier destruction runs from the expiration date of the certification authorizing the collection. See NSA Minimization Procedures, §§ 3(b)(1), 3(c), 5(3)(b), and 6(a)(1)(b). The NSA minimization procedures that were previously approved by the Court included a retention period of five years, but those procedures do not specify when the five-year period begins to run. The change proposed here harmonizes the procedures with the corresponding provision of the FBI minimization procedures for Section 702 that has already been approved by the Court. See FBI Minimization Procedures at 3 (¶ j).

The two remaining changes to the NSA minimization procedures are intended to clarify the scope of the existing procedures. The government has added language to Section 1 to make explicit that the procedures apply not only to NSA employees, but also to any other persons engaged in Section 702-related activities that are conducted under the direction, authority or control of the Director of NSA. NSA Minimization Procedures at 1. According to the government, this new language is intended to clarify that Central Security Service personnel conducting signals intelligence operations authorized by Section 702 are bound by the procedures, even when they are deployed with a military unit and subject to the military chain of

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

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

command. The second clarifying amendment is a change to the definition of “identification of a United States person” in Section 2. The new language eliminates a potential ambiguity that might have resulted in the inappropriate treatment of the name, unique title, or address of a United States person as non-identifying information in certain circumstances. *Id.* at 2. These amendments, which resolve any arguable ambiguity in favor of broader application of the protections found in the procedures, raise no concerns.

3. The Amended CIA Minimization Procedures

The CIA minimization procedures include a new querying provision similar to the provision that the government proposes to add to the NSA minimization procedures and that is discussed above. CIA Minimization Procedures § 4. The new language would allow the CIA to conduct queries of Section 702-acquired information using United States-person identifiers. All CIA queries of the Section 702 collection would be subject to review by the Department of Justice and the Office of the DNI. *See id.* For the reasons stated above with respect to the relaxed querying provision in the amended NSA minimization procedures, the addition of the new CIA querying provision does not preclude the Court from concluding that the amended CIA minimization procedures satisfy the statutory definition of minimization procedures and comply with the Fourth Amendment.²²

The amended CIA minimization procedures include a definition of “United States person identity,” a term that is not defined in the current version of the procedures. CIA Minimization

²² The Court understands that NSA does not share its upstream collection in unminimized form with the CIA. [REDACTED]

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

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

Procedures § 1.b. The proposed definition closely tracks the revised definition of “identification of a United States person” that is included in the amended NSA minimization procedures and discussed above. For the same reasons, the addition of this definition, which clarifies the range of protected information, raises no concerns in the context of the CIA minimization procedures.

Another new provision of the CIA minimization procedures prescribes the manner in which the CIA must store unminimized Section 702-acquired communications. See CIA Minimization Procedures § 2. The same provision establishes a default retention period for unminimized communications that do not qualify for longer retention under one of three separate provisions. See id. Absent an extension by the Director of the National Clandestine Service or one of his superiors, that default retention period is five years from the date of the expiration of the certification authorizing the collection. Id. As noted above, this is the same default retention period that appears in the FBI minimization procedures that have previously been approved by the Court. See FBI Minimization Procedures at 3 (¶ j).

The government also has added new language to the CIA minimization procedures to clarify that United States person information deemed to qualify for retention based on its public availability or on the consent of the person to whom it pertains may be kept indefinitely and stored separately from the unminimized information subject to the default storage and retention rules set forth in new Section 2, which is discussed above. CIA Minimization Procedures § 2. Because FISA’s minimization requirements are limited to the acquisition, retention, and dissemination of “nonpublicly available information concerning unconsenting United States persons,” this provision raises no statutory concern. See 50 U.S.C. §§ 1801(h)(1), 1821(4)(A)

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

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

(emphasis added). It likewise raises no Fourth Amendment problem. See Katz v. United States, 389 U.S. 347, 351 (1967) (“What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.”).

Finally, a new provision would expressly allow the CIA to retain information acquired pursuant to Section 702 in emergency backup systems that may be used to restore data in the event of a system failure. CIA Minimization Procedures § 6(e). Only non-analyst technical personnel will have access to data stored in data backup systems. Id. Further, in the event that such systems are used to restore lost, destroyed, or inaccessible data, the CIA must apply its minimization procedures to the transferred data. Id. The FBI minimization procedures that have previously been approved by the Court contemplate the storage of Section 702 collection in emergency backup systems that are not accessible to analysts, subject to similar restrictions. See FBI Minimization Procedures at 2 (¶ e.3). The Court likewise sees no problem with the addition of Section 6(e) to the CIA minimization procedures.

D. The Effect of the Government’s Disclosures Regarding NSA’s Acquisition of Internet Transactions

Based on the government’s prior representations, the Court has previously analyzed NSA’s targeting and minimization procedures only in the context of NSA acquiring discrete communications. Now, however, in light of the government’s revelations as to the manner in which NSA acquires Internet communications, it is clear that NSA acquires “Internet

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

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

Fourth Amendment.

For the reasons set forth below, the Court finds that NSA's targeting procedures, as the government proposes to implement them in connection with MCTs, are consistent with the requirements of 50 U.S.C. §1881a(d)(1). However, the Court is unable to find that NSA's minimization procedures, as the government proposes to apply them in connection with MCTs, are "reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], 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." 50 U.S.C. §§ 1801(h)(1) &1821(4)(A). The Court is also unable to find that NSA's targeting and minimization procedures, as the government proposes to implement them in connection with MCTs, are consistent with the Fourth Amendment.

1. The Scope of NSA's Upstream Collection

NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702, but the vast majority of these communications are obtained from Internet service providers and are not at issue here.²⁴ Sept. 9 Submission at 1; Aug. 16 Submission at Appendix A. Indeed, NSA's upstream collection constitutes only approximately

²⁴ In addition to its upstream collection, NSA acquires discrete Internet communications from Internet service providers such as [REDACTED] [REDACTED] [REDACTED] Aug. 16 Submission at 2; Aug. 30 Submission at 11; see also Sept. 7, 2011 Hearing Tr. at 75-77. NSA refers to this non-upstream collection as its "PRISM collection." Aug. 30 Submission at 11. The Court understands that NSA does not acquire "Internet transactions" through its PRISM collection. See Aug. 16 Submission at 1.

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

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

9% of the total Internet communications being acquired by NSA under Section 702. Sept. 9 Submission at 1; Aug. 16 Submission at 2.

Although small in relative terms, NSA's upstream collection is significant for three reasons. First, NSA's upstream collection is "uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information."²⁵ Docket No. [REDACTED].

Second, the Court now understands that, in order to collect those targeted Internet communications, NSA's upstream collection devices acquire Internet transactions, and NSA acquires millions of such transactions each year.²⁶ Third, the government has acknowledged that, due to the technological challenges associated with acquiring Internet transactions, NSA is unable to exclude certain Internet transactions from its upstream collection. See June 1 Submission at 3-12.

In its June 1 Submission, the government explained that NSA's upstream collection devices have technological limitations that significantly affect the scope of collection. [REDACTED]

[REDACTED]

²⁵ [REDACTED]

²⁶ NSA acquired more than 13.25 million Internet transactions through its upstream collection between January 1, 2011, and June 30, 2011. See Aug. 16 Submission at 2; see also Sept. 9 Submission at 1-2.

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

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

[REDACTED]. See id. at 7. Moreover, at the time of acquisition, NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector.²⁷ Id. at 2.

As a practical matter, this means that NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it, and:

[REDACTED]

See id. at 6.

The practical implications of NSA's acquisition of Internet transactions through its upstream collection for the Court's statutory and Fourth Amendment analyses are difficult to assess. The sheer volume of transactions acquired by NSA through its upstream collection is such that any meaningful review of the entire body of the transactions is not feasible. As a result, the Court cannot know for certain the exact number of wholly domestic communications acquired through this collection, nor can it know the number of non-target communications

[REDACTED]

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

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

acquired or the extent to which those communications are to or from United States persons or persons in the United States. Instead, NSA and the Court can only look at samples of the data and then draw whatever reasonable conclusions they can from those samples. Even if the Court accepts the validity of conclusions derived from statistical analyses, there are significant hurdles in assessing NSA's upstream collection. Internet service providers are constantly changing their protocols and the services they provide, and often give users the ability to customize how they use a particular service.²⁸ *Id.* at 24-25. As a result, it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future.

Recognizing that further revelations concerning what NSA has actually acquired through its 702 collection, together with the constant evolution of the Internet, may alter the Court's analysis at some point in the future, the Court must, nevertheless, consider whether NSA's targeting and minimization procedures are consistent with FISA and the Fourth Amendment based on the record now before it. In view of the revelations about how NSA is actually conducting its upstream collection, two fundamental underpinnings of the Court's prior assessments no longer hold true.

28



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

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

First, the Court previously understood that NSA's technical measures²⁹ would prevent the acquisition of any communication as to which the sender and all intended recipients were located in the United States ("wholly domestic communication") except for "theoretically possible" cases

[REDACTED]

[REDACTED]

[REDACTED] The Court now understands, however, that NSA has acquired, is acquiring, and, if the certifications and procedures now before the Court are approved, will continue to acquire, tens of thousands of wholly domestic communications. NSA's manual review of a statistically representative sample drawn from its upstream collection³⁰ reveals that NSA acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication.³¹ See Aug. 16 Submission at 9. In addition to these MCTs, NSA

²⁹ [REDACTED]

³⁰ In an effort to address the Court's concerns, NSA conducted a manual review of a random sample consisting of 50,440 Internet transactions taken from the more than 13.25 million Internet transactions acquired through NSA's upstream collection during a six month period. See generally Aug. 16 Submission (describing NSA's manual review and the conclusions NSA drew therefrom). The statistical conclusions reflected in this Memorandum Opinion are drawn from NSA's analysis of that random sample.

³¹ Of the approximately 13.25 million Internet transactions acquired by NSA through its upstream collection during the six-month period, between 996 and 4,965 are MCTs that contain a wholly domestic communication not to, from, or about a tasked selector. Aug. 16 Submission at 9.

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

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

likely acquires tens of thousands more wholly domestic communications every year,³² given that NSA's upstream collection devices will acquire a wholly domestic "about" SCT if it is routed internationally.³³ Moreover, the actual number of wholly domestic communications acquired

³² NSA's manual review focused on examining the MCTs acquired through NSA's upstream collection in order to assess whether any contained wholly domestic communications. Sept. 7, 2011 Hearing Tr. at 13-14. As a result, once NSA determined that a transaction contained a single, discrete communication, no further analysis of that transaction was done. See Aug. 16 Submission at 3. After the Court expressed concern that this category of transactions might also contain wholly domestic communications, NSA conducted a further review. See Sept. 9 Submission at 4. NSA ultimately did not provide the Court with an estimate of the number of wholly domestic "about" SCTs that may be acquired through its upstream collection. Instead, NSA has concluded that "the probability of encountering wholly domestic communications in transactions that feature only a single, discrete communication should be smaller – and certainly no greater – than potentially encountering wholly domestic communications within MCTs." Sept. 13 Submission at 2.

The Court understands this to mean that the percentage of wholly domestic communications within the universe of SCTs acquired through NSA's upstream collection should not exceed the percentage of MCTs containing a wholly domestic communication that NSA found when it examined all of the MCTs within its statistical sample. Since NSA found 10 MCTs with wholly domestic communications within the 5,081 MCTs reviewed, the relevant percentage is .197% (10/5,081). Aug. 16 Submission at 5.

NSA's manual review found that approximately 90% of the 50,440 transactions in the sample were SCTs. Id. at 3. Ninety percent of the approximately 13.25 million total Internet transactions acquired by NSA through its upstream collection during the six-month period, works out to be approximately 11,925,000 transactions. Those 11,925,000 transactions would constitute the universe of SCTs acquired during the six-month period, and .197% of that universe would be approximately 23,000 wholly domestic SCTs. Thus, NSA may be acquiring as many as 46,000 wholly domestic "about" SCTs each year, in addition to the 2,000-10,000 MCTs referenced above.

³³ Internet communications are "nearly always transmitted from a sender to a recipient through multiple legs before reaching their final destination." June 1 Submission at 6. For example, an e-mail message sent from the user of [REDACTED] to the user of (b) (1) [REDACTED] will at the very least travel from the (b) (1) [REDACTED] user's own computer, to (b) (1) (A) [REDACTED], to [REDACTED], and then to the computer of the [REDACTED] user. Id. Because the communication's route is made up of multiple legs, the transaction used to transmit the communication across any particular leg of the route need only identify the IP

(continued...)

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

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

may be still higher in view of NSA's inability conclusively to determine whether a significant portion of the MCTs within its sample contained wholly domestic communications.³⁴

Second, the Court previously understood that NSA's upstream collection would only acquire the communication of a United States person or a person in the United States if: 1) that

³³(...continued)

addresses at either end of that leg in order to properly route the communication. *Id.* at 7. As a result, for each leg of the route, the transaction header will only contain the IP addresses at either end of that particular leg. *Id.* [REDACTED]

[REDACTED]

³⁴ During its manual review, NSA was unable to determine whether 224 of the 5,081 MCTs reviewed contained any wholly domestic communications, because the transactions lacked sufficient information for NSA to determine the location or identity of the "active user" (*i.e.*, the individual using the electronic communications account/address/identifier to interact with his/her Internet service provider). Aug. 16 Submission at 7. NSA then conducted an intensive review of all available information for each of these MCTs, including examining the contents of each discrete communication contained within it, but was still unable to determine conclusively whether any of these MCTs contained wholly domestic communications. Sept. 9 Submission at 3. NSA asserts that "it is reasonable to presume that [the] 224 MCTs do not contain wholly domestic communications," but concedes that, due to the limitations of the technical means used to prevent the acquisition of wholly domestic communications, NSA may acquire wholly domestic communications. *See* Aug. 30 Submission at 7-8. The Court is prepared to accept that the number of wholly domestic communications acquired in this category of MCTs is relatively small, for the reasons stated in the government's August 30 Submission. However, when considering NSA's upstream collection as a whole, and the limitations of NSA's technical means, the Court is not prepared to presume that the number of wholly domestic communications contained within this category of communications will be zero. Accordingly, the Court concludes that this category of communications acquired through NSA's upstream collection may drive the total number of wholly domestic communications acquired slightly higher.

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

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

person was in direct contact with a targeted selector; 2) the communication referenced the targeted selector, and the communication fell into one of [REDACTED] specific categories of “about” communications; or 3) despite the operation of the targeting procedures, United States persons or persons inside the United States were mistakenly targeted. See Docket No. [REDACTED] [REDACTED]. But the Court now understands that, in addition to these communications, NSA’s upstream collection also acquires: a) the communications of United States persons and persons in the United States that are not to, from, or about a tasked selector and that are acquired solely because the communication is contained within an MCT that somewhere references a tasked selector [REDACTED] [REDACTED] and b) any Internet transaction that references a targeted selector, regardless of whether the transaction falls within one of the [REDACTED] previously identified categories of “about communications,” see June 1 Submission at 24-27. [REDACTED]

On the current record, it is difficult to assess how many MCTs acquired by NSA actually contain a communication of or concerning a United States person,³⁵ or a communication to or from a person in the United States. This is because NSA’s manual review of its upstream collection focused primarily on wholly domestic communications – i.e., if one party to the

³⁵ NSA’s minimization procedures define “[c]ommunications of a United States person” to include “all communications to which a United States person is a party.” NSA Minimization Procedures § 2(c). “Communications concerning a United States person” include “all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person. Id. § 2(b).

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

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

communication was determined to be outside the United States, the communication was not further analyzed. Aug. 16 Submission at 1-2. Nevertheless, NSA's manual review did consider the location and identity of the active user for each MCT acquired, and this information – when considered together with certain presumptions – shows that NSA is likely acquiring tens of thousands of discrete communications of non-target United States persons and persons in the United States, by virtue of the fact that their communications are included in MCTs selected for acquisition by NSA's upstream collection devices.³⁶

To illustrate, based upon NSA's analysis of the location and identity of the active user for the MCTs it reviewed, MCTs can be divided into four categories:

1. MCTs as to which the active user is the user of the tasked facility (i.e., the target of the acquisition) and is reasonably believed to be located outside the United States;³⁷
2. MCTs as to which the active user is a non-target who is believed to be located inside the United States;
3. MCTs as to which the active user is a non-target who is believed to be located outside the United States; and

³⁶ Although there is some overlap between this category of communications and the tens of thousands of wholly domestic communications discussed above, the overlap is limited to MCTs containing wholly domestic communications. To the extent that the wholly domestic communications acquired are SCTs, they are excluded from the MCTs referenced here. Similarly, to the extent communications of non-target United States persons and persons in the United States that are contained within the tens of thousands of MCTs referenced here are not wholly domestic, they would not be included in the wholly domestic communications referenced above.

³⁷ Although it is possible for an active user target to be located in the United States, NSA's targeting procedures require NSA to terminate collection if it determines that a target has entered the United States. NSA Targeting Procedures at 7-8. Accordingly, the Court excludes this potential category from its analysis.

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

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

4. MCTs as to which the active user's identity or location cannot be determined.

Aug. 16 Submission at 4-8.

With regard to the first category, if the target is the active user, then it is reasonable to presume that all of the discrete communications within an MCT will be to or from the target. Although United States persons and persons in the United States may be party to any of those communications, NSA's acquisition of such communications is of less concern than the communications described in the following categories because the communicants were in direct communication with a tasked facility, and the acquisition presumptively serves the foreign intelligence purpose of the collection. NSA acquires roughly 300-400 thousand such MCTs per year.³⁸

For the second category, since the active user is a non-target who is located inside the United States, there is no reason to believe that all of the discrete communications contained within the MCTs will be to, from, or about the targeted selector (although there would need to be at least one such communication in order for NSA's upstream devices to acquire the transaction). Further, because the active user is in the United States, the Court presumes that the majority of that person's communications will be with other persons in the United States, many of whom will be United States persons. NSA acquires approximately 7,000-8,000 such MCTs per year, each of which likely contains one or more non-target discrete communications to or from other

³⁸ NSA acquired between 168,853 and 206,922 MCTs as to which the active user was the target over the six-month period covered by the sample. Aug. 16 Submission at 9.

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

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

persons in the United States.³⁹

The third category is similar to the second in that the active user is a non-target. Therefore, there is no reason to believe that all of the communications within the MCTs will be to, from, or about the targeted selector (although there would need to be at least one such communication in order for NSA's upstream devices to acquire the transaction). However, because the active user is believed to be located outside the United States, the Court presumes that most of that persons's communications will be with other persons who are outside the United States, most of whom will be non-United States persons. That said, the Court notes that some of these MCTs are likely to contain non-target communications of or concerning United States persons, or that are to or from a person in the United States.⁴⁰ The Court has no way of knowing precisely how many such communications are acquired. Nevertheless, it appears that NSA acquires at least 1.3 million such MCTs each year,⁴¹ so even if only 1% of these MCTs

³⁹ In its manual review, NSA identified ten MCTs as to which the active user was in the United States and that contained at least one wholly domestic communication. See Aug. 16 Submission at 5-7. NSA also identified seven additional MCTs as to which the active user was in the United States. Id. at 5. Although NSA determined that at least one party to each of the communications within the seven MCTs was reasonably believed to be located outside the United States, NSA did not indicate whether any of the communicants were United States persons or persons in the United States. Id. The Court sees no reason to treat these two categories of MCTs differently because the active users for both were in the United States. Seventeen MCTs constitutes .3% of the MCTs reviewed (5,081), and .3% of the 1.29-1.39 million MCTs NSA acquires every six months (see id. at 8) is 3,870- 4,170, or 7,740-8,340 every year.

⁴⁰ The government has acknowledged as much in its submissions. See June 28 Submission at 5.

⁴¹ Based on its manual review, NSA assessed that 2668 of the 5,081 MCTs reviewed
(continued...)

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

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

contain a single non-target communication of or concerning a United States person, or that is to or from a person in the United States, NSA would be acquiring in excess of 10,000 additional discrete communications each year that are of or concerning United States persons, or that are to or from a person in the United States.

The fourth category is the most problematic, because without the identity of the active user – i.e., whether the user is the target or a non-target – or the active user’s location, it is difficult to determine what presumptions to make about these MCTs. NSA acquires approximately 97,000-140,000 such MCTs each year.⁴² In the context of wholly domestic communications, the government urges the Court to apply a series of presumptions that lead to the conclusion that this category would not contain any wholly domestic communications. Aug. 30 Submission at 4-8. The Court questions the validity of those presumptions, as applied to wholly domestic communications, but certainly is not inclined to apply them to assessing the likelihood that MCTs might contain communications of or concerning United States persons, or communications to or from persons in the United States. The active users for some of these

⁴¹(...continued)

(approximately 52%) had a non-target active user who was reasonably believed to be located outside the United States. Aug. 16 Submission at 4-5. Fifty-two percent of the 1.29 to 1.39 million MCTs that NSA assessed were acquired through its upstream collection every six months would work out to 670,800 - 722,800 MCTs, or approximately 1.3-1.4 million MCTs per year that have a non-target active user believed to be located outside the United States.

⁴² NSA determined that 224 MCTs of the 5,081 MCTs acquired during a six-month period (b) (1) (A)

From this, NSA concluded that it acquired between 48,609 and 70,168 such MCTs every six months through its upstream collection (or approximately 97,000-140,000 such MCTs each year). Id. at 9 n.27.

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

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

MCTs may be located in the United States, and, even if the active user is located overseas, the MCTs may contain non-target communications of or concerning United States persons or that are to or from persons in the United States. Accordingly, this “unknown” category likely adds substantially to the number of non-target communications of or concerning United States persons or that are to or from persons in the United States being acquired by NSA each year.

In sum, then, NSA’s upstream collection is a small, but unique part of the government’s overall collection under Section 702 of the FAA. NSA acquires valuable information through its upstream collection, but not without substantial intrusions on Fourth Amendment-protected interests. Indeed, the record before this Court establishes that NSA’s acquisition of Internet transactions likely results in NSA acquiring annually tens of thousands of wholly domestic communications, and tens of thousands of non-target communications of persons who have little or no relationship to the target but who are protected under the Fourth Amendment. Both acquisitions raise questions as to whether NSA’s targeting and minimization procedures comport with FISA and the Fourth Amendment.

2. NSA’s Targeting Procedures

The Court will first consider whether NSA’s acquisition of Internet transactions through its upstream collection, as described above, means that NSA’s targeting procedures, as implemented, are not “reasonably designed” to: 1) “ensure that any acquisition authorized under [the certifications] is limited to targeting persons reasonably believed to be located outside the United States”; and 2) “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

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

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

United States.” 50 U.S.C. § 1881a(d)(1); *id.* § (i)(2)(B). The Court concludes that the manner in which NSA is currently implementing the targeting procedures does not prevent the Court from making the necessary findings, and hence NSA’s targeting procedures do not offend FISA.

a. Targeting Persons Reasonably Believed to be Located Outside the United States

To the extent NSA is acquiring Internet transactions that contain a single discrete communication that is to, from, or about a tasked selector, the Court’s previous analysis remains valid. As explained in greater detail in the Court’s September 4, 2008 Memorandum Opinion, in this setting the person being targeted is the user of the tasked selector, and NSA’s pre-targeting and post-targeting procedures ensure that NSA will only acquire such transactions so long as there is a reasonable belief that the target is located outside the United States. Docket No.

[REDACTED]

But NSA’s acquisition of MCTs complicates the Court’s analysis somewhat. With regard to “about” communications, the Court previously found that the user of the tasked facility was the “target” of the acquisition, because the government’s purpose in acquiring such communications is to obtain information about that user. *See id.* at 18. Moreover, the communication is not acquired because the government has any interest in the parties to the communication, other than their potential relationship to the user of the tasked facility, and the parties to an “about” communication do not become targets unless and until they are separately vetted under the targeting procedures. *See id.* at 18-19.

In the case of “about” MCTs – *i.e.*, MCTs that are acquired because a targeted selector is referenced somewhere in the transaction – NSA acquires not only the discrete communication

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

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

that references the tasked selector, but also in many cases the contents of other discrete communications that do not reference the tasked selector and to which no target is a party. See May 2 Letter at 2-3 [REDACTED] By acquiring such MCTs, NSA likely acquires tens of thousands of additional communications of non-targets each year, many of whom have no relationship whatsoever with the user of the tasked selector. While the Court has concerns about NSA's acquisition of these non-target communications, the Court accepts the government's representation that the "sole reason [a non-target's MCT] is selected for acquisition is that it contains the presence of a tasked selector used by a person who has been subjected to NSA's targeting procedures." June 1 Submission at 4. Moreover, at the time of acquisition, NSA's upstream collection devices often lack the capability to determine whether a transaction contains a single communication or multiple communications, or to identify the parties to any particular communication within a transaction. See id. Therefore, the Court has no reason to believe that NSA, by acquiring Internet transactions containing multiple communications, is targeting anyone other than the user of the tasked selector. See United States v. Chemical Found., Inc., 272 U.S. 1, 14-15 (1926) ("The presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties.").

b. Acquisition of Wholly Domestic Communications

NSA's acquisition of Internet transactions complicates the analysis required by Section 1881a(d)(1)(B), since the record shows that the government knowingly acquires tens of thousands of wholly domestic communications each year. At first blush, it might seem obvious

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

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

that targeting procedures that permit such acquisitions could not be “reasonably designed . . . 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.” 50 U.S.C. § 1881a(d)(1)(B). However, a closer examination of the language of the statute leads the Court to a different conclusion.

The government focuses primarily on the “intentional acquisition” language in Section 1881a(d)(1)(B). Specifically, the government argues that NSA is not “intentionally” acquiring wholly domestic communications because the government does not intend to acquire transactions containing communications that are wholly domestic and has implemented technical means to prevent the acquisition of such transactions. See June 28 Submission at 12. This argument fails for several reasons.

NSA targets a person under Section 702 certifications by acquiring communications to, from, or about a selector used by that person. Therefore, to the extent NSA’s upstream collection devices acquire an Internet transaction containing a single, discrete communication that is to, from, or about a tasked selector, it can hardly be said that NSA’s acquisition is “unintentional.” In fact, the government has argued, and the Court has accepted, that the government intentionally acquires communications to and from a target, even when NSA reasonably – albeit mistakenly – believes that the target is located outside the United States. See Docket No. [REDACTED]

With respect to MCTs, the sole reason NSA acquires such transactions is the presence of a tasked selector within the transaction. Because it is technologically infeasible for NSA’s

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

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

upstream collection devices to acquire only the discrete communication to, from, or about a tasked selector that may be contained within an MCT, however, the government argues that the only way to obtain the foreign intelligence information found within the discrete communication is to acquire the entire transaction in which it is contained. June 1 Submission at 21. As a result, the government intentionally acquires all discrete communications within an MCT, including those that are not to, from or about a tasked selector. See June 28 Submission at 12, 14; see also Sept. 7, 2011 Hearing Tr. at 33-34.

The fact that NSA's technical measures cannot prevent NSA from acquiring transactions containing wholly domestic communications under certain circumstances does not render NSA's acquisition of those transactions "unintentional." The government repeatedly characterizes such acquisitions as a "failure" of NSA's "technical means." June 28 Submission at 12; see also Sept. 7, 2011 Hearing Tr. at 35-36. However, there is nothing in the record to suggest that NSA's technical means are malfunctioning or otherwise failing to operate as designed. Indeed, the government readily concedes that NSA will acquire a wholly domestic "about" communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server. See June 1 Submission at 29. And in the case of MCTs containing wholly domestic communications that are not to, from, or about a tasked selector, NSA has no way to determine, at the time of acquisition, that a particular communication within an MCT is wholly domestic. See id. Furthermore, now that NSA's manual review of a sample of its upstream collection has confirmed that NSA likely acquires tens of thousands of wholly domestic communications each year, there is no question that the

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

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

government is knowingly acquiring Internet transactions that contain wholly domestic communications through its upstream collection.⁴³

The government argues that an NSA analyst's post-acquisition discovery that a particular Internet transaction contains a wholly domestic communication should retroactively render NSA's acquisition of that transaction "unintentional." June 28 Submission at 12. That argument is unavailing. NSA's collection devices are set to acquire transactions that contain a reference to the targeted selector. When the collection device acquires such a transaction, it is functioning precisely as it is intended, even when the transaction includes a wholly domestic communication. The language of the statute makes clear that it is the government's intention at the time of acquisition that matters, and the government conceded as much at the hearing in this matter. Sept. 7, 2011 Hearing Tr. at 37-38.

Accordingly, the Court finds that NSA intentionally acquires Internet transactions that reference a tasked selector through its upstream collection with the knowledge that there are tens of thousands of wholly domestic communications contained within those transactions. But this is not the end of the analysis. To return to the language of the statute, NSA's targeting procedures must be reasonably designed to prevent the intentional acquisition of "any communication as to which the sender and all intended recipients are known at the time of

⁴³ It is generally settled that a person intends to produce a consequence either (a) when he acts with a purpose of producing that consequence or (b) when he acts knowing that the consequence is substantially certain to occur. Restatement (Third) of Torts § 1 (2010); see also United States v. Dyer, 589 F.3d 520, 528 (1st Cir. 2009) (in criminal law, "'intent' ordinarily requires only that the defendant reasonably knew the proscribed result would occur"), cert. denied, 130 S. Ct. 2422 (2010).

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

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

acquisition to be located in the United States.” 50 U.S.C. § 1881a(d)(1)(B) (emphasis added).

The underscored language requires an acquisition-by-acquisition inquiry. Thus, the Court must consider whether, at the time NSA intentionally acquires a transaction through its upstream collection, NSA will know that the sender and all intended recipients of any particular communication within that transaction are located in the United States.

Presently, it is not technically possible for NSA to configure its upstream collection devices (b) (1) (A)

[REDACTED]

[REDACTED] the practical effect of this technological limitation is that NSA cannot know at the time it acquires an Internet transaction whether the sender and all intended recipients of any particular discrete communication contained within the transaction are located inside the United States.

[REDACTED]

⁴⁴ See supra, note 33.

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

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

[REDACTED]

Given that NSA's upstream collection devices lack the capacity to detect wholly domestic communications at the time an Internet transaction is acquired, the Court is inexorably led to the conclusion that the targeting procedures are "reasonably designed" 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. This is true despite the fact that NSA knows with certainty that the upstream collection, viewed as a whole, results in the acquisition of wholly domestic communications.

By expanding its Section 702 acquisitions to include the acquisition of Internet transactions through its upstream collection, NSA has, as a practical matter, circumvented the spirit of Section 1881a(b)(4) and (d)(1) with regard to that collection. NSA's knowing acquisition of tens of thousands of wholly domestic communications through its upstream collection is a cause of concern for the Court. But the meaning of the relevant statutory provision is clear and application to the facts before the Court does not lead to an impossible or absurd result. The Court's review does not end with the targeting procedures, however. The Court must

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

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

also consider whether NSA's minimization procedures are consistent with §1881a(e)(1) and whether NSA's targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

3. NSA's Minimization Procedures, As Applied to MCTs in the Manner Proposed by the Government, Do Not Meet FISA's Definition of "Minimization Procedures"

The Court next considers whether NSA's minimization procedures, as the government proposes to apply them to Internet transactions, meet the statutory requirements. As noted above, 50 U.S.C. § 1881a(e)(1) requires that the minimization procedures "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4)" That definition requires "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 or physical search], 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." 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A). For the reasons stated below, the Court concludes that NSA's minimization procedures, as applied to MCTs in the manner proposed by the government, do not meet the statutory definition in all respects.

a. The Minimization Framework

NSA's minimization procedures do not expressly contemplate the acquisition of MCTs, and the language of the procedures does not lend itself to straightforward application to MCTs. Most notably, various provisions of the NSA minimization procedures employ the term

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

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

“communication” as an operative term. As explained below, for instance, the rules governing retention, handling, and dissemination vary depending whether or not a communication is deemed to constitute a “domestic communication” instead of a “foreign communication,” see NSA Minimization Procedures §§ 2(e), 5, 6, 7; a communication “of” or “concerning” a U.S. person, see id. §§ 2(b)-(c), 3(b)(1)-(2), 3(c); a “communication to, from, or about a target,” id. § 3(b)(4); or a “communication . . . reasonably believed to contain foreign intelligence information or evidence of a crime,” id. But MCTs can be fairly described as communications that contain several smaller communications. Applying the terms of the NSA minimization procedures to MCTs rather than discrete communications can produce very different results.

In a recent submission, the government explained how NSA proposes to apply its minimization procedures to MCTs. See Aug. 30 Submission at 8-11.⁴⁵ Before discussing the measures proposed by the government for handling MCTs, it is helpful to begin with a brief overview of the NSA minimization procedures themselves. The procedures require that all acquisitions “will be conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant to the authorized purpose of the collection.” NSA

⁴⁵ Although NSA has been collecting MCTs since before the Court’s approval of the first Section 702 certification in 2008, see June 1 Submission at 2, it has not, to date, applied the measures proposed here to the fruits of its upstream collection. Indeed, until NSA’s manual review of a six-month sample of its upstream collection revealed the acquisition of wholly domestic communications, the government asserted that NSA had never found a wholly domestic communication in its upstream collection. See id.

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

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

Minimization Procedures § 3(a).⁴⁶ Following acquisition, the procedures require that, “[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime.” Id. § 3(b)(4). “Foreign communication means a communication that has at least one communicant outside of the United States.” Id. § 2(e). “All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications.” Id. In addition, domestic communications include “[a]ny communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of the targeting was believed to be a non-United States person but was in fact a United States person” Id. § 3(d)(2). A domestic communication must be “promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that” the communication contains foreign intelligence

⁴⁶ Of course, NSA’s separate targeting procedures, discussed above, also govern the manner in which communications are acquired.

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

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

information or evidence of a crime, or that it falls into another narrow exception permitting retention. See id. § 5.⁴⁷

Upon determining that a communication is a “foreign communication,” NSA must decide whether the communication is “of” or “concerning” a United States person. Id. § 6.

“Communications of a United States person include all communications to which a United States person is a party.” Id. § 2(c). “Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person.” Id. § 2(b).

A foreign communication that is of or concerning a United States person and that is determined to contain neither foreign intelligence information nor evidence of a crime must be destroyed “at the earliest practicable point in the processing cycle,” and “may be retained no longer than five years from the expiration date of the certification in any event.” Id. § 3(b)(1).⁴⁸

⁴⁷ Once such a determination is made by the Director, the domestic communications at issue are effectively treated as “foreign communications” for purposes of the rules regarding retention and dissemination.

⁴⁸ Although Section 3(b)(1) by its terms applies only to “inadvertently acquired communications of or concerning a United States person,” the government has informed the Court that this provision is intended to apply, and in practice is applied, to all foreign communications of or concerning United States persons that contain neither foreign intelligence information nor evidence of a crime. Docket No. 702(i)-08-01, Sept. 2, 2008 Notice of Clarification and Correction at 3-5. Moreover, Section 3(c) of the procedures separately provides that foreign communications that do not qualify for retention and that “are known to contain communications of or concerning United States persons will be destroyed upon recognition,” and, like unreviewed communications, “may be retained no longer than five years from the

(continued...)

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

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

A foreign communication that is of or concerning a United States person may be retained indefinitely if the “dissemination of such communications with reference to such United States persons would be permitted” under the dissemination provisions that are discussed below, or if it contains evidence of a crime. Id. § 6(a)(2)-(3). If the retention of a foreign communication of or concerning a United States person is “necessary for the maintenance of technical databases,” it may be retained for five years to allow for technical exploitation, or for longer than five years if more time is required for decryption or if the NSA Signals Intelligence Director “determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements.” Id. § 6(a)(1).

As a general rule, “[a] report based on communications of or concerning a United States person may be disseminated” only “if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person.” Id. § 6(b). A report including the identity of the United States person may be provided to a “recipient requiring the identity of such person for the performance of official duties,” but only if at least one of eight requirements is also met – for instance, if “the identity of the United States person is necessary to understand foreign intelligence information or assess its importance,” or if “information indicates the United States

⁴⁸(...continued)
expiration date of the certification authorizing the collection in any event.”

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

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

person may be . . . an agent of a foreign power” or that he is “engaging in international terrorism activities.” Id.⁴⁹

b. Proposed Minimization Measures for MCTs

The government proposes that NSA’s minimization procedures be applied to MCTs in the following manner. After acquisition, upstream acquisitions, including MCTs, will reside in NSA repositories until they are accessed (e.g., in response to a query) by an NSA analyst performing his or her day-to-day work. NSA proposes adding a “cautionary banner” to the tools its analysts use to view the content of communications acquired through upstream collection under Section 702. See Aug. 30 Submission at 9. The banner, which will be “broadly displayed on [such] tools,” will “direct analysts to consult guidance on how to identify MCTs and how to handle them.” Id. at 9 & n.6.⁵⁰ Analysts will be trained to identify MCTs and to recognize wholly domestic communications contained within MCTs. See id. at 8-9.

When an analyst identifies an upstream acquisition as an MCT, the analyst will decide whether or not he or she “seek[s] to use a discrete communication within [the] MCT,”

⁴⁹ The procedures also permit NSA to provide unminimized communications to the CIA and FBI (subject to their own minimization procedures), and to foreign governments for the limited purpose of obtaining “technical and linguistic assistance.” NSA Minimization Procedures §§ 6(c), 8(b). Neither of these provisions has been used to share upstream acquisitions. Sept. 7, 2011 Hearing Tr. at 61-62.

⁵⁰ The banner will not be displayed for communications that “can be first identified through technical means where the active user is NSA’s tasked selector or that contain only a single, discrete communication based on particular stable and well-known protocols.” Aug. 30 Submission at 9 n.6. See infra, note 27, and supra, note 54.

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

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

presumably by reviewing some or all of the MCT's contents. Id. at 8.⁵¹ “NSA analysts seeking to use a discrete communication contained in an MCT (for example, in a FISA application, intelligence report, or Section 702 targeting) will assess whether the discrete communication is to, from, or about a tasked selector.” Id. The following framework will then be applied:

- If the discrete communication that the analyst seeks to use is to, from, or about a tasked selector, “any U.S. person information in that communication will be handled in accordance with the NSA minimization procedures.” Id. Presumably, this means that the discrete communication will be treated as a “foreign communication” that is “of” or “concerning” a United States person, as described above. The MCT containing that communication remains available to analysts in NSA’s repositories without any marking to indicate that it has been identified as an MCT or as a transaction containing United States person information.
- If the discrete communication sought to be used is not to, from, or about a tasked selector, and also not to or from an identifiable United States person, “that communication (including any U.S. person information therein) will be handled in accordance with the NSA minimization procedures.” Id. at 8-9.⁵² Presumably, this means that the discrete communication will be treated as a “foreign communication” or, if it contains information concerning a United States person, as a “foreign communication” “concerning a United States person,” as described above. The MCT itself remains available to analysts in NSA’s repositories without any marking to indicate that it has been identified as an MCT or that it contains one or more communications that are not to, from, or about a targeted selector.

⁵¹ A transaction that is identified as an SCT rather than an MCT must be handled in accordance with the standard minimization procedures that are discussed above.

⁵² The Court understands that absent contrary information, NSA treats the user of an account who appears to be located in the United States as “an identifiable U.S. person.” See Aug. 30 Submission at 9 n.7 (“To help determine whether a discrete communication not to, from, or about a tasked selector is to or from a U.S. person, NSA would perform the same sort of technical analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its section 702 targeting procedures.”).

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

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

- A discrete communication that is not to, from, or about a tasked selector but that is to or from an identifiable United States person “cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations).” *Id.* at 9. Presumably, this is a reference to Section 1 of the minimization procedures, which allows NSA to deviate from the procedures in such narrow circumstances, subject to the requirement that prompt notice be given to the Office of the Director of National Intelligence, the Department of Justice, and the Court that the deviation has occurred. Regardless of whether or not the discrete communication is used for this limited purpose, the MCT itself remains in NSA’s databases without any marking to indicate that it is an MCT, or that it contains at least one communication that is to or from an identifiable United States person. *See id.*; Sept. 7, 2011 Hearing Tr. at 61.
- If the discrete communication sought to be used by the analyst (or another discrete communication within the MCT) is recognized as being wholly domestic, the entire MCT will be purged from NSA’s systems. *See* Aug. 30 Submission at 3.

c. Statutory Analysis

i. Acquisition

The Court first considers how NSA’s proposed handling of MCTs bears on whether NSA’s minimization procedures are “reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition . . . 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.” *See* 50 U.S.C. § 1801(h)(1) (emphasis added). Insofar as NSA likely acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication that is neither to, from, nor about a targeted selector,⁵³ and tens of thousands of communications of or

⁵³ As noted above, NSA’s upstream collection also likely results in the acquisition of tens
(continued...)

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

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

concerning United States persons with no direct connection to any target, the Court has serious concerns. The acquisition of such non-target communications, which are highly unlikely to have foreign intelligence value, obviously does not by itself serve the government's need to "obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. § 1801(h)(1).

The government submits, however, that the portions of MCTs that contain references to targeted selectors are likely to contain foreign intelligence information, and that it is not feasible for NSA to limit its collection only to the relevant portion or portions of each MCT – i.e., the particular discrete communications that are to, from, or about a targeted selector. The Court

⁵³(...continued)

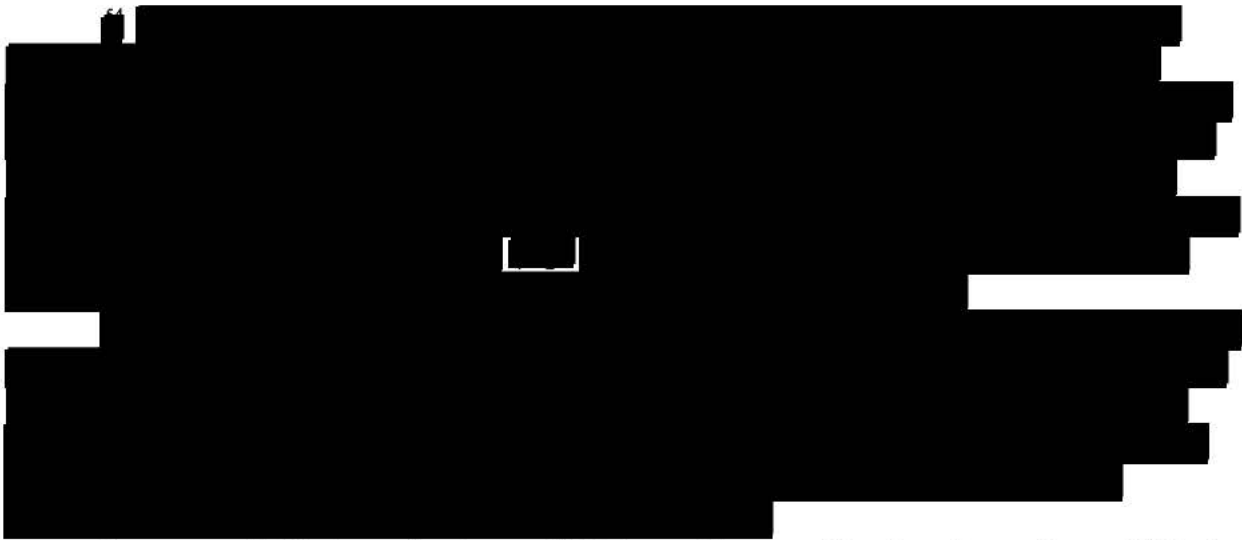
of thousands of wholly domestic SCTs that contain references to targeted selectors. See supra, pages 33-34 & note 33 (discussing the limits [REDACTED])

Although the collection of wholly domestic "about" SCTs is troubling, they do not raise the same minimization-related concerns as discrete, wholly domestic communications that are neither to, from, nor about targeted selectors, or as discrete communications of or concerning United States persons with no direct connection to any target, either of which may be contained within MCTs. The Court has effectively concluded that certain communications containing a reference to a targeted selector are reasonably likely to contain foreign intelligence information, including communications between non-target accounts that contain the name of the targeted facility in the body of the message. See Docket No. 07-449, May 31, 2007 Primary Order at 12 (finding probable cause to believe that certain "about" communications were "themselves being sent and/or received by one of the targeted foreign powers"). Insofar as the discrete, wholly domestic "about" communications at issue here are communications between non-target accounts that contain the name of the targeted facility, the same conclusion applies to them. Accordingly, in the language of FISA's definition of minimization procedures, the acquisition of wholly domestic communications about targeted selectors will generally be "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. 1801(h)(1). Nevertheless, the Court understands that in the event NSA identifies a discrete, wholly domestic "about" communication in its databases, the communication will be destroyed upon recognition. See NSA Minimization Procedures § 5.

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

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

accepts the government's assertion that the collection of MCTs yields valuable foreign intelligence information that by its nature cannot be acquired except through upstream collection. See Sept. 7, 2011 Hearing Tr. at 69-70, 74. For purposes of this discussion, the Court further accepts the government's assertion that it is not feasible for NSA to avoid the collection of MCTs as part of its upstream collection or to limit its collection only to the specific portion or portions of each transaction that contains the targeted selector. See id. at 48-50; June 1 Submission at 27.⁵⁴ The Court therefore concludes that NSA's minimization procedures are, given the current state of NSA's technical capability, reasonably designed to minimize the acquisition 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.



In any event, it is incumbent upon NSA to continue working to enhance its capability to limit acquisitions only to targeted communications.

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

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

ii. Retention

The principal problem with the government's proposed handling of MCTs relates to what will occur, and what will not occur, following acquisition. As noted above, the NSA minimization procedures generally require that, "[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime," see NSA Minimization Procedures § 3(b)(4), so that it can be promptly afforded the appropriate treatment under the procedures. The measures proposed by the government for MCTs, however, largely dispense with the requirement of prompt disposition upon initial review by an analyst. Rather than attempting to identify and segregate information "not relevant to the authorized purpose of the acquisition" or to destroy such information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information, including information of or concerning United States persons with no direct connection to any target. See id. § 3(b)(1).

The proposed measures focus almost exclusively on the discrete communications within MCTs that analysts decide, after review, that they wish to use. See Aug. 30 Submission at 8-10. An analyst is not obligated to do anything with other portions of the MCT, including any wholly domestic discrete communications that are not immediately recognized as such, and communications of or concerning United States persons that have no direct connection to the targeted selector. See id.; Sept. 7, 2011 Hearing Tr. at 61. If, after reviewing the contents of an

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

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

entire MCT, the analyst decides that he or she does not wish to use any discrete communication contained therein, the analyst is not obligated to do anything unless it is immediately apparent to him or her that the MCT contains a wholly domestic communication (in which case the entire MCT is deleted).⁵⁵ See Aug. 30 Submission at 8-10.

Except in the case of those recognized as containing at least one wholly domestic communication, MCTs that have been reviewed by analysts remain available to other analysts in NSA's repositories without any marking to identify them as MCTs. See *id.*; Sept. 7, 2011 Hearing Tr. at 61. Nor will MCTs be marked to identify them as containing discrete communications to or from United States persons but not to or from a targeted selector, or to indicate that they contain United States person information. See Aug. 30 Submission at 8-10; Sept. 7, 2011 Hearing Tr. at 61. All MCTs except those identified as containing one or more wholly domestic communications will be retained for a minimum of five years. The net effect is that thousands of wholly domestic communications (those that are never reviewed and those that are not recognized by analysts as being wholly domestic), and thousands of other discrete

⁵⁵ The government's submissions make clear that, in many cases, it will be difficult for analysts to determine whether a discrete communication contained within an MCT is a wholly domestic communication. NSA's recent manual review of a six-month representative sample of its upstream collection demonstrates how challenging it can be for NSA to recognize wholly domestic communications, even when the agency's full attention and effort are directed at the task. See generally Aug. 16 and Aug. 30 Submissions. It is doubtful that analysts whose attention and effort are focused on identifying and analyzing foreign intelligence information will be any more successful in identifying wholly domestic communications. Indeed, each year the government notifies the Court of numerous compliance incidents involving good-faith mistakes and omissions by NSA personnel who work with the Section 702 collection.

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

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

communications that are not to or from a targeted selector but that are to, from, or concerning a United States person, will be retained by NSA for at least five years, despite the fact that they have no direct connection to a targeted selector and, therefore, are unlikely to contain foreign intelligence information.

It appears that NSA could do substantially more to minimize the retention of information concerning United States persons that is unrelated to the foreign intelligence purpose of its upstream collection. The government has not, for instance, demonstrated why it would not be feasible to limit access to upstream acquisitions to a smaller group of specially-trained analysts who could develop expertise in identifying and scrutinizing MCTs for wholly domestic communications and other discrete communications of or concerning United States persons. Alternatively, it is unclear why an analyst working within the framework proposed by the government should not be required, after identifying an MCT, to apply Section 3(b)(4) of the NSA minimization procedures to each discrete communication within the transaction. As noted above, Section 3(b)(4) states that “[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime.” NSA Minimization Procedures § 3(b)(4). If the MCT contains information “of” or “concerning” a United States person within the meaning of Sections (2)(b) and (2)(c) of the NSA minimization procedures, it is unclear why the analyst should not be required to mark it to identify it as such. At a minimum, it seems that the entire MCT could be marked as an MCT. Such markings would

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

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

alert other NSA personnel who might encounter the MCT to take care in reviewing it, thus reducing the risk of error that seems to be inherent in the measures proposed by the government, which are applied by each analyst, acting alone and without the benefit of his or her colleagues' prior efforts.⁵⁶ Another potentially helpful step might be to adopt a shorter retention period for MCTs and unreviewed upstream communications so that such information "ages off" and is deleted from NSA's repositories in less than five years.

This discussion is not intended to provide a checklist of changes that, if made, would necessarily bring NSA's minimization procedures into compliance with the statute. Indeed, it may be that some of these measures are impracticable, and it may be that there are other plausible (perhaps even better) steps that could be taken that are not mentioned here. But by not fully exploring such options, the government has failed to demonstrate that it has struck a reasonable balance between its foreign intelligence needs and the requirement that information concerning United States persons be protected. Under the circumstances, the Court is unable to find that, as applied to MCTs in the manner proposed by the government, NSA's minimization procedures are "reasonably designed in light of the purpose and technique of the particular surveillance to minimize the . . . retention . . . of nonpublicly available information concerning unconsenting

⁵⁶ The government recently acknowledged that "it's pretty clear that it would be better" if NSA used such markings but that "[t]he feasibility of doing that [had not yet been] assessed." Sept. 7, 2011 Hearing Tr. at 56.

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

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

United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.”⁵⁷ See 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A).

iii. Dissemination

The Court next turns to dissemination. At the outset, it must be noted that FISA imposes a stricter standard for dissemination than for acquisition or retention. While the statute requires procedures that are reasonably designed to “minimize” the acquisition and retention of information concerning United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information, the procedures must be reasonably designed to “prohibit” the dissemination of information concerning United States persons consistent with that need. See 50 U.S.C. § 1801(h)(1) (emphasis added).

⁵⁷ NSA’s minimization procedures contain two provisions that state, in part, that “[t]he communications that may be retained [by NSA] include electronic communications acquired because of limitations

[REDACTED]. The government further represented that it “ha[d] not seen” such a circumstance in collection under the Protect America Act (“PAA”), which was the predecessor to Section 702. *Id.* at 29, 30. And although NSA apparently was acquiring Internet transactions under the PAA, the government made no mention of such acquisitions in connection with these provisions of the minimization procedures (or otherwise). See *id.* at 27-31. Accordingly, the Court does not read this language as purporting to justify the procedures proposed by the government for MCTs. In any event, such a reading would, for the reasons stated, be inconsistent with the statutory requirements for minimization.

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

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

As the Court understands it, no United States-person-identifying information contained in any MCT will be disseminated except in accordance with the general requirements of NSA’s minimization procedures for “foreign communications” “of or concerning United States persons” that are discussed above. Specifically, “[a] report based on communications of or concerning a United States person may be disseminated” only “if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person.” NSA Minimization Procedures § 6(b). A report including the identity of the United States person may be provided to a “recipient requiring the identity of such person for the performance of official duties,” but only if at least one of eight requirements is also met – for instance, if “the identity of the United States person is necessary to understand foreign intelligence information or assess its importance.” *Id.*⁵⁸

This limitation on the dissemination of United States-person-identifying information is helpful. But the pertinent portion of FISA’s definition of minimization procedures applies not merely to information that identifies United States persons, but more broadly to the dissemination of “information concerning unconsenting United States persons.” 50 U.S.C. § 1801(h)(1) (emphasis added).⁵⁹ The government has proposed several additional restrictions that

⁵⁸ Although Section 6(b) uses the term “report,” the Court understands it to apply to the dissemination of United States-person-identifying information in any form.

⁵⁹ Another provision of the definition of minimization procedures bars the dissemination of information (other than certain forms of foreign intelligence information) “in a manner that
(continued...) ”

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

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

will have the effect of limiting the dissemination of “nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to disseminate foreign intelligence information.” *Id.* First, as noted above, the government will destroy MCTs that are recognized by analysts as containing one or more discrete wholly domestic communications. Second, the government has asserted that NSA will not use any discrete communication within an MCT that is determined to be to or from a United States person but not to, from, or about a targeted selector, except when necessary to protect against an immediate threat to human life. *See* Aug. 30 Submission at 9. The Court understands this to mean, among other things, that no information from such a communication will be disseminated in any form unless NSA determines it is necessary to serve this specific purpose. Third, the government has represented that whenever it is unable to confirm that at least one party to a discrete communication contained in an MCT is located outside the United States, it will not use any information contained in the discrete communication. *See* Sept. 7, 2011 Hearing Tr. at 52. The Court understands this limitation to mean that no information from such a discrete communication will be disseminated by NSA in any form.

Communications as to which a United States person or a person inside the United States

⁵⁹(...continued)

identifies any United States person,” except when the person’s identity is necessary to understand foreign intelligence information or to assess its importance. *See* 50 U.S.C. §§ 1801(h)(2), 1821(4)(b). Congress’s use of the distinct modifying terms “concerning” and “identifying” in two adjacent and closely-related provisions was presumably intended to have meaning. *See, e.g., Russello v. United States*, 464 U.S. 16, 23 (1983).

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

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

is a party are more likely than other communications to contain information concerning United States persons. And when such a communication is neither to, from, nor about a targeted facility, it is highly unlikely that the “need of the United States to disseminate foreign intelligence information” would be served by the dissemination of United States-person information contained therein. Hence, taken together, these measures will tend to prohibit the dissemination of information concerning unconsenting United States persons when there is no foreign-intelligence need to do so.⁶⁰ Of course, the risk remains that information concerning United States persons will not be recognized by NSA despite the good-faith application of the measures it proposes. But the Court cannot say that the risk is so great that it undermines the reasonableness of the measures proposed by NSA with respect to the dissemination of information concerning United States persons.⁶¹ Accordingly, the Court concludes that NSA’s

⁶⁰ Another measure that, on balance, is likely to mitigate somewhat the risk that information concerning United States persons will be disseminated in the absence of a foreign-intelligence need is the recently-proposed prohibition on running queries of the Section 702 upstream collection using United States-person identifiers. See Aug. 30 Submission at 10-11. To be sure, any query, including a query based on non-United States-person information, could yield United States-person information. Nevertheless, it stands to reason that queries based on information concerning United States persons are at least somewhat more likely than other queries to yield United States-person information. Insofar as information concerning United States persons is not made available to analysts, it cannot be disseminated. Of course, this querying restriction does not address the retention problem that is discussed above.

⁶¹ In reaching this conclusion regarding the risk that information concerning United States persons might be mistakenly disseminated, the Court is mindful that by taking additional steps to minimize the retention of such information, NSA would also be reducing the likelihood that it might be disseminated when the government has no foreign intelligence need to do so.

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

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

minimization procedures are reasonably designed to “prohibit the dissemination[] of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to . . . disseminate foreign intelligence information.” See 50 U.S.C.

§ 1801(h)(1).⁶²

4. NSA’S Targeting and Minimization Procedures Do Not, as Applied to Upstream Collection that Includes MCTs, Satisfy the Requirements of the Fourth Amendment

The final question for the Court is whether the targeting and minimization procedures are, as applied to upstream collection that includes MCTs, consistent with the Fourth Amendment.

See 50 U.S.C. § 1881a(i)(3)(A)-(B). The Fourth Amendment 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.

The Court has assumed in the prior Section 702 Dockets that at least in some circumstances, account holders have a reasonable expectation of privacy in electronic communications, and hence that the acquisition of such communications can result in a “search” or “seizure” within the meaning of the Fourth Amendment. See, e.g., Docket No. [REDACTED]. [REDACTED]. The government accepts the proposition that the acquisition of

⁶² The Court further concludes that the NSA minimization procedures, as the government proposes to apply them to MCTs, satisfy the requirements of 50 U.S.C. §§ 1801(h)(2)-(3) and 1821(4)(B)-(C). See supra, note 59 (discussing 50 U.S.C. §§ 1801(h)(2) & 1821(4)(B)). The requirements of 50 U.S.C. §§ 1801(h)(4) and 1821(4)(D) are inapplicable here.

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

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

electronic communications can result in a “search” or “seizure” under the Fourth Amendment. See Sept. 7, 2011 Hearing Tr. at 66. Indeed, the government has acknowledged in prior Section 702 matters that the acquisition of communications from facilities used by United States persons located outside the United States “must be in conformity with the Fourth Amendment.” Docket Nos. [REDACTED]. The same is true of the acquisition of communications from facilities used by United States persons and others within the United States. See United States v. Verdugo-Urquidez, 494 U.S. 259, 271 (1990) (recognizing that “aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country”).

a. The Warrant Requirement

The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the “foreign intelligence exception” to the warrant requirement of the Fourth Amendment. See Docket No. [REDACTED]. [REDACTED]. The government’s recent revelations regarding NSA’s acquisition of MCTs do not alter that conclusion. To be sure, the Court now understands that, as a result of the transactional nature of the upstream collection, NSA acquires a substantially larger number of communications of or concerning United States persons and persons inside the United States than previously understood. Nevertheless, the collection as a whole is still directed at [REDACTED] [REDACTED] [REDACTED] conducted for the purpose of national security – a

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

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

purpose going “well beyond any garden-variety law enforcement objective.” See id. (quoting In re Directives, Docket No. 08-01, Opinion at 16 (FISA Ct. Rev. Aug. 22, 2008) (hereinafter “In re Directives”)).⁶³ Further, it remains true that the collection is undertaken in circumstances in which there is a “high degree of probability that requiring a warrant would hinder the government’s ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake.” Id. at 36 (quoting In re Directives at 18). Accordingly, the government’s revelation that NSA acquires MCTs as part of its Section 702 upstream collection does not disturb the Court’s prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA’s targeting and minimization procedures.

b. Reasonableness

The question therefore becomes whether, taking into account NSA’s acquisition and proposed handling of MCTs, the agency’s targeting and minimization procedures are reasonable under the Fourth Amendment. As the Foreign Intelligence Surveillance Court of Review (“Court of Review”) has explained, a court assessing reasonableness in this context must consider “the nature of the government intrusion and how the government intrusion is implemented. The more important the government’s interest, the greater the intrusion that may be constitutionally

⁶³ A redacted, de-classified version of the opinion in In re Directives is published at 551 F.3d 1004. The citations herein are to the unredacted, classified version of the opinion.

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

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

tolerated.” In re Directives at 19-20 (citations omitted), quoted in Docket No. [REDACTED]

[REDACTED]. The court must therefore

balance the interests at stake. If the protections that are in place for individual privacy interests are sufficient in light of the government interest at stake, the constitutional scales will tilt in favor of upholding the government’s actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Id. at 20 (citations omitted), quoted in Docket No. [REDACTED].

In conducting this balancing, the Court must consider the “totality of the circumstances.” Id. at 19. Given the all-encompassing nature of Fourth Amendment reasonableness review, the targeting and minimization procedures are most appropriately considered collectively. See Docket No. [REDACTED] (following the same approach).⁶⁴

The Court has previously recognized that the government’s national security interest in conducting acquisitions pursuant to Section 702 “is of the highest order of magnitude.” Docket No. [REDACTED] (quoting In re Directives at 20). The Court has further accepted the government’s representations that NSA’s upstream collection is “uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information.” Docket No. [REDACTED] (quoting

⁶⁴ Reasonableness review under the Fourth Amendment is broader than the statutory assessment previously addressed, which is necessarily limited by the terms of the pertinent provisions of FISA.

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

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

government filing). There is no reason to believe that the collection of MCTs results in the acquisition of less foreign intelligence information than the Court previously understood.

Nevertheless, it must be noted that NSA's upstream collection makes up only a very small fraction of the agency's total collection pursuant to Section 702. As explained above, the collection of telephone communications under Section 702 is not implicated at all by the government's recent disclosures regarding NSA's acquisition of MCTs. Nor do those disclosures affect NSA's collection of Internet communications directly from Internet service providers [REDACTED], which accounts for approximately 91% of the Internet communications acquired by NSA each year under Section 702. See Aug. 16 Submission at Appendix A. And the government recently advised that NSA now has the capability, at the time of acquisition, to identify approximately 40% of its upstream collection as constituting discrete communications (non-MCTs) that are to, from, or about a targeted selector. See *id.* at 1 n.2. Accordingly, only approximately 5.4% (40% of 9%) of NSA's aggregate collection of Internet communications (and an even smaller portion of the total collection) under Section 702 is at issue here. The national security interest at stake must be assessed bearing these numbers in mind.

The government's recent disclosures regarding the acquisition of MCTs most directly affect the privacy side of the Fourth Amendment balance. The Court's prior approvals of the targeting and minimization procedures rested on its conclusion that the procedures "reasonably confine acquisitions to targets who are non-U.S. persons outside the United States," who thus

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

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

“are not protected by the Fourth Amendment.” Docket No. [REDACTED]

[REDACTED] The Court’s approvals also rested upon the understanding that acquisitions under the procedures “will intrude on interests protected by the Fourth Amendment only to the extent that (1) despite the operation of the targeting procedures, U.S. persons, or persons actually in the United States, are mistakenly targeted; or (2) U.S. persons, or persons located in the United States, are parties to communications to or from tasked selectors (or, in certain circumstances, communications that contain a reference to a tasked selector).” *Id.* at 38. But NSA’s acquisition of MCTs substantially broadens the circumstances in which Fourth Amendment-protected interests are intruded upon by NSA’s Section 702 collection. Until now, the Court has not considered these acquisitions in its Fourth Amendment analysis.

Both in terms of its size and its nature, the intrusion resulting from NSA’s acquisition of MCTs is substantial. The Court now understands that each year, NSA’s upstream collection likely results in the acquisition of roughly two to ten thousand discrete wholly domestic communications that are neither to, from, nor about a targeted selector, as well as tens of thousands of other communications that are to or from a United States person or a person in the United States but that are neither to, from, nor about a targeted selector.⁶⁵ In arguing that NSA’s

⁶⁵ As discussed earlier, NSA also likely acquires tens of thousands of discrete, wholly domestic communications that are “about” a targeted facility. Because these communications are reasonably likely to contain foreign intelligence information and thus, generally speaking, serve the government’s foreign intelligence needs, they do not present the same Fourth Amendment concerns as the non-target communications discussed here. *See supra*, note 53.

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

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

targeting and minimization procedures satisfy the Fourth Amendment notwithstanding the acquisition of MCTs, the government stresses that the number of protected communications acquired is relatively small in comparison to the total number of Internet communications obtained by NSA through its upstream collection. That is true enough, given the enormous volume of Internet transactions acquired by NSA through its upstream collection (approximately 26.5 million annually). But the number is small only in that relative sense. The Court recognizes that the ratio of non-target, Fourth Amendment-protected communications to the total number of communications must be considered in the Fourth Amendment balancing. But in conducting a review under the Constitution that requires consideration of the totality of the circumstances, see In re Directives at 19, the Court must also take into account the absolute number of non-target, protected communications that are acquired. In absolute terms, tens of thousands of non-target, protected communications annually is a very large number.

The nature of the intrusion at issue is also an important consideration in the Fourth Amendment balancing. See, e.g., Board of Educ. v. Earls, 536 U.S. 822, 832 (2002); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 659 (1995). At issue here are the personal [REDACTED] communications of U.S. persons and persons in the United States. A person's "papers" are among the four items that are specifically listed in the Fourth Amendment as subject to protection against unreasonable search and seizure. Whether they are transmitted by letter,

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

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

telephone or e-mail, a person's private communications are akin to personal papers. Indeed, the Supreme Court has held that the parties to telephone communications and the senders and recipients of written communications generally have a reasonable expectation of privacy in the contents of those communications. See Katz, 389 U.S. at 352; United States v. United States Dist. Ct. (Keith), 407 U.S. 297, 313 (1972); United States v. Jacobsen, 466 U.S. 109, 114 (1984). The intrusion resulting from the interception of the contents of electronic communications is, generally speaking, no less substantial.⁶⁶

The government stresses that the non-target communications of concern here (discrete wholly domestic communications and other discrete communications to or from a United States person or a person in the United States that are neither to, from, nor about a targeted selector) are acquired incidentally rather than purposefully. See June 28 Submission at 13-14. Insofar as NSA acquires entire MCTs because it lacks the technical means to limit collection only to the discrete portion or portions of each MCT that contain a reference to the targeted selector, the Court is satisfied that is the case. But as the government correctly recognizes, the acquisition of non-target information is not necessarily reasonable under the Fourth Amendment simply

⁶⁶ Of course, not every interception by the government of a personal communication results in a "search" or "seizure" within the meaning of the Fourth Amendment. Whether a particular intrusion constitutes a search or seizure depends on the specific facts and circumstances involved.

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

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

because its collection is incidental to the purpose of the search or surveillance. See id. at 14.

There surely are circumstances in which incidental intrusions can be so substantial as to render a search or seizure unreasonable. To use an extreme example, if the only way for the government to obtain communications to or from a particular targeted [REDACTED] required also acquiring all communications to or from every other [REDACTED], such collection would certainly raise very serious Fourth Amendment concerns.

Here, the quantity and nature of the information that is “incidentally” collected distinguishes this matter from the prior instances in which this Court and the Court of Review have considered incidental acquisitions. As explained above, the quantity of incidentally-acquired, non-target, protected communications being acquired by NSA through its upstream collection is, in absolute terms, very large, and the resulting intrusion is, in each instance, likewise very substantial. And with regard to the nature of the acquisition, the government acknowledged in a prior Section 702 docket that the term “incidental interception” is “most commonly understood to refer to an intercepted communication between a target using a facility subject to surveillance and a third party using a facility not subject to surveillance.” Docket Nos.

[REDACTED] This is the sort of acquisition that the Court of Review was addressing in In re Directives when it stated that “incidental collections occurring as a result of constitutionally permissible acquisitions do not

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

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

render those acquisitions unlawful.” In re Directives at 30. But here, by contrast, the incidental acquisitions of concern are not direct communications between a non-target third party and the user of the targeted facility. Nor are they the communications of non-targets that refer directly to a targeted selector. Rather, the communications of concern here are acquired simply because they appear somewhere in the same transaction as a separate communication that is to, from, or about the targeted facility.⁶⁷

The distinction is significant and impacts the Fourth Amendment balancing. A discrete communication as to which the user of the targeted facility is a party or in which the targeted

⁶⁷ The Court of Review plainly limited its holding regarding incidental collection to the facts before it. See In re Directives at 30 (“On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.”) (emphasis added). The dispute in In re Directives involved the acquisition by NSA of discrete to/from communications from an Internet Service Provider, not NSA’s upstream collection of Internet transactions. Accordingly, the Court of Review had no occasion to consider NSA’s acquisition of MCTs (or even “about” communications, for that matter). Furthermore, the Court of Review noted that “[t]he government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary.” Id. Here, however, the government proposes measures that will allow NSA to retain non-target United States person information in its databases for at least five years.

The Title III cases cited by the government (see June 28 Submission at 14-15) are likewise distinguishable. Abraham v. County of Greenville, 237 F.3d 386, 391 (4th Cir. 2001), did not involve incidental overhears at all. The others involved allegedly non-pertinent communications to or from the facilities for which wiretap authorization had been granted, rather than communications to or from non-targeted facilities. See Scott v. United States, 436 U.S. 128, 130-31 (1978), United States v. McKinnon, 721 F.2d 19, 23 (1st Cir. 1983), and United States v. Doolittle, 507 F.2d 1368, 1371, *aff’d en banc*, 518 F.2d 500 (5th Cir. 1975).

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

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

facility is mentioned is much more likely to contain foreign intelligence information than is a separate communication that is acquired simply because it happens to be within the same transaction as a communication involving a targeted facility. Hence, the national security need for acquiring, retaining, and disseminating the former category of communications is greater than the justification for acquiring, retaining, and disseminating the latter form of communication.

The Court of Review and this Court have recognized that the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information. See In re Directives at 29-30; Docket No. [REDACTED]. As explained in the discussion of NSA's minimization procedures above, the measures proposed by NSA for handling MCTs tend to maximize, rather than minimize, the retention of non-target information, including information of or concerning United States persons. Instead of requiring the prompt review and proper disposition of non-target information (to the extent it is feasible to do so), NSA's proposed measures focus almost exclusively on those portions of an MCT that an analyst decides, after review, that he or she wishes to use. An analyst is not required to determine whether other portions of the MCT constitute discrete communications to or from a United States person or a person in the United States, or contain information concerning a United States person or person inside the United States, or, having made such a determination, to do anything about it. Only

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

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

those MCTs that are immediately recognized as containing a wholly domestic discrete communication are purged, while other MCTs remain in NSA's repositories for five or more years, without being marked as MCTs. Nor, if an MCT contains a discrete communication of, or other information concerning, a United States person or person in the United States, is the MCT marked as such. Accordingly, each analyst who retrieves an MCT and wishes to use a portion thereof is left to apply the proposed minimization measures alone, from beginning to end, and without the benefit of his colleagues' prior review and analysis. Given the limited review of MCTs that is required, and the difficulty of the task of identifying protected information within an MCT, the government's proposed measures seem to enhance, rather than reduce, the risk of error, overretention, and dissemination of non-target information, including information protected by the Fourth Amendment.

In sum, NSA's collection of MCTs results in the acquisition of a very large number of Fourth Amendment-protected communications that have no direct connection to any targeted facility and thus do not serve the national security needs underlying the Section 702 collection as a whole. Rather than attempting to identify and segregate the non-target, Fourth-Amendment protected information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information and hence to enhance the risk that it will be used and disseminated. Under the totality of the circumstances, then, the Court is unable to find that

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

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

the government's proposed application of NSA's targeting and minimization procedures to MCTs is consistent with the requirements of the Fourth Amendment. The Court does not foreclose the possibility that the government might be able to tailor the scope of NSA's upstream collection, or adopt more stringent post-acquisition safeguards, in a manner that would satisfy the reasonableness requirement of the Fourth Amendment.⁶⁸

V. CONCLUSION

For the foregoing reasons, the government's requests for approval of the certifications and procedures contained in the April 2011 Submissions are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the “upstream collection” of Internet transactions containing multiple communications, or MCTs – is, in some respects, deficient on statutory and constitutional grounds. Specifically, the Court finds as follows:

1. Certifications [REDACTED] and the amendments to the Certifications in the Prior 702 Dockets, contain all the required elements;

⁶⁸ As the government notes, see June 1 Submission at 18-19, the Supreme Court has “repeatedly refused to declare that only the ‘least intrusive’ search practicable can be reasonable under the Fourth Amendment.” City of Ontario v. Quon, — U.S. —, 130 S. Ct. 2619, 2632 (2010) (citations and internal quotation marks omitted). The foregoing discussion should not be understood to suggest otherwise. Rather, the Court holds only that the means actually chosen by the government to accomplish its Section 702 upstream collection are, with respect to MCTs, excessively intrusive in light of the purpose of the collection as a whole.

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

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

2. As applied to telephone communications and discrete Internet communications that are to or from a facility tasked for collection, to non-MCT “about” communications falling within the [REDACTED] categories previously described by the government,⁶⁹ and to MCTs as to which the “active user” is known to be a tasked selector, 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;

3. NSA’s targeting procedures, as the government proposes to implement them in connection with the acquisition of MCTs, meet the requirements of 50 U.S.C. § 1881a(d);

4. NSA’s minimization procedures, as the government proposes to apply them to MCTs as to which the “active user” is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention; and

5. NSA’s targeting and minimization procedures, as the government proposes to apply them to MCTs as to which the “active user” is not known to be a tasked selector, are inconsistent with the requirements of the Fourth Amendment.

⁶⁹ See Docket No. [REDACTED].

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

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

Orders approving the certifications and amendments in part are being entered contemporaneously herewith.

ENTERED this 3rd day of October, 2011.



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

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

[REDACTED], Deputy Clerk,
FISC, certify that this document
is a true and correct copy of
the original. [REDACTED]

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

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



ORDER

These matters are before the Court on: (1) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was filed

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

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

on April 20, 2011; (2) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was filed on April 22, 2011; and (3) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was also filed on April 22, 2011 (collectively, the “April 2011 Submissions”).

Through the April 2011 Submissions, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA” or the “Act”), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth in the accompanying Memorandum Opinion, the government’s requests for approval are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the “upstream collection” of Internet transactions containing multiple communications, or “MCTs” – is, in some respects, deficient on statutory and constitutional grounds. Specifically, the Court finds as follows:

1. DNI/AG 702(g) Certifications [REDACTED], as well as the amendments to the other certifications listed above and contained in the April 2011 Submissions,

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

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

contain all the required elements;

2. As applied to telephone communications and discrete Internet communications that are to or from a facility tasked for collection, to non-MCT “about” communications falling within the [REDACTED] categories previously described by the government,¹ and to MCTs as to which the “active user” is known to be a tasked selector, 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;

3. NSA’s targeting procedures, as the government proposes to implement them in connection with the acquisition of MCTs, meet the requirements of 50 U.S.C. § 1881a(d);

4. NSA’s minimization procedures, as the government proposes to apply them to MCTs as to which the “active user” is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention; and

5. NSA’s targeting and minimization procedures, as the government proposes to apply them to MCTs as to which the “active user” is not known to be a tasked selector, are inconsistent with the requirements of the Fourth Amendment.

Accordingly, pursuant to 50 U.S.C. § 1881a(i)(3)(B), the government shall, at its election:

(a) not later than 30 days from the issuance of this Order, correct the deficiencies identified in the accompanying Memorandum Opinion; or,

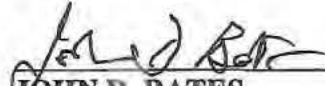
¹ See Docket No. 702(i)-08-01, Sept. 4, Memorandum Opinion at 17-18 n.14.

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

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

(b) cease the implementation of the Certifications insofar as they permit the acquisition of MCTs as to which the "active user" is not known to be a tasked selector.

ENTERED this 3rd day of October, 2011, at 4:55 p.m. Eastern Time.



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

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



I,  Deputy Clerk,
FISC, certify that this document
is a true and correct copy of
the original. 

EXHIBIT C

~~TOP SECRET//SI//ORCON,NOFORN~~

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

b(1) and b(3)



MEMORANDUM OPINION

This matter is before the Foreign Intelligence Surveillance Court (“FISC” or “Court”) on the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications,” which was filed on August 24, 2012

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

(“August 24 Submission”). Through the August 24 Submission, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA” or the “Act”), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth below, the government’s request for approval is granted.

I. BACKGROUND

The August 24 Submission includes (b)(1) and (b)(3)

(b)(1) and (b)(3)

(b)(1) and (b)(3) all of which were executed by the Attorney General and the Acting Director of National Intelligence (“DNI”) pursuant to Section 702. Each of the (b)(1) and (b)(3) certifications is accompanied by the supporting affidavits of the Acting 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 NSA and FBI respectively; and four sets of minimization procedures, for use by NSA, FBI, CIA, and the National Counterterrorism Center (“NCTC”), respectively.

Like the acquisitions approved by the Court in all prior Section 702 dockets, collection under Certifications (b)(1) and (b)(3) is limited to “the targeting of non-United States persons reasonably believed to be located outside the United States.”

(b)(1) and (b)(3)

(b)(1) and (b)(3)

(b)(1) and (b)(3)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

b(1) and b(3)

The August 24 Submission also includes amendments to certifications that have been submitted by the government and approved by the Court in all prior Section 702 dockets. See

Docket Nos.

b(1) and b(3)

b(1) and b(3)

(collectively, the "Prior

702 Dockets"). The amendments, which have been authorized by the Attorney General and the

DNI, provide that information collected under the certifications in the Prior 702 Dockets will,

effective upon the Court's approval of Certifications b(1) and b(3) be handled

subject to the same minimization procedures that have been submitted for use in connection with

Certifications

b(1) and b(3)

b(1) and b(3)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

II. REVIEW OF CERTIFICATIONS

b(1) and b(3)

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 of Certifications b(1) and b(3) confirms that:

(1) the certifications have been made under oath by the Attorney General and the DNI,¹ as required by 50 U.S.C. § 1881a(g)(1)(A). see b(1) and b(3)

(2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see b(1) and b(3)

(3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures² and minimization procedures,³

(4) each of the certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);⁴ and

(5) each of the certifications includes an effective date for the authorization in compliance

¹ The Principal Deputy Director of National Intelligence, in her capacity as Acting DNI, executed the Certifications in accordance with 50 U.S.C. § 403-3A(a)(6), which provides in pertinent part that “the Principal Deputy Director of National Intelligence shall act for, and exercise the powers of, the Director of National Intelligence during the absence or disability of the Director of National Intelligence.”

b(1) and b(3) ² The NSA targeting procedures and FBI targeting procedures are attached to each of the certifications as Exhibits A and C, respectively.

³ The NSA minimization procedures, FBI minimization procedures, CIA minimization procedures, and NCTC minimization procedures are attached to each of the b(1) and b(3) certifications as Exhibits B, D, E, and G, respectively.

⁴ See Affidavits of John C. Inglis, Acting Director, NSA (Tab 1 to b(1) and b(3)); Affidavits of Robert S. Mueller, III, Director, FBI (Tab 2 to b(1) and b(3)); Affidavits of David H. Petraeus, Director, CIA (Tab 3 to b(1) and b(3))

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

with 50 U.S.C. § 1881a(g)(2)(D), see [redacted] b(1) and b(3)
[redacted] b(1) and b(3)

The Court therefore finds that [redacted] b(1) and b(3)

[redacted] b(1) and b(3) contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

III. REVIEW OF THE AMENDMENTS TO THE CERTIFICATIONS IN THE PRIOR DOCKETS

Under the judicial review procedures that apply to amendments by virtue of Section 1881a(i)(1)(C), the Court must review each of the amended certifications “to determine whether the certification contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court has previously determined that each of the certifications filed in the Prior 702 dockets, as originally submitted to the Court and previously amended, contained all the required elements. Like the prior certifications and amendments, the amendments now before the Court were executed under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), and submitted to the Court within the time allowed under 50 U.S.C. § 1881a(i)(1)(C). See

[redacted] b(1) and b(3) Pursuant to

Section 1881a(g)(2)(A)(ii), the latest amendments include the attestations of the Attorney General and the DNI that the accompanying NSA and CIA minimization procedures meet the statutory definition of minimization procedures, are consistent with the requirements of the Fourth Amendment, and will be submitted to the Court for approval. [redacted] b(1) and b(3)

[redacted] b(1) and b(3) The latest amendments also

⁵ 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).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

include effective dates that comply with 50 U.S.C. § 1881a(g)(2)(D) and § 1881a(i)(1).

b(1) and b(3)

All other aspects

of the certifications in the Prior 702 dockets – including the further attestations made therein in accordance with Section 1881a(g)(2)(A), the FBI and NSA targeting procedures submitted therewith in accordance with Section 1881a(g)(2)(B),⁶ and the affidavits executed in support thereof in accordance with Section 1881a(g)(2)(C) – are unaltered by the latest amendments.

In light of the foregoing, the Court finds that the certifications in the Prior 702 Dockets, as amended, each contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

IV. 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). See 50 U.S.C. § 1881a(i)(2)(B) and (C); see also 50 U.S.C. § 1881a(i)(1)(C) (providing that amended procedures must be reviewed under the same standard). 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 [50 U.S.C. §§] 1801(h) or 1821(4),” which is set out

⁶ Of course, targeting under the certifications filed in the Prior 702 Dockets will no longer be permitted once b(1) and b(3) take effect.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

in full in Subpart B below. Finally, the Court must determine whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A).

A. The NSA and FBI Targeting Procedures Meet the Statutory Requirements.

The NSA and FBI targeting procedures included as Exhibits A and C, respectively, to the August 24 Submission differ in several respects from the corresponding procedures that have previously been approved by the Court. The government has edited Sections II and IV of the NSA targeting procedures, which address “Post-Targeting Analysis by NSA” and “Oversight and Compliance,” respectively. Section II.b of the targeting procedures describes the process used by NSA to determine when collection on a tasked electronic communications facility (e.g., an e-mail account) must stop because a user of the facility has entered the United States. See Amended NSA Targeting Procedures at 6 (§ II.b). The changes, which are clarifying rather than substantive in nature, serve the purpose of describing this process more precisely. The revised provision is consistent with the government’s prior representations to the Court regarding NSA’s post-targeting analysis and presents no difficulty under Section 1881a(d). See Docket Nos.

(b)(1) and (b)(3) June 2, 2010 Mem. Op. at 19-23.

The government has made three changes to Section IV of the NSA targeting procedures. First, the provision has been amended to require NSA to “implement a compliance program” and “conduct ongoing oversight, with respect to its exercise of the authority under section 702 of the Act, including the associated targeting and minimization procedures adopted in accordance with Section 702.” Amended NSA Targeting Procedures at 7 (§ IV). The addition of this undertaking

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

obviously raises no issue under Section 1881a(d). Second, the government has replaced several references to particular components of NSA in Section IV with references to NSA generally. Id. at 7-8 (§ IV). This change has the effect of making the entire agency, rather than any particular component, responsible for ensuring adherence to particular oversight and compliance requirements set forth in the procedures. Because this change does not alter what must be done, it also presents no concern for the Court under Section 1881a(d). Third, no issue is presented by changing the required frequency for oversight reviews by the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) “at least once every sixty days,” see Docket No. [REDACTED] NSA Targeting Procedures at 8 (§ IV), to “approximately once every two months,” see Amended NSA Targeting Procedures at 8 (§ IV).

The government has made only one change to the FBI targeting procedures that have previously been approved by the Court. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] See Amended FBI Targeting Procedures at 2 (§ I.4). [REDACTED]

[REDACTED] his alteration does not result in any substantive change and, therefore, presents no issue under Section 1881a(d)(1).

For the reasons stated above and in the Court’s opinions in the Prior 702 Dockets, the Court concludes that the revised NSA and FBI targeting procedures are reasonably designed: (1) to ensure that any acquisition authorized under Certifications [REDACTED] is

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

limited to targeting persons reasonably believed to be located outside the United States, and (2) 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, as required by Section 1881a(d).

B. All Four Sets of Minimization Procedures Satisfy the Statutory Requirements.

The NSA, FBI, and CIA minimization procedures attached as Exhibits B, D, and E of the August 24 Submission differ in some respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications b(1) and b(3)

b(1) and b(3) The NCTC minimization procedures included as Exhibit G to the August Submission are entirely new.

As noted above, the Court must determine whether these procedures meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) and 1821(4). See 50 U.S.C. § 1881a(e)(1). The definitions at Sections 1801(h) and 1821(4) are substantively identical for present purposes and define “minimization procedures” in pertinent part as:

(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 [or physical search], 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;[⁷]

⁷ Section 1801(e) defines “foreign intelligence information” as

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –

(continued...)

~~TOP SECRET//SI//ORCON,NOFORN~~

Page 9

~~TOP SECRET//SI//ORCON,NOFORN~~

(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); see also *id.* § 1821(4).⁸ For the reasons set forth below, the Court concludes that the minimization procedures filed as part of the August 24 Submission satisfy this definition, as required by 50 U.S.C. § 1881a(e).

⁷(...continued)

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or a foreign territory that relates to, and if concerning a United States person is necessary to –

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

⁸ The definitions of “minimization procedures” set forth in these provisions are substantively identical (although Section 1821(4)(A) refers to “the purposes . . . of the particular physical search”) (emphasis added). For ease of reference, subsequent citations refer only to the definition set forth at Section 1801(h).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

I. *The CIA Minimization Procedures.*

The government has made several changes to the CIA minimization procedures.

Queries of Section 702 Information. The government has modified Section 4, which addresses the querying by CIA of information collected pursuant to Section 702. Like the previously-approved provision, the revised provision still generally requires that CIA queries of Section 702 information be “reasonably designed to find and extract foreign intelligence information”; that CIA keep records of such queries; and that DOJ and ODNI review the query records. See Amended CIA Minimization Procedures at 3 (§ 4). However, new qualifying language in the amended provision states that notwithstanding these general requirements, CIA personnel may: (1) “query CIA electronic and data storage systems that contain metadata to find, extract, and analyze metadata⁹ pertaining to communications”; (2) “use such metadata to analyze communications”; (3) “upload or transfer some or all such metadata to other CIA electronic and data storage systems for authorized foreign intelligence purposes”; and (4) “disseminat[e] . . . metadata from communications acquired under Section 702 of the Act . . . in accordance with the applicable provisions of these procedures.” Id. (§ 4.a).

The FBI Minimization Procedures previously approved by the Court contain a similar provision for metadata queries. See, e.g., Docket No. b(1) and b(3) FBI Minimization Procedures at 16 (§ 3.D (“Retention - Queries of Electronic and Data Storage Systems

⁹ The procedures provide that “‘metadata’ is dialing, routing, addressing, or signaling information associated with a communication, but does not include information concerning the substance, purport, or meaning of the communication.” Amended CIA Minimization Procedures at 1 (§ 1.c).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

Containing Raw FISA-acquired Information”)). b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED]

[REDACTED] b(1) and b(3)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Section 4 of the CIA minimization procedures has also been modified to clarify that for purposes of the procedures, “the term query does not include a user’s search or query of a CIA electronic and data storage system that contains raw FISA-acquired information, where the user does not receive the underlying raw FISA-acquired information in response to the search or otherwise have access to the raw FISA-acquired information that is searched.” Amended CIA Minimization Procedures at 3 (§ 4.b). This addition to Section 4 clarifies that a search that merely notifies the querying analyst of the existence of responsive Section 702 information – without actually providing access to the information itself – is not subject to the general querying restrictions of Section 4. Because this addition does not affect the circumstances under which CIA may acquire, retain, or disseminate U.S.-person information, it presents no concern under Section 1801(h).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

Oversight Functions and Vulnerability Assessments. The government has also added two new provisions to Section 6 of the CIA minimization procedures. The first provides that nothing in the procedures prohibits the performance of “lawful oversight functions” by CIA itself, or by DOJ, ODNI, or the “applicable Offices of the Inspectors General.” Amended CIA Minimization Procedures at 4 (§6.f). The new language merely makes explicit that the procedures should not be read to obstruct or hinder lawful and appropriate oversight functions. The Court has previously approved a similar provision in the Section 702 context. The previously-approved FBI minimization procedures, for instance, include a provision stating b(1), b(3), and b(7)(E)

b(1) and b(3) Docket No. b(1) and b(3), FBI Minimization Procedures at 3 (§ I.F). The new CIA provision is broader, insofar as it expressly contemplates that certain agencies outside of CIA may perform oversight functions and in so doing could conceivably receive U.S. person information. The Court is satisfied, however, that limited disclosure of information to these recipients in order for them to discharge their oversight responsibility does not run afoul of Section 1801(h).

The second new component of Section 6 states that nothing in the procedures prevents CIA from conducting “vulnerability assessments using information acquired pursuant to Section 702 of the Act in order to ensure that CIA systems have not been compromised.” Amended CIA Minimization Procedures at 4 (§ 6.g). This language allows CIA to use information collected under Section 702 in efforts to prevent its information systems from being compromised by malware or other similar threats and to detect and remedy intrusions after they have occurred. The new language states that Section 702 information used for vulnerability assessments may be

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

“retained for one year solely for that limited purpose,” and “may be disseminated only in accordance with the applicable provisions of these procedures.” *Id.* at 4-5 (§ 6.g). This provision changes nothing about the circumstances in which CIA may acquire or disseminate Section 702 information. Though the new provision broadens CIA’s authority to retain certain Section 702 information, including U.S. person information, the resulting change is modest in scope. Furthermore, the new provision is narrowly tailored to serve an important national security purpose; maintaining the integrity of CIA’s systems is essential to the agency’s fulfillment of its mission to produce, obtain, and disseminate foreign intelligence information. This amendment is consistent with Section 1801(h).

Waiver of Destruction Requirement. Finally, the government has made a minor change to Section 8 of the CIA minimization procedures. Section 8 generally requires the CIA to destroy any communication that is acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-U.S. person located outside the United States, but who was in fact, at the time of acquisition, a U.S. person or a person located in the United States. Amended CIA Minimization Procedures at 7 (§ 8). The Director of the CIA may waive the destruction requirement for such a communication by making a specific determination in writing that the communication contains significant foreign intelligence information or evidence of a crime. *Id.* New language further clarifies that such waiver determinations must be made “on a communication-by-communication” basis. *Id.* This further specification of the waiver process presents no issue under Section 1801(h).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

2. *The FBI and NCTC Minimization Procedures.*¹⁰

Presumptions Regarding U.S. Person Status. The government has altered the language of the FBI minimization procedures regarding when it is appropriate [REDACTED]

[REDACTED] Under the previously-approved procedures, [REDACTED]

[REDACTED] the procedures require the FBI to [REDACTED]

[REDACTED] See

Docket No. [REDACTED] FBI Minimization Procedures at 2 (§ I.C). However, the previously-approved procedures permitted the FBI to [REDACTED] See

id. at 3 (§ I.C). The amended procedures adopt a uniform rule that allows the FBI [REDACTED]

[REDACTED]

[REDACTED] Amended FBI Minimization Procedures at 2-3 (§ I.D).

This change brings the FBI minimization procedures into line with [REDACTED]

¹⁰ The FBI minimization procedures previously submitted by the government and approved by the Court consist of a copy of the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search, modified in a number of respects by a three-page cover document. *See, e.g.*, Docket No. [REDACTED] Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amendment Certifications, Exh. D (filed Apr. 22, 2011). Although the amended FBI minimization procedures are substantively similar in many respects to the previously-approved procedures, the amended procedures consist of a single, self-contained document that does not resort to cross-referencing. This formatting change reduces the risk of confusion and mistake and serves to bring the procedures into conformity with the FISC rules, which now restrict cross-referencing in procedures submitted to the Court for review. *See* FISC Rule 12 (adopted Nov. 1, 2010).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] See, e.g., Docket No. [REDACTED] Oct. 31, 2011 [REDACTED] b(1), b(3), and b(7)(E)

[REDACTED]. In the context of acquisitions that are directed at non-U.S. persons located outside the United States, the Court concludes that this change to the FBI minimization procedures, [REDACTED] b(1), b(3), and b(7)(E) comports with the definition of minimization procedures set forth at Section 1801(h).

[REDACTED] b(1), b(3), and b(7)(E) The government has added language providing that notwithstanding the remainder of the procedures, [REDACTED] (1), b(3), and b(7)(E)

[REDACTED]

[REDACTED] Amended FBI Minimization Procedures at 3 (§ I.G). Like the similar provision of the amended CIA minimization procedures that is discussed above, this new provision of the FBI procedures is narrowly tailored to serve its purpose. See *id.* at 3-4 (§I.G) [REDACTED] b(1), b(3), and b(7)(E)

[REDACTED] The Court similarly finds that this change to the FBI procedures is consistent with the requirements of Section 1801(h).¹¹

[REDACTED] b(7)(E) The government has modified the previously-

¹¹ The government has also broadened Section I.G to include “lawful oversight” of the FBI by DOJ, ODNI, and “applicable Offices of the Inspectors General,” in addition to oversight by the FBI itself. See Amended FBI Minimization Procedures at 3 (§ I.G). Like the similar amendment to the CIA minimization procedures discussed above, this change presents no issue under Section 1801(h).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

approved provision regarding FBI queries of information acquired under Section 702. [REDACTED]

[REDACTED]

[REDACTED] Amended FBI Minimization Procedures at 11

(§ III.D). [REDACTED]

[REDACTED]

[REDACTED] See *id.* Like the similar change to the CIA minimization procedures discussed above, this change presents no issue under Section 1801(h).

[REDACTED] The government has deleted the provisions of the FBI minimization procedures limiting the acquisition and use of [REDACTED] See Docket No. [REDACTED] FBI Minimization Procedures at 8-9 (§ 2.C); *id.* at 13-14 (§ III.C.2). In the context of telephone and Internet communications, the term [REDACTED]

[REDACTED]

[REDACTED] See *id.* at 8-9 (§ 2.C). The Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search limit the circumstances in which such communications can be retained and used for investigative or analytical purposes. See Docket No. [REDACTED] Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search at 13-14 (§ III.C.2) (as approved by the FISC on May 18, 2012). Although the same restrictions appear in prior versions of the FBI's Section 702 minimization procedures, they have no practical effect because

[REDACTED]

See Docket No. [REDACTED]

FBI Minimization Procedures, Cover Document at 1. In light of that definition (which is retained

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

in the amended procedures¹²), there are no [redacted] for the FBI to minimize. Because the deletion of the provisions regarding [redacted] does not alter the manner in which the FBI acquires, retains, or disseminates Section 702 information, this change is not problematic under Section 1801(h).¹³

[redacted] The government has added a new provision to the FBI minimization procedures requiring the FBI to [redacted].
[redacted] See Amended FBI Minimization Procedures at 9-10 (§ III.C.2). This change obviously presents no issue under Section 1801(h).

[redacted] The government has made a minor change to the [redacted] provision set forth in the final paragraph of Section III.A of the amended FBI minimization procedures. This provision, [redacted] generally requires the FBI to remove from its systems any communication that is acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-U.S. person located outside the United States but who is located inside the United States at the time of acquisition or is subsequently determined to be a U.S. person. See Amended FBI Minimization Procedures at 6 (§ III.A). The Director or Deputy Director of the FBI may

¹² See Amended FBI Minimization Procedures at 2 (§ I.B.3) [redacted]
[redacted]

¹³ The Court reaches this conclusion with the understanding the FBI does not acquire, either directly or through NSA, so-called “about” communications – i.e., communications that are not to or from a tasked facility but merely contain a reference to a tasked facility. Certain “about” communications are acquired by NSA through its upstream collection of Internet communications, the fruits of which are not shared with FBI or CIA in unminimized form. See Nov. 30 Op., *supra*, at 7 n.3.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

[REDACTED] by making a specific determination in writing that [REDACTED] b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED]

[REDACTED] Id. The amended provision contains new language further clarifying that [REDACTED] b(1), b(3), and b(7)(E) must be made

[REDACTED] b(1), b(3), and b(7)(E) basis. [REDACTED] b(1), b(3), and b(7)(E)

[REDACTED] this amendment to the FBI procedures does not alter the requirements of the [REDACTED] b(1), b(3), and b(7)(E) and therefore presents no issue under Section 1801(h).

[REDACTED] b(1), b(3), b(7)(E) The amended FBI minimization procedures retain a previously-approved provision requiring that [REDACTED] FBI b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED]

Amended FBI Minimization Procedures at 19 (§ III.G.1.a). However, new language provides

that an AD (or his superior) can [REDACTED] b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED] Id. The amended provision further states that [REDACTED] b(1), b(3), and b(7)(E)

[REDACTED]

[REDACTED] Id. This change limits the FBI's discretion to [REDACTED] b(1), b(3), and b(7)(E) Section 702 information and, therefore, presents no concern under Section 1801(h).

[REDACTED] b(1), b(3), b(7)(E) The amended FBI minimization procedures retain the

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

previously-approved requirements for [REDACTED], with one minor change. See Amended FBI Minimization Procedures at 12-16 (§ III.E). The previously-approved minimization procedures require that, when the FBI determines that [REDACTED]

[REDACTED] has been identified, the FBI shall [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
Docket No. [REDACTED], FBI Minimization Procedures at 18 (§ III.E.1.c) & 20 (§ III.E.2.c). The amended FBI Minimization Procedures require the FBI to [REDACTED]

[REDACTED] See Amended FBI Minimization Procedures at 12-13 (§ III.E.1.c) & 14 (§ III.E.2.c). The Court recently approved identical changes to the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search. See Docket Numbers [REDACTED] May 18, 2012 Mem. Op. and Order (“May 18 Opinion”) at 18-19. The Court sees no reason to reach a different result here, in the context of collection that is directed at non-U.S. persons located outside the United States and, therefore, less likely to [REDACTED]

Dissemination. The dissemination provisions of the FBI minimization procedures reflect a number of changes from the previously-approved procedures. Three of these changes conform the Section 702 minimization procedures to the dissemination provisions of the recently-revised Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search:

- The amended FBI minimization procedures [REDACTED]

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

b(1), b(3), and b(7)(E)
[Redacted]
[Redacted] Amended FBI Minimization Procedures at 21 (§ IV.A) (emphasis added).

• With regard to foreign governments, the amended FBI minimization procedures explicitly b(1), b(3), and b(7)(E) [Redacted]. See Amended FBI Minimization Procedures at 22-24 (§ IV.C).

• The amended FBI minimization procedures b(1), b(3), and b(7)(E) [Redacted]. The previously-approved procedures state that the FBI b(1), b(3), and b(7)(E) [Redacted]. See Docket No. b(1) and b(3) FBI Minimization Procedures at 27 (§ IV.A) (emphasis added).¹⁴ In contrast, the amended procedures b(1), b(3), and b(7)(E) [Redacted]. Amended FBI Minimization Procedures at 21 (§ IV.A) (emphasis added). As discussed in the May 18 Opinion, b(1), b(3), and b(7)(E) [Redacted]. See May 18 Op. at 14-15.¹⁵

¹⁴ Section IV.A of the previously-approved FBI minimization procedures further provides that b(1), b(3), and b(7)(E) [Redacted] (Emphasis added.) This language is stricken by the amendments to the FBI procedures and rendered superfluous by b(1), b(3), and b(7)(E) [Redacted].

¹⁵ The amendments to the FBI procedures also replace certain references to b(1), b(3), and b(7)(E) [Redacted]. Compare, e. g., Docket No. [Redacted] FBI Minimization Procedures at 30-31 (§ IV.D), with Amended FBI Minimization Procedures at 24 (§ IV.D). The government advises that this change in terminology is not (continued...)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

For the reasons set forth in the May 18 Opinion approving the same modifications to the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search, the Court concludes that these changes to the amended FBI minimization procedures for Section 702 acquisitions also are consistent with the requirements of Section 1801(h). In reaching this conclusion, the Court relies upon the same Executive Branch representations on which it relied in the May 18 Opinion.

The amended FBI minimization procedures contain a new provision permitting the FBI, in the event Section 702 information **b(1), b(3), and b(7)(E)**

[REDACTED]

[REDACTED]

[REDACTED] Amended FBI Minimization

Procedures at 26 (§ IV.H). This provision closely tracks language that the Court has approved as a supplemental minimization procedure in numerous orders granting authority to conduct

electronic surveillance and physical search in cases **b(1), b(3), and b(7)(E)**

[REDACTED] See, e.g., Docket No. **b(1) and b(3)** Primary Order and Warrant at 10.

The Court sees no issue under Section 1801(h) with the inclusion of such a provision in the Section 702 minimization procedures.

Finally, the amended FBI minimization procedures **b(7)(E)**

[REDACTED] **b(1), b(3), and b(7)(E)**

¹⁵(...continued)
intended to have any substantive effect. See May 18 Op. at 13 n.23.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

b(1), b(3), and b(7)(E)

[Redacted]

[Redacted] Amended FBI Minimization Procedures at 26 (§ IV.G) b(7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

NCTC is “the primary organization in the United States Government for analyzing and integrating all intelligence . . . pertaining to terrorism and counterterrorism,” excepting exclusively domestic matters. 50 U.S.C. § 404o(d)(1). Its responsibilities include “ensur[ing] that agencies, as appropriate, have access to and receive all-source intelligence support needed to execute their counterterrorism plans” and “disseminat[ing] terrorism information, including current terrorism threat analysis, to the President” and other executive branch officials, as well as “the appropriate committees of Congress.” § 404o(d)(4), (f)(1)(D). It also has “primary responsibility within the United States Government for conducting net assessments of terrorist threats.” § 404o(f)(1)(G).

Pursuant to an order issued in 2008, NCTC was authorized to receive certain FISA-

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

derived information from terrorism cases that FBI had uploaded to its [redacted] does not contain raw FISA information. Rather, it contains FBI investigative reports and other work product, some of which contain FISA information. As a result, FISA-derived information regarding U.S. persons that NCTC personnel can access [redacted] has already been subject to minimization by the FBI. The Court approved procedures in 2008 that permit the FBI to [redacted]

[redacted]
[redacted]
[redacted]

[redacted] Docket No. [redacted] Oct. 8, 2008 Mem. Op. at 3-6. The Court found that [redacted]

[redacted]. *Id.* at 3.

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

See Docket No. [redacted] [redacted]

¹⁶ [redacted]

(continued...)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

The new Section IV.G of the amended Section 702 FBI minimization procedures and the new NCTC minimization procedures are consistent with the requirements of Section 1801(h). In light of NCTC's important role in analyzing and processing intelligence regarding terrorism and counterterrorism, providing it with access to terrorism- and counterterrorism-related information in FBI general indices is consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information, as required by Section 1801(h)(1). Given the non-U.S. person, overseas focus of Section 702 collection, the information at issue b(1), b(3) and b(7)(E) to contain U.S. person information that is not foreign intelligence information as defined in Section 1801(e)(1), which is the principal concern of Section 1801(h)(2). Finally, the FBI will have applied its own minimization procedures to the information at issue here before it is shared with NCTC, and those procedures allow the dissemination of evidence of a crime for law enforcement purposes. See Amended FBI Minimization Procedures at 22-24 (§ IV.B & C). Accordingly, the Court is satisfied that the FBI and NCTC minimization procedures, taken together, permit the dissemination of evidence of a crime for law enforcement purposes, as required by Section 1801(h)(3).

3. *The NSA Minimization Procedures.*

The NSA minimization procedures have been altered in a number of respects. Before addressing the changes, some background discussion is warranted.

¹⁶(...continued)

b(1), b(3), and b(7)(E)

The amended FBI procedures at issue here do not permit the sharing of unminimized Section 702 information with NCTC.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

a. *The Scope of NSA's Upstream Collection.*

Last year, following the submission of Certifications ~~(b)(1) and b(3)~~ for renewal, the government made a series of submissions to the Court disclosing that it had materially misrepresented the scope of NSA's "upstream collection" under Section 702 (and prior authorities including the Protect America Act). The term "upstream collection" refers to the acquisition of Internet communications as they transit the "internet backbone" facilities ~~(b)(1) and b(3)~~ as opposed to the collection of communications directly from Internet service providers like ~~(b)(1) and b(3)~~. See Docket Nos. ~~(b)(1) and b(3)~~ ~~(b)(1) and b(3)~~ Oct. 3, 2011 Memorandum Opinion ("Oct. 3 Op.") at 5 n.3. Since 2006, the government had represented that NSA's upstream collection only acquired discrete communications to or from a facility tasked for acquisition and communications that referenced the tasked facility (so-called "about" communications). See *id.* at 15-16. With regard to the latter category, the government had repeatedly assured the Court that NSA only acquired ~~(b)(1)~~ specific categories of "about" communications. *Id.*

The government's 2011 submissions made clear, however, that NSA's upstream collection was much broader than the government had previously represented. For the first time, the government explained that NSA's upstream collection results in the acquisition of "Internet transactions" instead of discrete communications to, from or about a tasked selector. See *id.* at 15. Internet transactions, the government would ultimately acknowledge, could and often do contain multiple discrete communications, including wholly domestic non-target communications and other non-target communications to, from, or concerning U.S. persons. *Id.*

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

While the government was able to show that the percentage of wholly domestic non-target communications and other non-target communications to, from, or concerning U.S. persons being acquired was small relative to the total volume of Internet communications acquired by the NSA pursuant to section 702, the acquisition of such communications nonetheless presented a significant issue for the Court in reviewing the procedures. In fact, it appeared that NSA was annually acquiring tens of thousands of Internet transactions containing at least one wholly domestic communication; that many of these wholly domestic communications were not to, from, or about a targeted facility; and that NSA was also likely annually acquiring tens of thousands of additional Internet transactions containing one or more non-target communications to or from U.S. persons or persons in the United States. *Id.* at 33, 37.

In the October 3 Opinion, the Court approved in large part Certifications b(1) and b(3) and the accompanying targeting and minimization procedures. The Court concluded, however, that one aspect of the proposed collection – NSA’s upstream collection of Internet transactions containing multiple communications, or “MCTs” – was, in some respects, deficient on statutory and constitutional grounds. The Court concluded that although NSA’s targeting procedures met the statutory requirements, the NSA minimization procedures, as the government proposed to apply them to MCTs, did not satisfy the statutory definition of “minimization procedures” with respect to retention. Oct. 3 Op. at 59-63. As applied to the upstream collection of Internet transactions, the Court found that the procedures were not reasonably designed to minimize the retention of U.S. person information consistent with the government’s national security needs. *Id.* at 62-63. The Court explained that the net effect of the

~~TOP SECRET//SI//ORCON,NOFORN~~

THIS PAGE WAS RELEASED IN FULL

~~TOP SECRET//SI//ORCON,NOFORN~~

procedures would have been that thousands of wholly domestic communications, and thousands of other discrete communications that are not to or from a targeted selector but that are to, from, or concerning United States persons, would be retained by NSA for at least five years, despite the fact that they have no direct connection to a targeted selector and, therefore, were unlikely to contain foreign intelligence information. *Id.* at 60-61. For the same reason, the Court concluded that NSA's procedures, as the government proposed to apply then to MCTs, failed to satisfy the requirements of the Fourth Amendment. *Id.* at 78-79. The Court noted that the government might be able to remedy the deficiencies that it had identified, either by tailoring its upstream acquisition or by adopting more stringent post-acquisition safeguards. *Id.* at 61-62, 79.

By operation of the statute, the government was permitted to continue the problematic portion of its collection for 30 days while taking steps to remedy the deficiencies identified in the October 3 order and opinion. *See* 50 U.S.C. § 1881a(i)(3)(B). In late October of 2011, the government timely submitted amended NSA minimization procedures that included additional provisions regarding NSA's upstream collection. The amended procedures, which took effect on October 31, 2011 ("Oct. 31, 2011 NSA Minimization Procedures"), require NSA to restrict access to the portions of its ongoing upstream collection that are most likely to contain wholly domestic communications and non-target information that is subject to statutory or Fourth Amendment protection. *See* Nov. 30 Op. at 7-9. Segregated Internet transactions can be moved to NSA's general repositories only after having been determined by a specially trained analyst not to contain a wholly domestic communication. *Id.* at 8. Any transaction containing a wholly domestic communication (whether segregated or not) would be purged upon recognition. *Id.* at

~~TOP SECRET//SI//ORCON,NOFORN~~

Page 28

THIS PAGE WAS RELEASED IN FULL

ER 824

THIS PAGE WAS RELEASED IN FULL

~~TOP SECRET//SI//ORCON,NOFORN~~

8, 9. Any transaction moved from segregation to NSA's general repositories would be permanently marked as having previously been segregated. *Id.* at 8. On the non-segregated side, any discrete communication within an Internet transaction that an analyst wishes to use is subject to additional checks. *Id.* at 8-10. NSA is not permitted to use any discrete, non-target communication that is determined to be to or from a U.S. person or a person who appears to be in the United States, other than to protect against an immediate threat to human life. *Id.* at 9. Finally, all upstream acquisitions are retained for a default maximum period of two, rather than five, years. *Id.* at 10-11.

The Court concluded in the November 30 Opinion that the October 31, 2011 NSA Minimization Procedures adequately remedied the deficiencies that had been identified in the October 3 opinion. *Id.* at 14-15. Accordingly, NSA was able to continue its upstream collection of Internet transactions (including MCTs) without interruption, but pursuant to amended procedures that are consistent with statutory and constitutional requirements.

However, issues remained with respect to the past upstream collection residing in NSA's databases. Because NSA's upstream collection almost certainly included at least some acquisitions constituting "electronic surveillance" within the meaning of 50 U.S.C. § 1801(f), any overcollection resulting from the government's misrepresentation of the scope of that collection implicates 50 U.S.C. § 1809(a)(2). Section 1809(a)(2) makes it a crime to "disclose[] or use[] 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 Court therefore directed the government to make a written submission addressing

~~TOP SECRET//SI//ORCON,NOFORN~~

Page 29

THIS PAGE WAS RELEASED IN FULL

~~TOP SECRET//SI//ORCON,NOFORN~~

the applicability of Section 1809(a), which the government did on November 22, 2011. See Docket No. [REDACTED] Oct. 13, 2011 Briefing Order, and Government's Response to the Court's Briefing Order of Oct. 13, 2011 (arguing that Section 1809(a)(2) does not apply).

Beginning late in 2011, the government began taking steps that had the effect of mitigating any Section 1809(a)(2) problem, including the risk that information subject to the statutory criminal prohibition might be used or disclosed in an application filed before this Court. The government informed the Court in October 2011 that although the amended NSA procedures do not by their terms apply to information acquired before October 31, NSA would apply portions of the procedures to the past upstream collection, including certain limitations on the use or disclosure of such information. See Nov. 30 Opinion at 20-21. Although it was not technically feasible for NSA to segregate the past upstream collection in the same way it is now segregating the incoming upstream acquisitions, the government explained that it would apply the remaining components of the amended procedures approved by the Court to the previously-collected data, including (1) the prohibition on using discrete, non-target communications determined to be to or from a U.S. person or a person in the United States, and (2) the two-year age-off requirement. See id. at 21.

Thereafter, in April 2012, the government orally informed the Court that NSA had made a "corporate decision" to purge all data in its repositories that can be identified as having been acquired through upstream collection before the October 31, 2011 effective date of the amended NSA minimization procedures approved by the Court in the November 30 Opinion. NSA's

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

effort to purge that information, to the extent it is reasonably feasible to do so, is now complete.

See Aug. 24 Submission at 9-10.¹⁷

Finally, NSA has adopted measures to deal with the possibility that it has issued reports based on upstream collection that was unauthorized. NSA has identified ~~(b)(1) and (b)(3)~~ reports that were issued from the inception of its collection under Section 702 to October 31, 2011, that rely at least in part on information derived from NSA's upstream acquisitions from that period. See Sept. 12, 2012 Supplement to the Government's Ex Parte Submission of Reauthorization Certifications at 2 ("Sept. 12 Submission"). The government advises that, of the ~~(b)(1) and (b)(3)~~ reports, ~~(b)(1)~~ have been confirmed to be based entirely upon communications that are to, from or about persons properly targeted under Section 702 and therefore present no issue under Section 1809(a)(2). See id. The government is unable to make similar assurances, however, regarding the remaining ~~(b)(1)~~ reports. Accordingly, NSA will direct the recipients of those ~~(b)(1)~~ reports (both within NSA and outside the agency) not to further use or disseminate information contained therein without first obtaining NSA's express approval. Id. at 3-4. Upon receipt of such a request, NSA will review the relevant report to determine whether continued use thereof is

¹⁷ The government has informed the Court that NSA stores some of the past upstream collection in repositories in which it may no longer be identifiable as such. ~~(b)(1) and (b)(3)~~

~~(b)(1) and (b)(3)~~. See Aug. 24 Submission at 14-16. Assuming that NSA cannot with reasonable effort identify information in its repositories as the fruit of an unauthorized electronic surveillance, such information falls outside the scope of Section 1809(a)(2), which by its terms applies only when there is knowledge or "reason to know that the information was obtained through electronic surveillance not authorized" by statute.

~~TOP SECRET//SI//ORCON,NOFORN~~

THIS PAGE WAS RELEASED IN FULL

~~TOP SECRET//SI//ORCON,NOFORN~~

appropriate. *Id.* at 4.¹⁸ Finally, the government has informed the Court that it will not use any report that cites to upstream collection acquired prior to October 31, 2011 in an application to this Court absent express notice to, and approval of, the Court. Aug. 24 Submission at 24.

Taken together, the remedial steps taken by the government since October 2011 greatly reduce the risk that NSA will run afoul of Section 1809(a)(2) in its handling of the past upstream acquisitions made under color of Section 702. NSA's self-imposed prohibition on using non-target communications to or from a U.S. person or a person in the United States helped to ensure that the fruits of unauthorized electronic surveillance were not used or disclosed while it was working to purge the pre-October 31, 2011 upstream collection. And NSA's subsequent purge of that collection from its repositories and the above-described measures it has taken with respect to derivative reports further reduce the risk of a problem under Section 1809(a)(2). Finally, the amended NSA minimization procedures provide that in the event, despite NSA's effort to purge the prior upstream collection, the agency discovers an Internet transaction acquired before October 31, 2011, such transaction must be purged upon recognition. See Amended NSA Minimization Procedures at 8 § 3(c)(3). In light of the foregoing, it appears to the Court that the outstanding issues raised by NSA's upstream collection of Internet transactions have been resolved, subject to the discussion of changes to the minimization procedures that appears

¹⁸ For instance, NSA may determine that the report is fully supported by cited communications other than the ones obtained through upstream communication. Sept. 12 Submission at 4. In other instances, NSA may revise the report so that it no longer relies upon upstream communications and reissue it. *Id.* If such steps are not feasible because the report cannot be supported without the upstream communication, NSA will cancel the report. *Id.*

~~TOP SECRET//SI//ORCON,NOFORN~~

Page 32

THIS PAGE WAS RELEASED IN FULL

~~TOP SECRET//SI//ORCON,NOFORN~~

below.¹⁹

b. Changes to the NSA Minimization Procedures.

“Processing” versus “handling” information. In a number of places in the amended NSA minimization procedures, the government has replaced the term “processed” with the word “handled.” See Amended NSA Minimization Procedures at 9 (§ 5(1)) & 12 (§§ 6(c)(1) & 6(c)(2)). Both the previously-approved NSA minimization procedures and the amended procedures define the terms “processed” or “processing” to mean “any step necessary to convert a communication into an intelligible form intended for human inspection.” *Id.* at 2 (§ 2(h)). The previously-approved procedures did not uniformly use the terms in a manner consistent with that narrow definition. This clarifying change remedies that inconsistency by using the distinct term “handled” or “handling” to refer to the treatment of communications after they have been rendered intelligible for human inspection. This non-substantive change reduces the potential for confusion and mistake and raises no issue under Section 1801(h).

Oversight Functions. Like the amended CIA and FBI minimization procedures discussed above, the amended NSA minimization procedures contain language stating that the procedures do not restrict the exercise of “lawful oversight” of NSA by NSA itself, DOJ, ODNI, or “the applicable Offices of Inspectors General.” Amended NSA Minimization Procedures at 1 (§ 1). For the same reasons, the Court finds that this provision is consistent with Section 1801(h).

¹⁹ Under the circumstances, the Court finds it unnecessary to further address the arguments advanced by the government in its November 22, 2011 response to the Court’s October 13, 2011 briefing order regarding Section 1809(a), particularly those regarding the scope of prior Section 702 authorizations.

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

Vulnerability or Network Assessments. The amended NSA minimization procedures also state that the procedures do not restrict NSA's performance of "vulnerability or network assessments using information acquired pursuant to Section 702 . . . in order to ensure that NSA systems are not or have not been compromised." Amended NSA Minimization Procedures at 1 (§ 1). (b)(1), (b)(3), and (b)(7)(E)

[REDACTED], this "vulnerability or network assessments" language also raises no concern under Section 1801(h). The language allows NSA to use information collected under Section 702 in efforts to prevent its information systems from being compromised by malware or other similar threats and to detect and remedy intrusions after they have occurred. Maintaining the integrity of NSA's systems is essential to the agency's fulfillment of its national security mission, including the acquisition, production, and dissemination of foreign intelligence information. The new language is narrowly crafted to serve that purpose, stating that Section 702 information used for vulnerability or network assessments may be "retained for one year solely for that limited purpose," and "may be disseminated only in accordance with the applicable provisions of these procedures." *Id.* at 1 (§ 1).

Upstream Collection. The government has made several changes to Section 3(b) of the NSA minimization procedures, which, among other things, addresses NSA's handling of Internet transactions acquired through its upstream collection. Section (3)(b)(4)(a)²⁰ generally requires NSA to use technical means to segregate and restrict access to the two categories of MCTs that

²⁰ The government has renumbered portions of Section 3 so that the substance of Section 3(b)(5) of the previously-approved procedures now appears in Section 3(b)(4).

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

are most likely to contain non-target information concerning U.S. persons or persons in the United States. See Nov. 30, 2012 Mem. Op. at 11-12. The amended procedures include new language stating that notwithstanding this general segregation requirement, “NSA may process Internet transactions . . . in order to render such transactions intelligible to analysts.” See Amended NSA Minimization Procedures at 4 (§ 3(b)(4)(a)(1)). The Court’s understanding is that this new language permits NSA to render Internet transactions intelligible to humans before segregating them in accordance with Section 3(b)(4)(a). With the understanding that the procedures continue to preclude access to Internet transactions by intelligence analysts until after segregation (and even then, only in accordance with the remainder of the procedures), the Court is satisfied that this amendment is consistent with Section 1801(h).

The previously approved procedures required NSA to “destroy[] upon recognition” any Internet transaction containing a discrete wholly domestic communications (i.e., a communication as to which the sender and all intended recipients are reasonably believed to be in the United States). See Oct. 31, 2011 NSA Minimization Procedures at 4 § 3(b)(5)(a)(1)(a); see also Nov. 30, 2011 Mem. Op. at 9. The amended procedures state that Internet transactions recognized as containing a discrete wholly domestic communication must “be handled in accordance with Section 5 below.” Amended NSA Minimization Procedures at 4-5 (§§ 3(b)(4)(a)(2)(a), 3(b)(4)(b)(1)). Section 5 requires as a general rule that “a communication identified as a domestic communication (and if applicable the Internet transaction in which it is contained) will be promptly destroyed upon recognition.” Id. at 8 (§ 5). As explained below, however, Section 5 allows the Director of NSA to waive the destruction of a particular

~~TOP SECRET//SI//ORCON,NOFORN~~

Page 35

ER 831

~~TOP SECRET//SI//ORCON,NOFORN~~

communication under certain circumstances. Id. at 8-9 (§ 5). Accordingly, the effect of this amendment to Section 3(b) is to convert what was an absolute destruction requirement into a qualified destruction requirement. Nevertheless, as discussed below, the circumstances in which a Director's waiver may be granted are narrowly defined, so that the Court is satisfied that this amendment to the NSA minimization procedures is consistent with Section 1801(h).

Another change to Section 3(b) of the NSA minimization procedures involves metadata. The procedures approved by the Court in the November 30, 2011 Memorandum Opinion contain a provision allowing NSA to copy metadata from Internet transactions that are not subject to segregation pursuant to Section 3(b) without first complying with the other rules for handling non-segregated transactions – i.e., without ruling out that the metadata pertained to a discrete wholly domestic communication or to a discrete non-target communication to or from a U.S. person or a person inside the United States. See Nov. 30, 2011 Mem. Op. at 15-20. Metadata copied pursuant to this provision must be handled in accordance with the other provisions of the procedures. Id. at 16. Furthermore, in the event that NSA later identifies an Internet transaction as containing a wholly domestic communication, any metadata that has been extracted from that transaction must be destroyed. Id.

The amended procedures retain this provision, but now expressly limit it to Internet transactions acquired on or after October 31, 2011. Amended NSA Minimization Procedures at 6 (§ 3(b)(4)(b)(4)). This date change accounts for the fact that, as discussed above, NSA's upstream acquisitions before that date have been subject to an earlier set of minimization procedures that did not provide for the extraction and use of metadata by NSA. See Nov. 30,

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

2011 Mem. Op. at 20-21. The addition of the date makes clear that although the amended NSA minimization procedures now generally apply to Section 702 information acquired by NSA under all certifications, this metadata provision continues to apply only to information acquired under the 2011 and 2012 certifications. Because this amendment serves only to preserve the status quo with respect to metadata, it presents no issue under Section 1801(h).

Destruction of Raw Data. The government has amended Section 3(c) of the NSA minimization procedures, which limits the retention of raw Section 702 information acquired by NSA. Like the previously-approved procedures, the amended procedures provide a default retention period of two years for upstream Internet communications and a default retention period of five years for all other communications. See Amended NSA Minimization Procedures at 7 (§ 3(c)). The government has added language to Section 3(c) to make clearer that these retention limits are subject to separate provisions of the procedures, which may allow a particular communication to be retained longer – e.g., because it contains U.S. person-identifying information that is necessary to understand foreign intelligence information or assess its importance. See id. at 7 (§ 3(c)); id. at 10-11 (§ 6). New language also makes clear that the determination that a communication qualifies for retention beyond the default “age off” period must be made by NSA on a communication-by-communication basis and, in the case of Internet transactions, is subject to the special rules set forth in Section 3(b) of the procedures. Id. at 7 (§ 3(c)). These clarifying changes raise no issue under Section 1801(h).

The final change to Section 3(c) is new language requiring NSA to destroy upon recognition “[a]ny Internet transaction acquired through NSA’s upstream collection techniques

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

prior to October 31, 2011.” Amended NSA Minimization Procedures at 8 (§ 3(c)(3)). As discussed above, NSA has deleted “all data objects identified as acquired through NSA’s upstream Internet collection techniques on or before October 31, 2011.” See Aug. 24 Submission at 9. This new language formalizes NSA’s undertaking to destroy any additional information that is hererafter identified as having been acquired through its prior upstream Internet collection and presents no issue under Section 1801(h).

Waiver of Destruction Requirement. The previously-approved NSA minimization procedures generally require that NSA destroy upon recognition any communication that is defined as a domestic communication. Oct. 31, 2011 NSA Minimization Procedures at 8 (§ 5). Domestic communications include: (1) any communication that does not have at least one communicant outside the United States, see id. at 2 (§ 2(e)); (2) any communication acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communication was acquired, id. at 7 (§ 3(d)(2)); and (3) any communication acquired by targeting a person who at the time of targeting was believed to be a non-U.S. person but was in fact a U.S. person, id. The destruction requirement can be waived, however, if the Director or Acting Director of the NSA “specifically determines in writing” that:

- (1) the communication is “reasonably believed to contain significant foreign intelligence information,” in which case it can be “provided to the FBI (including United States person identities) for possible dissemination in accordance with its minimization procedures”;
- (2) the communication is “reasonably believed to contain evidence of a crime,” in which case it can be disseminated to appropriate federal law enforcement authorities and retained for a reasonable period of time to permit appropriate

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

access by law enforcement agencies;

(3) the communication is reasonably believed to contain information necessary to be retained for cryptanalytic, traffic analytic, or signal exploitation purposes, or information necessary to understand or assess a security vulnerability, in which case it can be obtained for a period sufficient to permit exploitation; or

(4) the communication contains information pertaining to a threat of serious harm to life or property.

See *id.* The previously-approved procedures further provide that notwithstanding these requirements: (1) “if a domestic communication indicates that a target has entered the United States, NSA may advise FBI of that fact”; and (2) NSA may retain and provide to FBI and CIA certain information deemed necessary “for collection avoidance purposes.” *Id.* at 9 (§ 5).

~~(b)(1), (b)(3), and (b)(7)(E)~~

~~_____~~, the government has amended Section 5 to further clarify that waivers may only be made on a “communication-by-communication basis.” See Amended NSA Minimization Procedures at 8 (§ 5). This change does not alter the requirements of the waiver provision and raises no concern under Section 1801(h).²¹

²¹ In October 2011, the government reported a compliance incident involving NSA’s application of Section 5. The incident was the subject of a more detailed follow-up submission made on August 28, 2012 (“Aug. 28 Submission”). As previously approved by the Court, Section 5 states that a waiver may occur only when “the Director (or Acting Director) specifically determines, in writing,” that one of the four enumerated criteria is met with respect to “[a] communication.” See, e.g., Oct. 31, 2011 NSA Minimization Procedures at 8 (§ 5). In accordance with this language, the government represented to the Court in 2008 that the waiver provision would be applied on a “case-by-case basis” rather than categorically. Docket No. ~~(b)(1) and (b)(3)~~ Aug. 27, 2008 Hrg. Tr. at 36-37. The Court relied on this representation in approving Section 5. Docket No. ~~(b)(1) and (b)(3)~~ Sept. 4, 2008 Mem. Op. at 25 n.24.

In March 2011, however, the Acting Director of NSA made an “advance waiver

(continued...)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

Another change to Section 5 is the addition of new language that limits the types of domestic communications that may be the subject of a destruction waiver. As amended, the provision requires the Director (or Acting Director) to specifically determine in writing not only that one of the four enumerated conditions is satisfied, but also that “the sender or intended recipient of the domestic communication had been properly targeted under Section 702 of the Act.” See Amended NSA Minimization Procedures at 8 (§ 5). The change has the practical effect of limiting the reach of the waiver provision to domestic communications acquired with the reasonable but mistaken belief that the target is a non-U.S. person located outside the United States. This narrowing amendment is consistent with the requirements of Section 1801(h).

A third change to Section 5 of the NSA minimization procedures broadens the effect of a waiver made on the ground that the communication at issue contains significant foreign intelligence information. While the previously-approved language of Section 5(1) states that a

²¹(...continued)

determination” pursuant to which NSA personnel could thereafter deem “certain terrorism-related communications that met specific criteria . . . to contain ‘significant foreign intelligence’ and hence . . . subject to a destruction waiver.” Aug. 28 Submission at 2. This advance waiver determination was relied upon seven times by NSA personnel until September 2011, when it was rescinded as inconsistent with the requirements of Section 5. Id. It was later determined, however, that in six of those instances no waiver was required. Id. After reporting the incident to the Court, DOJ and NSA undertook a review of NSA’s practice under Section 5 of the procedures. That review revealed that NSA has used the waiver provision on 16 other occasions and that each of those other waivers was consistent with the requirements of Section 5. Id. at 3. Furthermore, NSA, working together with DOJ, has undertaken a number of steps to improve coordination of guidance involving NSA’s FISA authorities (including Section 702) and is continuing to strengthen its internal compliance infrastructure. Id. at 3-6. In light of the corrective measures taken by the government following the “advance waiver determination” incident, the Court is satisfied that the incident does not preclude a finding that NSA’s minimization procedures satisfy the requirements of Section 1801(h).

~~TOP SECRET//SI//ORCON,NOFORN~~

Page 40

ER 836

~~TOP SECRET//SI//ORCON,NOFORN~~

communication retained on that basis can be “provided to the FBI . . . for possible dissemination in accordance with its minimization procedures,” Oct. 31, 2011 NSA Minimization Procedures at 8 (§ 5(1)), the amended provision states that such a communication “may be retained, handled, and disseminated in accordance with these procedures,” Amended NSA Minimization Procedures at 9 (§ 5(1)). The result of this change is that NSA may retain, use, and disseminate such a communication as if it constitutes a “foreign communication.” See Amended NSA Minimization Procedures at 10-12 (§§ 6-7) (setting forth rules for retention and dissemination of foreign communications). Read in isolation, this amendment appears to give NSA substantially more leeway to retain, use, and disseminate a domestic communication that is the subject of the waiver on “significant foreign intelligence” grounds. As discussed in the preceding paragraph, however, the waiver provision, as amended, now may be applied only to those domestic communications acquired with a reasonable, but mistaken, belief that the target is a non-U.S. person located outside the United States. The Court has previously recognized that Section 702 authorizes the government to acquire such communications. See Docket No. [REDACTED] Sept. 4, 2008 Mem. Op. at 25-26. Moreover, if a communication retained on this basis contains U.S.-person identifying information, that information must be deleted before the communication can be disseminated outside NSA unless one of eight specific exceptions applies. See Amended NSA Minimization Procedures at 11-12 (§ 6(b)). Under the circumstances, the Court is satisfied that this amendment to Section 5(1) of the NSA minimization procedures is consistent with Section 1801(h).

Another change to the NSA minimization procedures provides that in the event a

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

domestic communication subject to a waiver by the Director or Acting Director is contained within an Internet transaction, NSA may retain the entire transaction. See Amended Minimization Procedures at 9 (§ 5). This change addresses NSA's inability to disaggregate Internet transactions that it has acquired under Section 702 without destabilizing its systems. See Docket Nos. b(1) and b(3) Government's Response to the Court's Briefing Order of May 9, 2011 (filed June 1, 2012) at 22. The change permits NSA to retain not just the particular portion of an Internet transaction that is deemed to qualify for a waiver, but also other unrelated portions of the transaction within which it was acquired, which may include non-target U.S. person information with no foreign intelligence value. For several reasons, the Court is satisfied that this change is consistent with the requirements of Section 1801(h). First, NSA has only applied the waiver provision 16 times since Section 702 collection commenced in 2008. See Aug. 28 Submission at 2. Furthermore, as discussed above and in the November 30 Opinion, NSA's minimization procedures include special handling requirements for Internet transactions, including protections for non-target U.S. person information, that will apply to any transaction that is retained by NSA following a Section 5 waiver. Finally, the procedures require NSA to delete U.S.-person identifying information from a communication before disseminating it outside the agency, unless one of eight specific exceptions applies. See Amended NSA Minimization Procedures at 11-12 (§ 6(b)).

The final change to Section 5 involves what NSA may do, absent a Director's waiver, in the event that a domestic communication indicates that a target has entered the United States. The previously-approved procedures allow NSA to advise the FBI of the fact of the target's entry

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

into the United States and to retain and provide to FBI and CIA technical information about the communication for “collection avoidance purposes.” Oct. 31, 2011 NSA Minimization Procedures at 9 (§ 5). The amended procedures permit NSA not only to inform the FBI of the fact of the target’s entry into the United States and share with the FBI and CIA the same technical “collection avoidance” information, but also to provide to the FBI “any information concerning the target’s location that is contained in the communication.” Amended NSA Minimization Procedures at 10 (§ 5). In addition, the amended provision states that NSA “may retain the communication from which such information is derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL).” *Id.* This change to Section 5 allows NSA to share limited information with the FBI and serves to better facilitate the transition from Section 702 coverage of the target to other forms of surveillance or investigation that are permitted within the United States. The Court is satisfied that this amendment to the procedures is consistent with Section 1801(h).

C. The Targeting and Minimization Procedures Are Consistent with the Fourth Amendment.

The final question before the Court is whether the targeting and minimization procedures included as part of the August 24 Submission are consistent with the Fourth Amendment. *See* 50 U.S.C. § 1881a(i)(3)(A). Largely for the same reasons that the Court has concluded that the amended procedures meet the requirements of Section 1881a(d)-(e), the Court is also satisfied that the amended procedures are reasonable under the Fourth Amendment. The basic framework of protections formed by the previously-approved procedures remains intact. Many of the amendments made by the government add to those protections or merely serve to clarify what is

~~TOP SECRET//SI//ORCON,NOFORN~~

~~TOP SECRET//SI//ORCON,NOFORN~~

required of the government. The remaining changes do not individually or collectively alter the Court's prior conclusion that the targeting and minimization procedures are consistent with the Fourth Amendment.

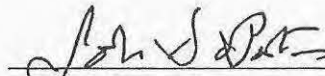
IV. CONCLUSION

For the foregoing reasons, the Court finds that the certifications and amendments submitted in the above-captioned dockets pursuant to Section 1881a(g) contain 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 subsections and with the Fourth Amendment.

Orders approving the certifications, the amendments, and the use of the accompanying procedures are being entered contemporaneously herewith.

ENTERED this 20th day of September 2012, in Docket Nos. b(1) and b(3)

b(6), b(7)(C)



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

b(6), b(7)(C)

~~TOP SECRET//SI//ORCON,NOFORN~~

~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

b(1) and b(3)



ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications referenced above contain all the required elements and that the targeting procedures and minimization procedures approved for use in connection with those certifications are consistent with 50 U.S.C. §1881a(d)-(e) and with the Fourth Amendment.

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications and the use of such procedures are approved.

ENTERED this 20th day of September 2012, at _____ Eastern Time, in

09-20-2012 09:56

Docket Nos. _____

b(1) and b(3)





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

b(6), b(7)(C)



~~SECRET~~

~~SECRET~~

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

b(1) and b(3)



ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance upon the entire record in this matter, the Court finds, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the certifications referenced above, as amended on August 23, 2012, contain all the required elements and that the targeting procedures and minimization procedures approved for use in connection with those amended certifications are consistent with the requirements of 50 U.S.C. §1881a(d)-(e) and with the Fourth Amendment.

~~SECRET~~

~~SECRET~~

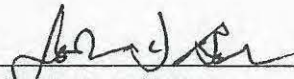
Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that the amended certifications and the use of such procedures are approved.

09-20-2012 P05:56

ENTERED this 25th day of September 2012, at _____ Eastern Time, in

Docket Nos.

b(1) and b(3)
[Redacted]



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

b(6), b(7)(C)
[Redacted]

~~SECRET~~