UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

Docket Number: PR/TT [redacted]

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 metadata[1] about Internet communications. The government's application also seeks Court authorization to query and use information previously obtained by NSA, regardless of whether the information was authorized to be acquired under

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

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

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

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

[redacted]

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]

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] See [redacted] Opinion at 72-80.[5] When known, the particular customers [redacted] were identified in the Court's order pursuant to 50 U.S.C. § 1842(d)(2)(A)(ii). See [redacted] Opinion at 22-23.

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

[redacted]

[redacted]

The government proposed to collect these categories of metadata from [redacted]

[redacted]

[redacted]

[redacted]

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]

[redacted]

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

---

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

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

It was anticipated that the authorized PR/TT surveillance would "encompass [redacted] 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] 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.

([redacted] 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. [redacted] 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 [redacted] communications," at least as compared with the entire universe of Internet communications, [redacted] 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. [redacted] 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.

[redacted]

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] such that the entire mass of collected metadata is relevant to investigating [redacted] affiliated persons. Id. at 48-49; see also id. at 53-54 (relying on government's explanation why bulk collection is "necessary to identify and monitor [redacted] operatives whose Internet communications would otherwise go undetected in the huge streams of [redacted] communications").

B. First Disclosure of Overcollection

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

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

As described by the government, the unauthorized collection resulted from failures to [redacted] in the manner required. [redacted] Decl. at 8-11.[12] By the government's account, the lack of required [redacted] did not result from technical difficulty or malfunction, but rather from a failure of "those NSA officials who understood in detail the requirements of the [redacted] Opinion] . . . to communicate those requirements effectively

[redacted]

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

The Court had specifically directed the government to explain whether this unauthorized collection involved the acquisition of information other than the approved Categories [redacted] 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] 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] Docket Nos. [redacted] Transcript of Hearing Conducted [redacted] at 16-17.

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

The initial bulk PR/TT authorization granted by the [redacted] Opinion was set to expire on [redacted] shortly after the government had disclosed this unauthorized collection. On that date, Judge Kollar-Kotelly granted an application for continued bulk PR/TT acquisition; however, in that application, the government only requested authorization for acquisition [redacted] that had not been subject to the [redacted] See Docket No. PR/TT [redacted] Application filed on [redacted] ("[redacted] Application"), at 9-15; Primary Order issued on [redacted] at 2-5.[14] The government represented that the PR/TT [redacted] had "fully complied with the orders of the Court."

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

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

C. Overcollection Disclosed in [redacted]

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

[15] See [redacted]

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

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

D. Non-Compliance Disclosed [redacted]

The next relevant compliance problems surfaced in [redacted] and involved three general subjects: (1) accessing of metadata; (2) disclosure of query results and information derived therefrom; and (3) overcollection. These compliance disclosures generally coincided with revelations about similar problems under a separate line of FISC orders providing for NSA's bulk acquisition of metadata for telephone communications pursuant to 50 U.S.C. § 1861.[16]

1. Accessing Metadata

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

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

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

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

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

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

(continued...)

compliance measures being taken with regard to the bulk PR/TT program, see [redacted] Response at 6-7, which Judge Walton adopted as requirements in his order authorizing continued bulk PR/TT surveillance on [redacted]. See Docket No. PR/TT [redacted] Primary Order issued [redacted] at 13-14. Finally, the government's response noted the commencement by NSA of a "complete ongoing end-to-end system engineering and process review (technical and operational) of NSA's handling of PR/TT metadata to ensure that the material is handled in strict compliance with the terms of the PR/TT Orders and the NSA's descriptions to the Court." [redacted] Alexander Decl. at 16.[18]

---

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

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

2. Disclosure of Query Results and Information Derived Therefrom

Also in the [redacted] 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. [redacted] 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. [redacted], [redacted] 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 [redacted] & BR 09-06, Order issued on [redacted] Order"), at 7.

On [redacted], 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)
[redacted] Order at 2, the Court ordered NSA not to "resume automated querying of the PR/TT metadata without the prior approval of the Court." Id. at 3.

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

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

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

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

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

application for continued bulk PR/TT authorization. In that application, the government represented that "**all the technologies used by NSA to implement the authorizations granted by docket number PR/TT [redacted] and previous docket numbers only collect, or collected, authorized metadata.**" Docket No. PR/TT [redacted] Application filed on [redacted] 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][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] id. at 3, included the acquisition of [redacted] id. at 2. The government reported that NSA had ceased querying PR/TT metadata and suspended receipt of metadata [redacted] Id. The government later advised that this continuous overcollection acquired

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

many other types of data[20] and that "[v]irtually every PR/TT record" generated by this program included some data that had not been authorized for collection. [redacted]pplication, 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] 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] On the record before the Court, the most charitable interpretation possible is that the same factors identified by the government [redacted] remained unabated and in full effect: non-communication with the technical personnel directly responsible [redacted] resulting from poor management. However, given the duration of this problem, the oversight measures ostensibly taken since [redacted] to detect overcollection, and the extraordinary

[redacted]

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

E. Expiration of Bulk PR/TT Authorities

The PR/TT authorization granted in Docket No. PR/TT [redacted] was set to expire on [redacted] On [redacted] the government submitted a proposed renewal application, which acknowledged [redacted] information that may not have been contemplated under prior orders. See Docket No. PR/TT [redacted] Supplemental Order issued on [redacted] Order"), at 2. The proposed application sought approval [redacted] subject to the restrictions that NSA analysts would not query the PR/TT metadata previously received by NSA[21] and that information prospectively obtained [redacted] would be stored [redacted] and not [redacted] o access or use. Id. at 2. After Judge Walton expressed concern about the merits of the

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

proposed application,[22] the government elected not to submit a final application. Id. at 3. As a result, the authorization for bulk PR/TT surveillance expired on [redacted] Judge Walton directed that the government "shall not access the information [previously] obtained . . . for any analytic or investigative purpose" and shall not "transfer to any other NSA facility information . . . currently stored [redacted] Id. at 4-5. He also provided that, "[i]n the extraordinary event that the government determines immediate access to the [PR/TT metadata] is necessary in order to protect against an imminent threat to human life, the government may access the information," and shall thereafter "provide a written report to the Court describing the circumstances and results of the access." Id. at 5.[23]

F. The Current Application

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

---

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

[23] In compliance with this requirement, the government has reported that, under this emergency exception, NSA has run queries of the bulk metadata in response to threats stemming from (i) [redacted] See, e.g., Docket No. PR/TT [redacted] Reports filed on [redacted] and various reports filed from [redacted]

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

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

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

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

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

A. The Applicable Statutory Definitions

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

> (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . . ;[24]

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

> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

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

> (1) "Electronic communication" is defined as:
>
> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include – (A) any wire or oral communication.[25]

18 U.S.C. § 2510(12).

> (2) "Wire communication" is defined as:
>
> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

18 U.S.C. § 2510(1).

---

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

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

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

[redacted]

As explained by the government, the proposed collection [redacted] Declaration of Gen. Keith B. Alexander, Director of NSA, at 23-24 (attached as Exhibit A to [redacted] Application) ([redacted] Alexander Decl."). [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).

[redacted] 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 [redacted] 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

[redacted]

communication under the definitions set forth above.[28] The end-result of the collection process[29] 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).

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

C. The Requested Information

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

1. The Proper Understanding of DRAS Information and Contents

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

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

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

37, the ordinary meanings of the terms "dialing," "routing," addressing," and "signaling" – which are not defined by the statute – are relatively broad. Moreover, as noted above, the term "contents" is broadly defined to include "any information concerning the substance, purport, or meaning of [an electronic] communication." 18 U.S.C. § 2510(8) (emphasis added). And "electronic communication," too, is defined broadly to mean "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system . . . ." 18 U.S.C. § 2510(12) (emphasis added).

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

[31] See Newton's Telecom Dictionary 971 (24th ed. 2008).

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

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

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

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

In determining whether or not the types of information sought by the government constitute DRAS information, the Court is guided by the ordinary meanings of the terms "addressing," "routing," and "signaling," and by the context in which the terms are used.[34] As the government asserts, "addressing information" may generally be understood to be "information that identifies recipients of communications or participants in a communication" and "may refer to people [or] devices." Memorandum of Law at 37.[35] The Court also agrees with the government that "routing information" can generally be understood to include information regarding "the path or means by which information travels." Memorandum of Law at 37. As will be explained more fully in the discussion of "communications actions" below, the Court adopts a somewhat narrower definition of "signaling information" than the government. In summary, the Court concludes that signaling information includes information that is utilized in

---

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

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

[35] See Newton's Telecom Dictionary at 89 ("An address comprises the characters identifying the recipient or originator of transmitted data.").

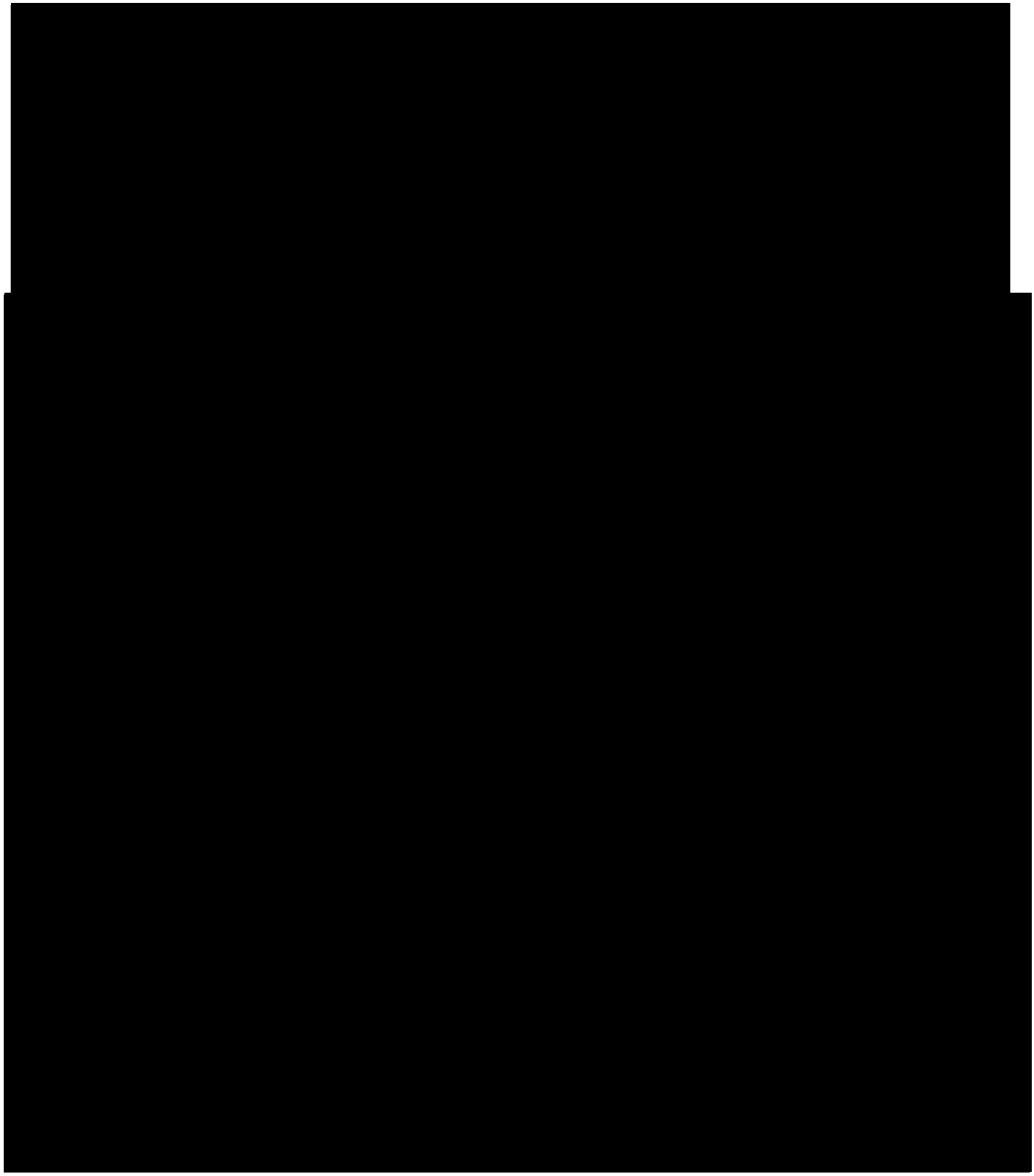
or pertains to (1) logging into or out of an account or (2) processing or transmitting an e-mail or IM communication. See pages 50-56, infra.[36]

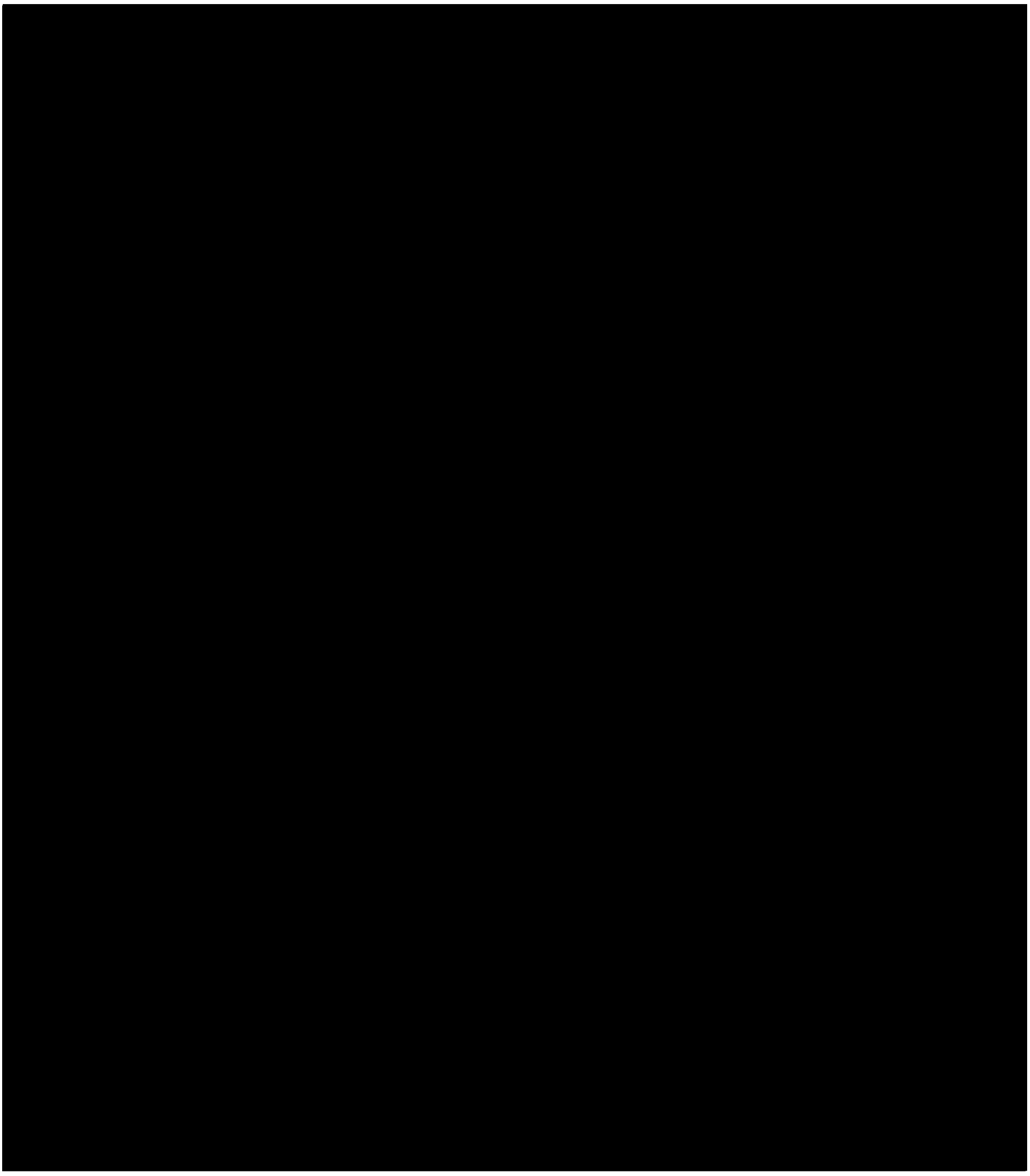
With regard to "contents," the Court is, of course, bound by the definition set forth in Section 2510(8), which, as noted, covers "any information concerning the substance, purport, or meaning" of the wire or electronic communication to which the information relates. When the communication at issue is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

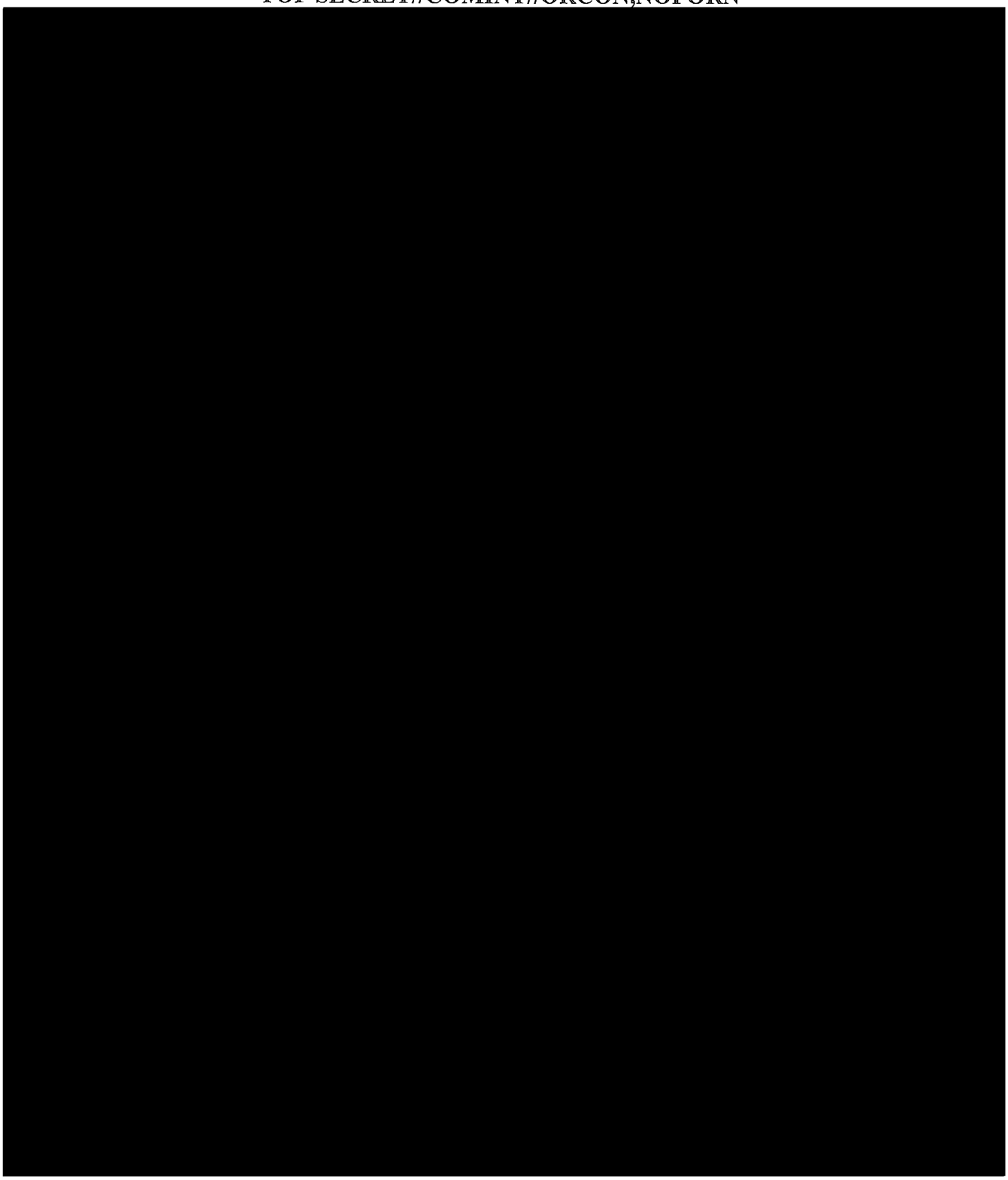
2. The Categories of Metadata Sought for Acquisition

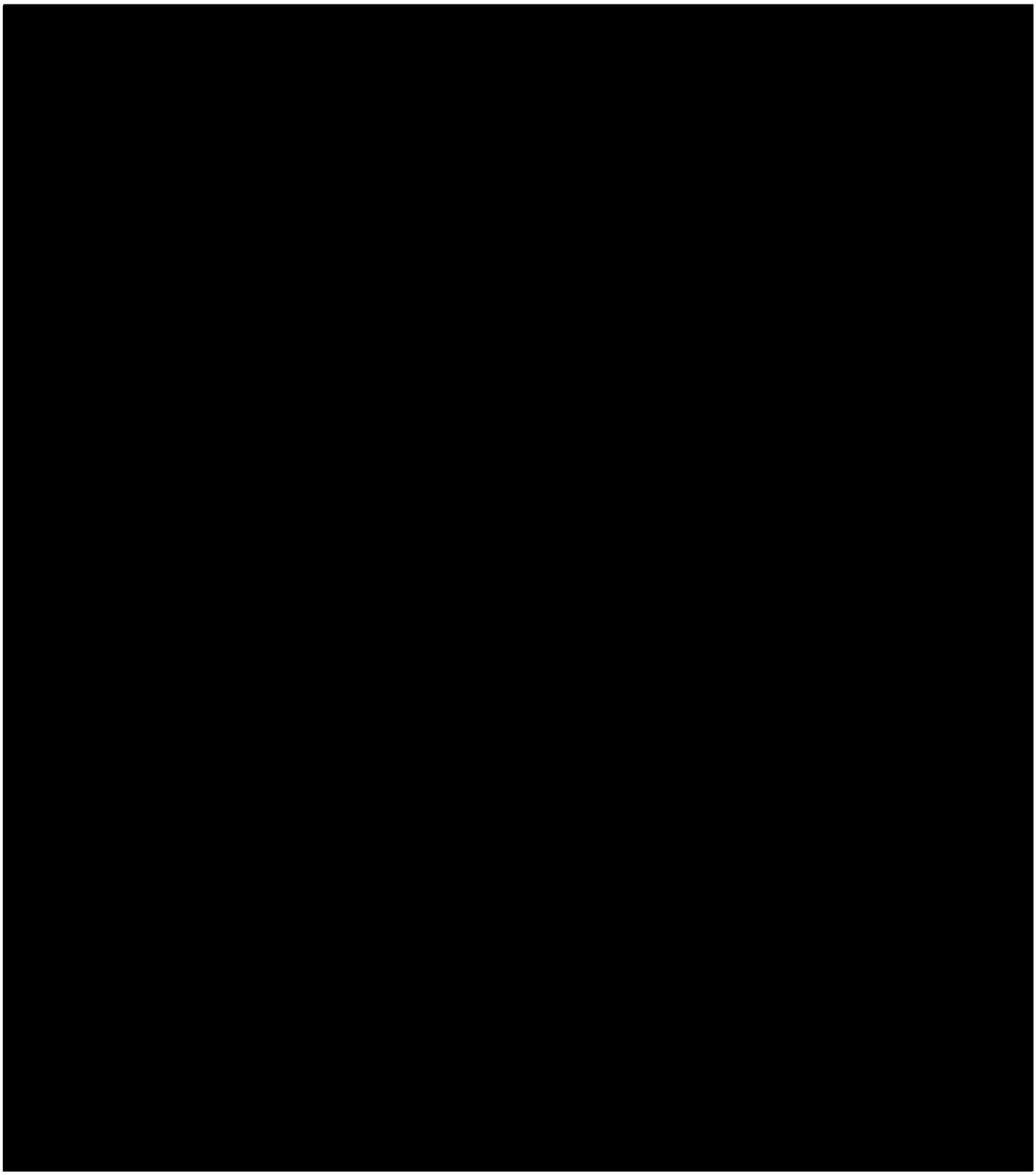
The government requests authority to [redacted] categories of [redacted]

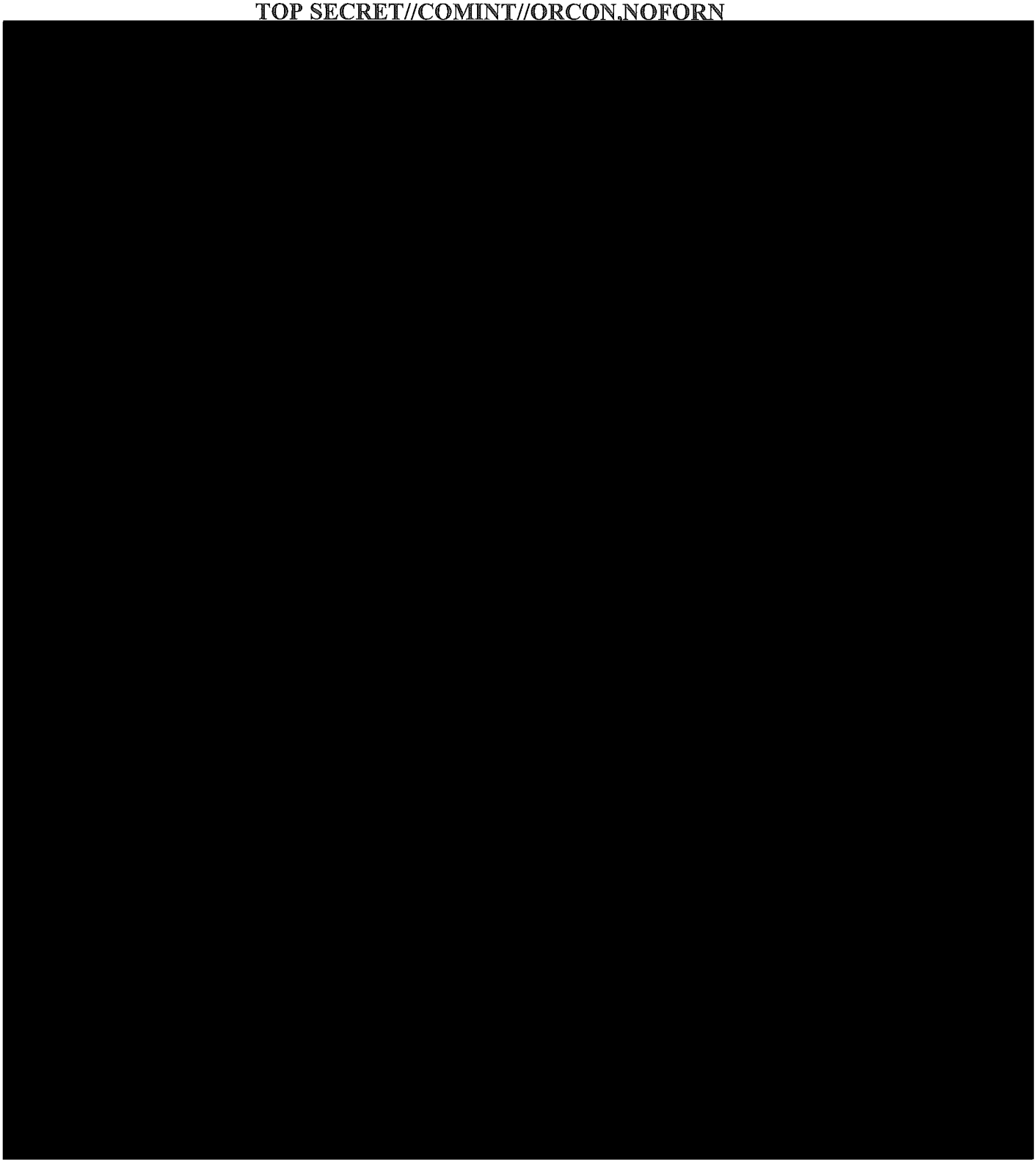
[36] For purposes of this Opinion, the term "e-mail communications" refers to e-mail messages sent between e-mail users [redacted]

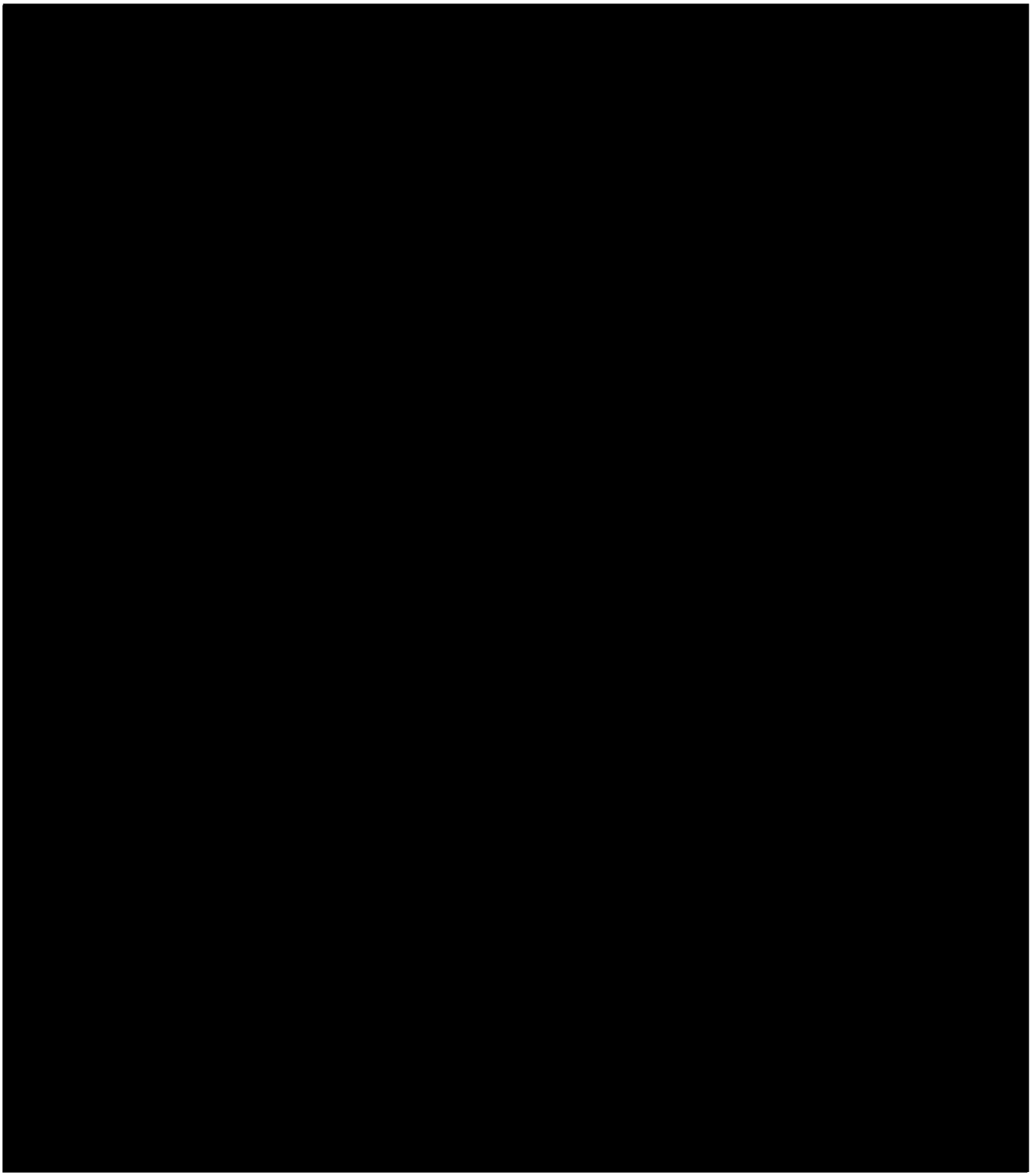


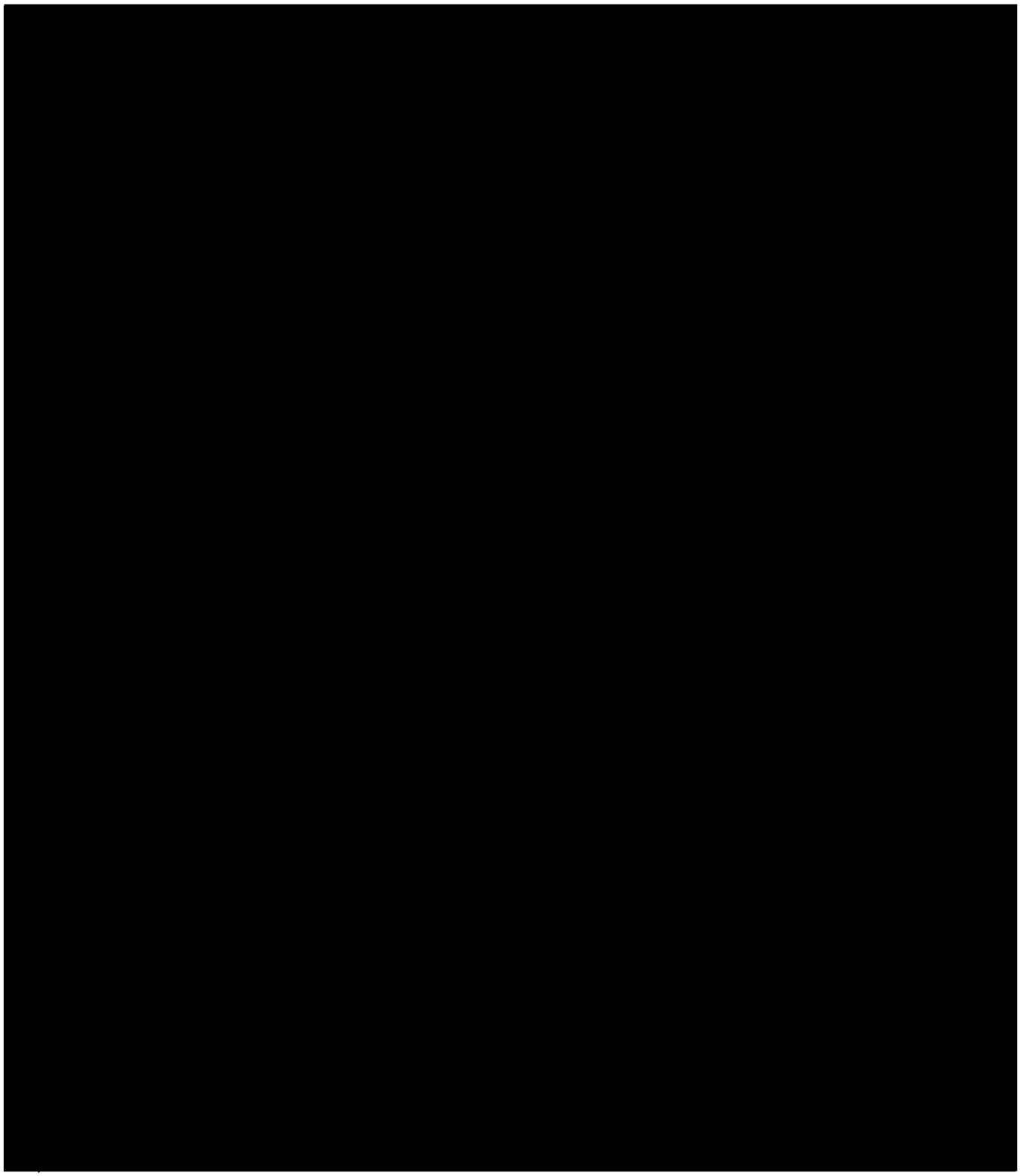


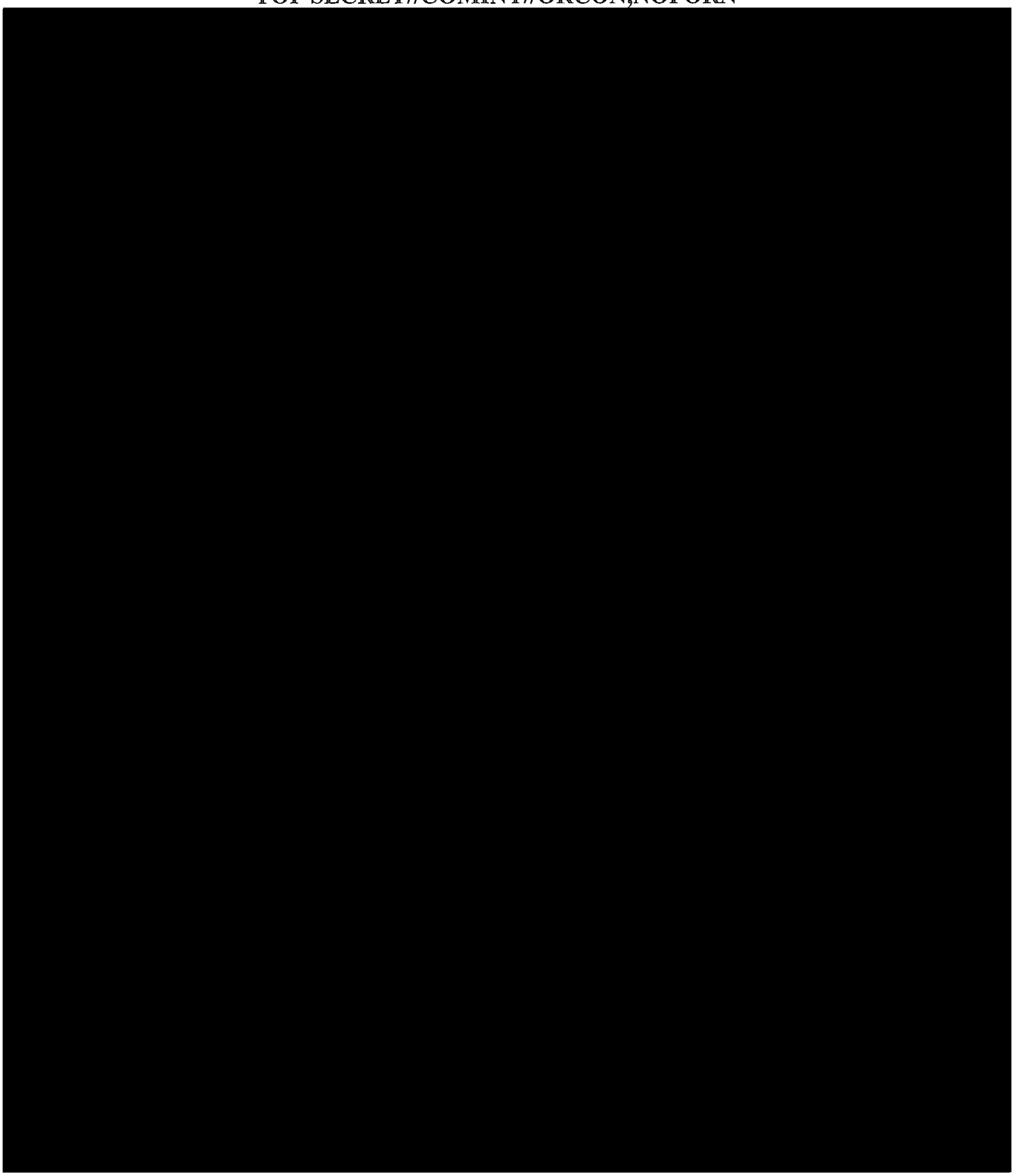


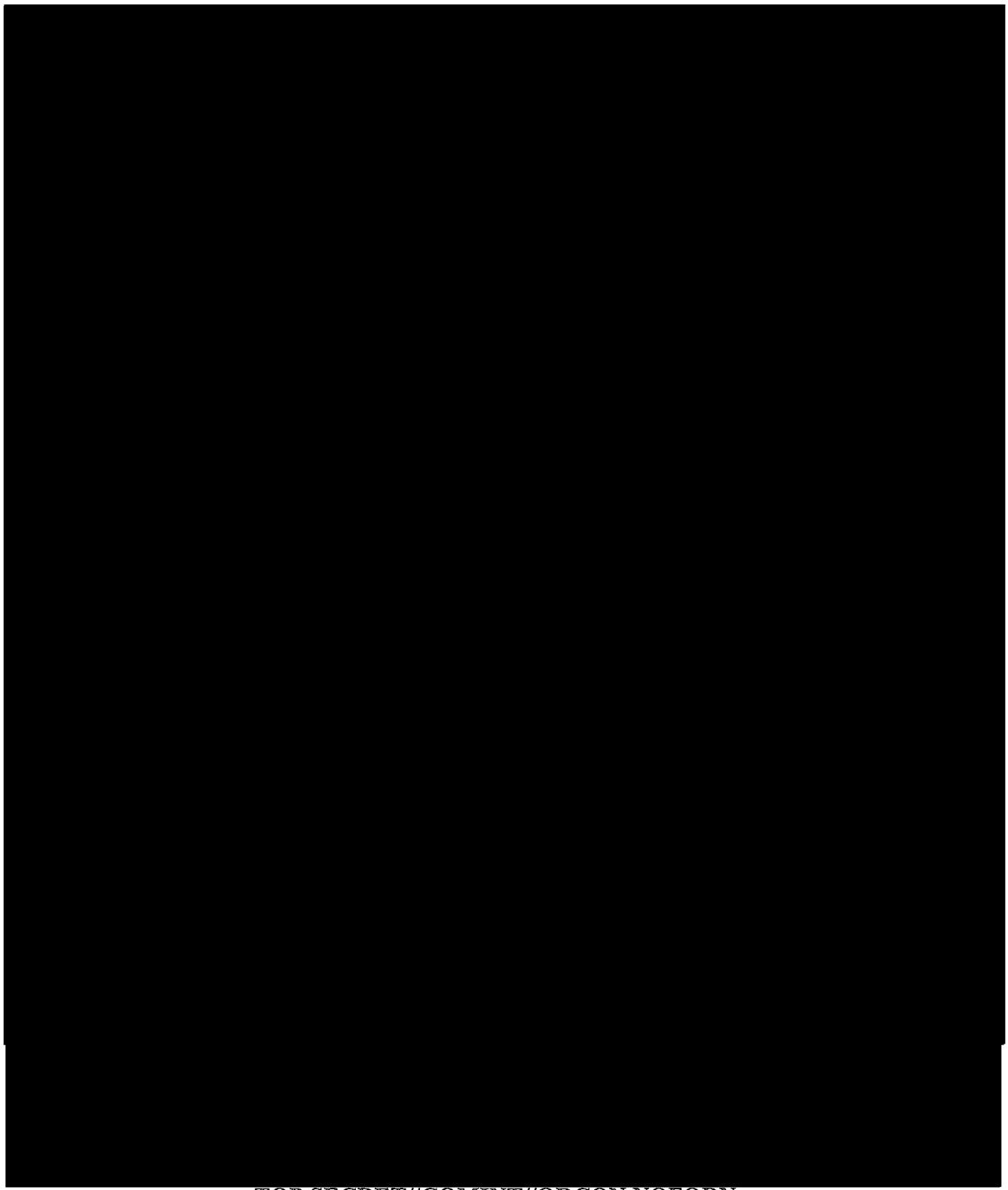


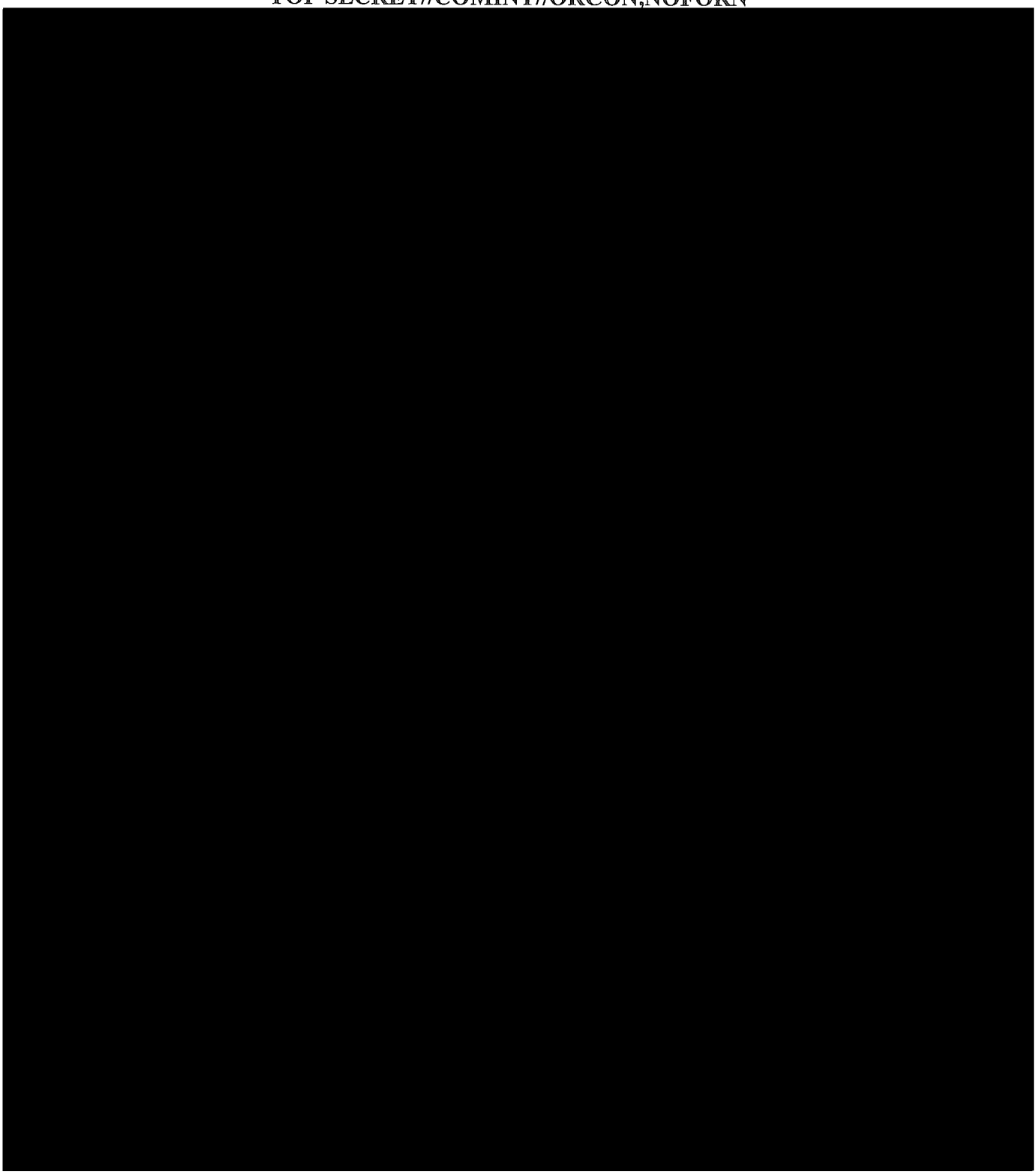


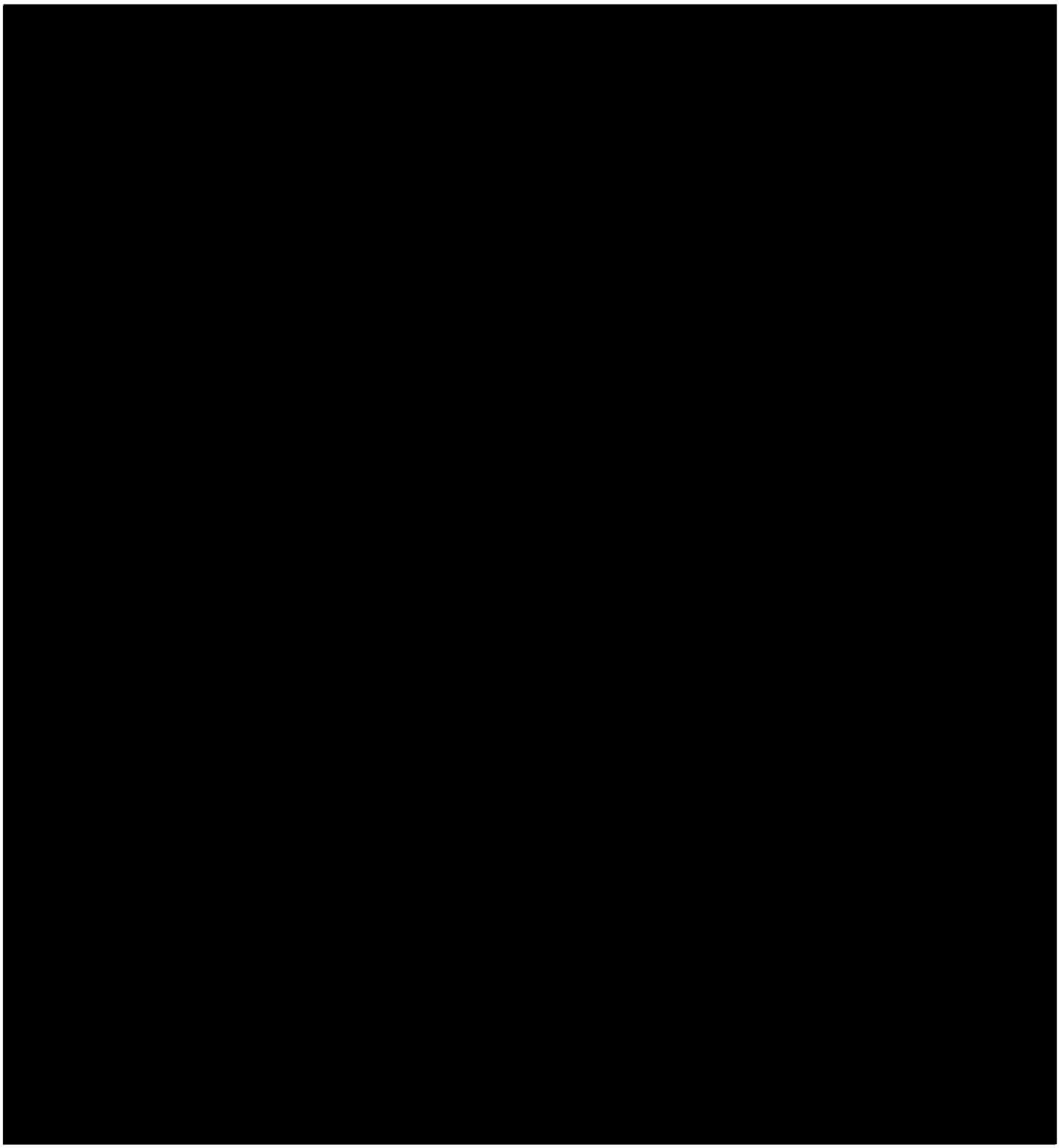


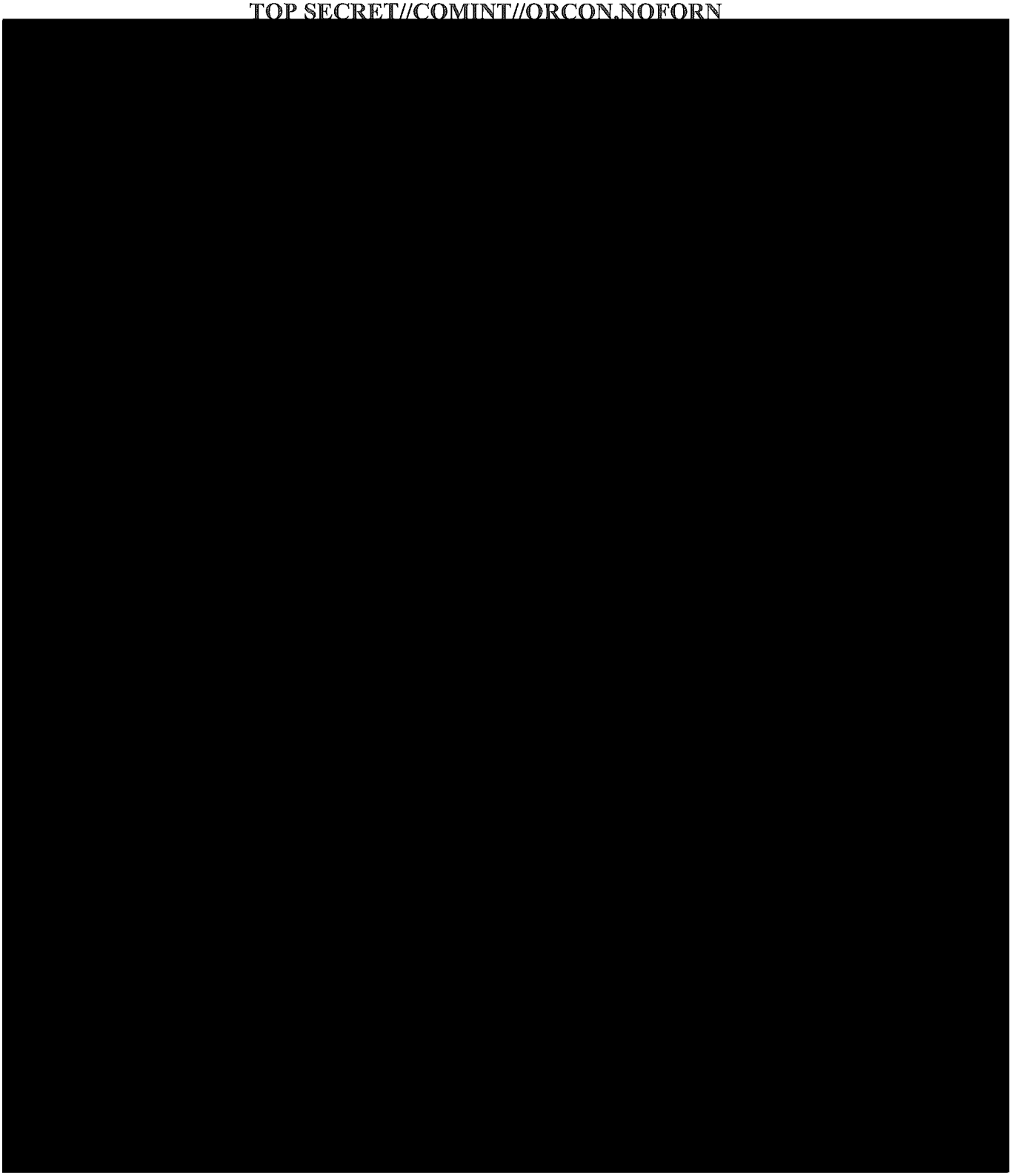


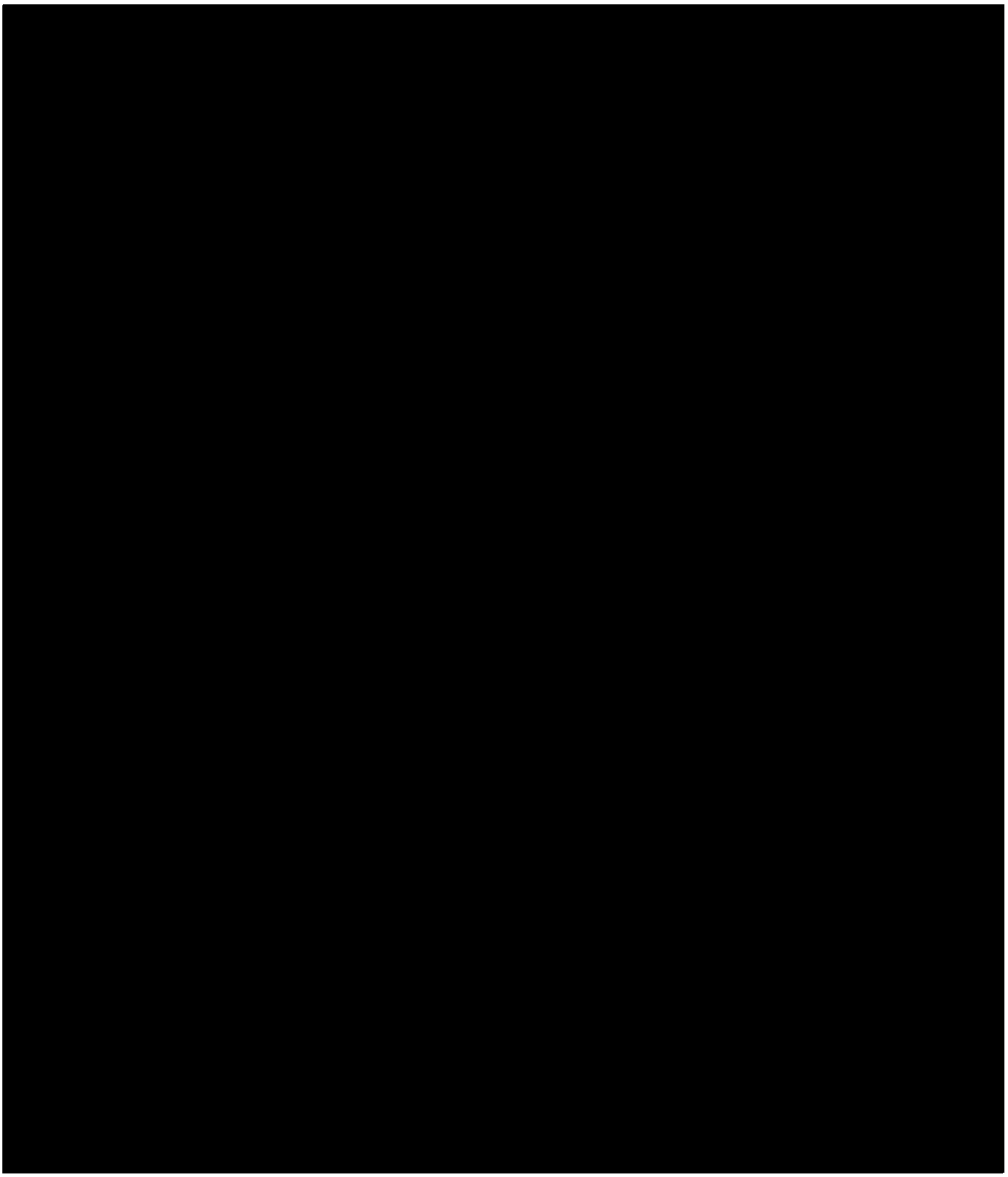


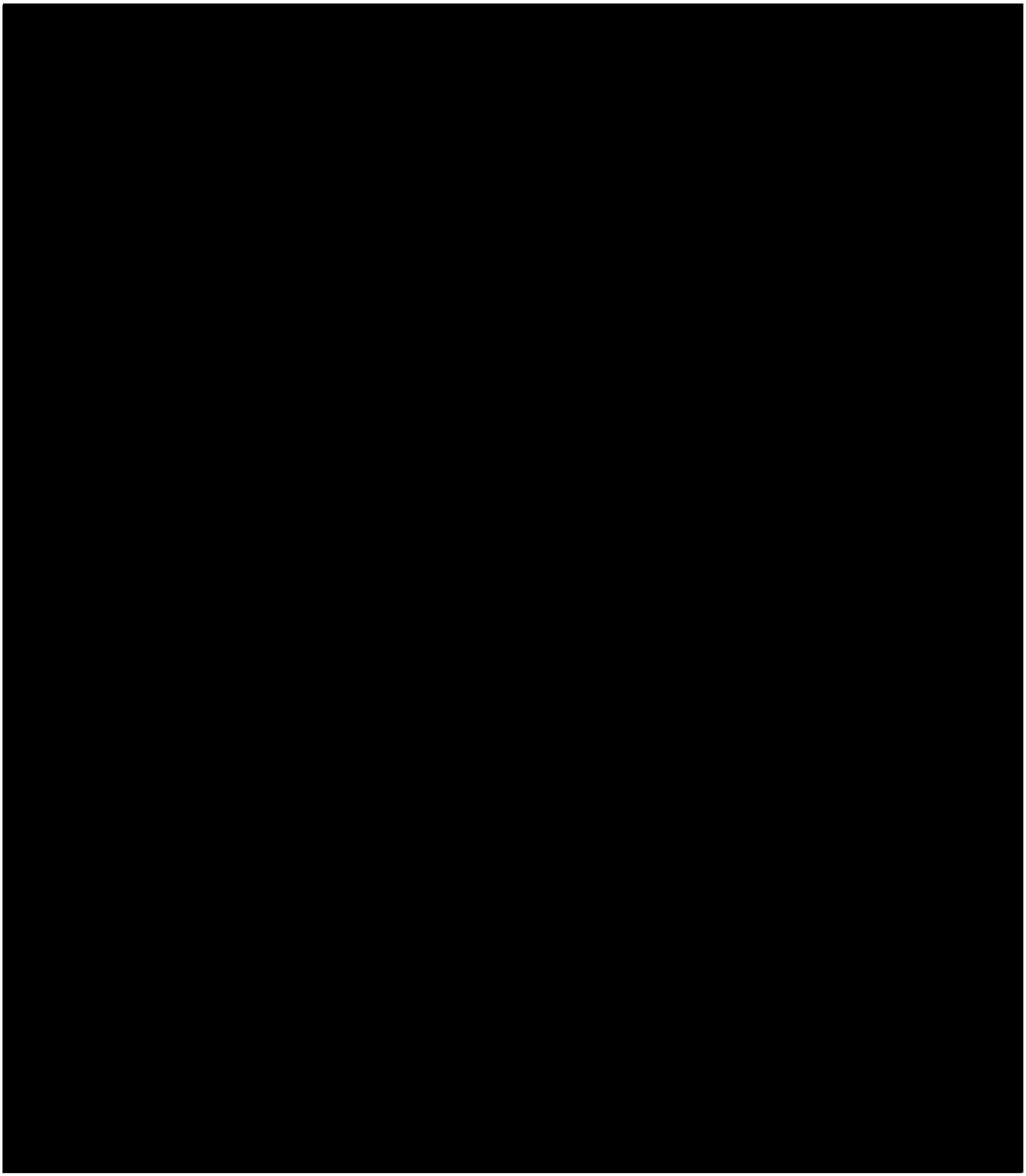


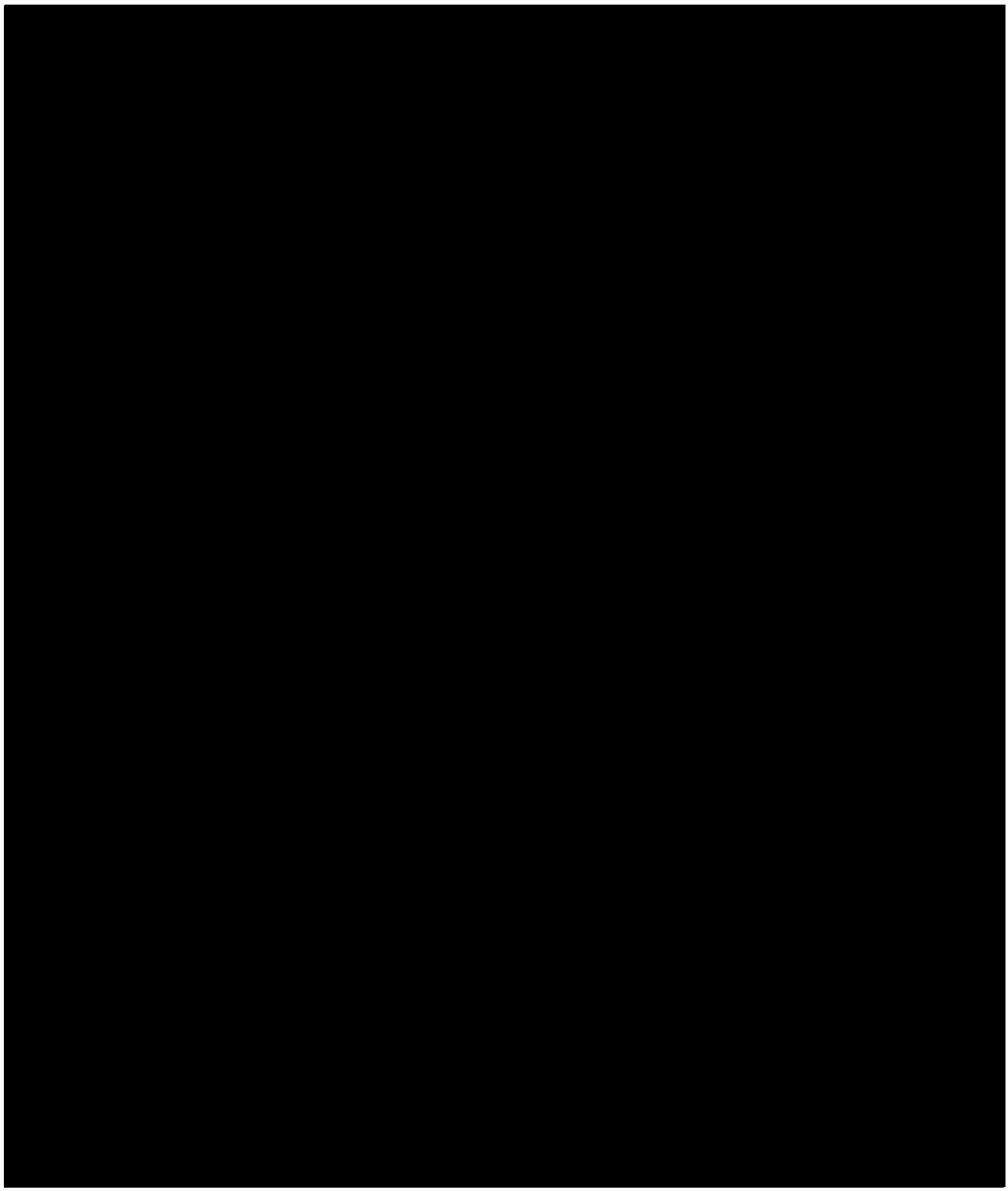


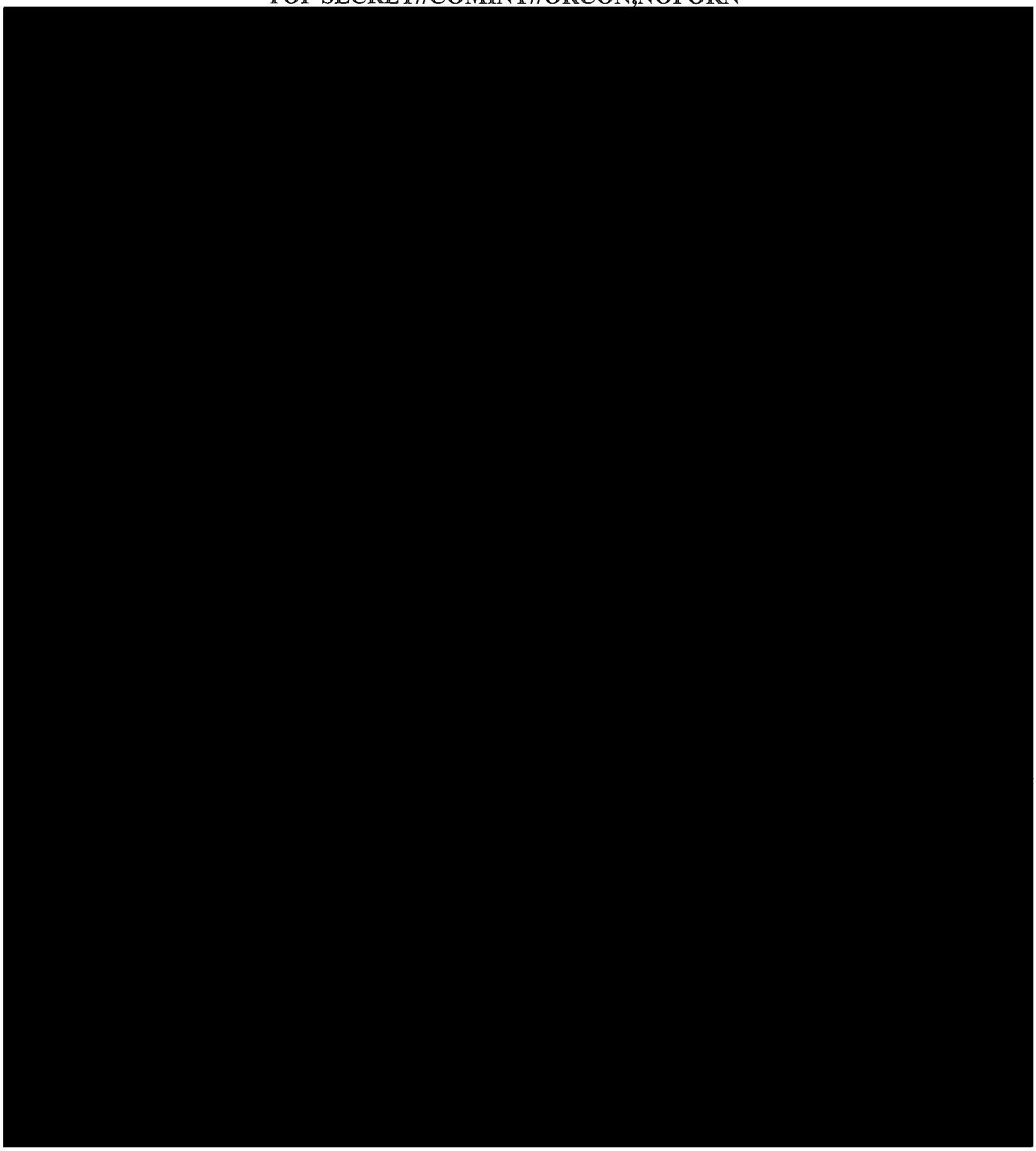












[redacted]

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

[redacted]

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

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

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

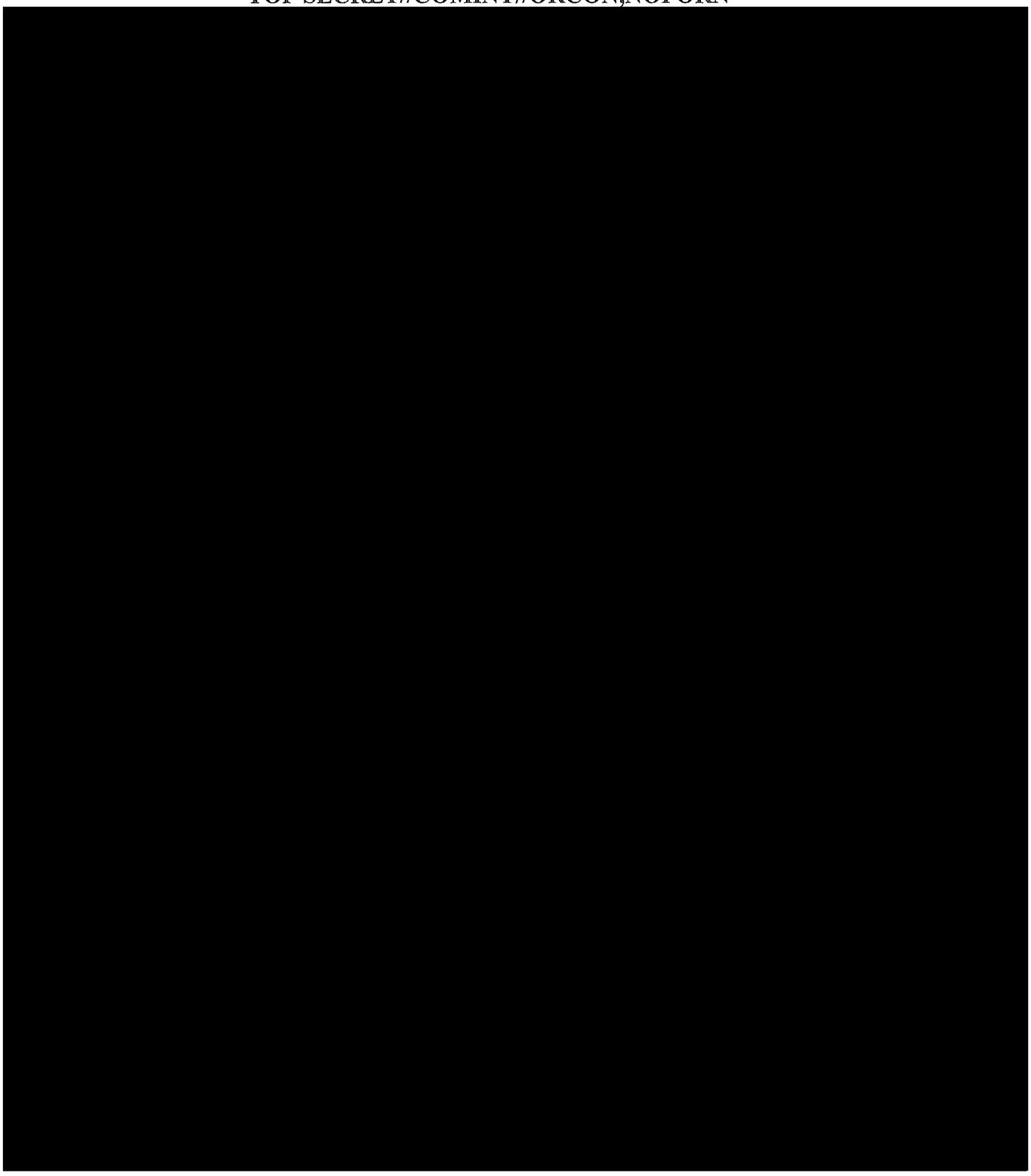
> A government agency authorized to install and use a pen register or trap and trace device . . . shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing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

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

[redacted]

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. [redacted]

[redacted]



[redacted]

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.

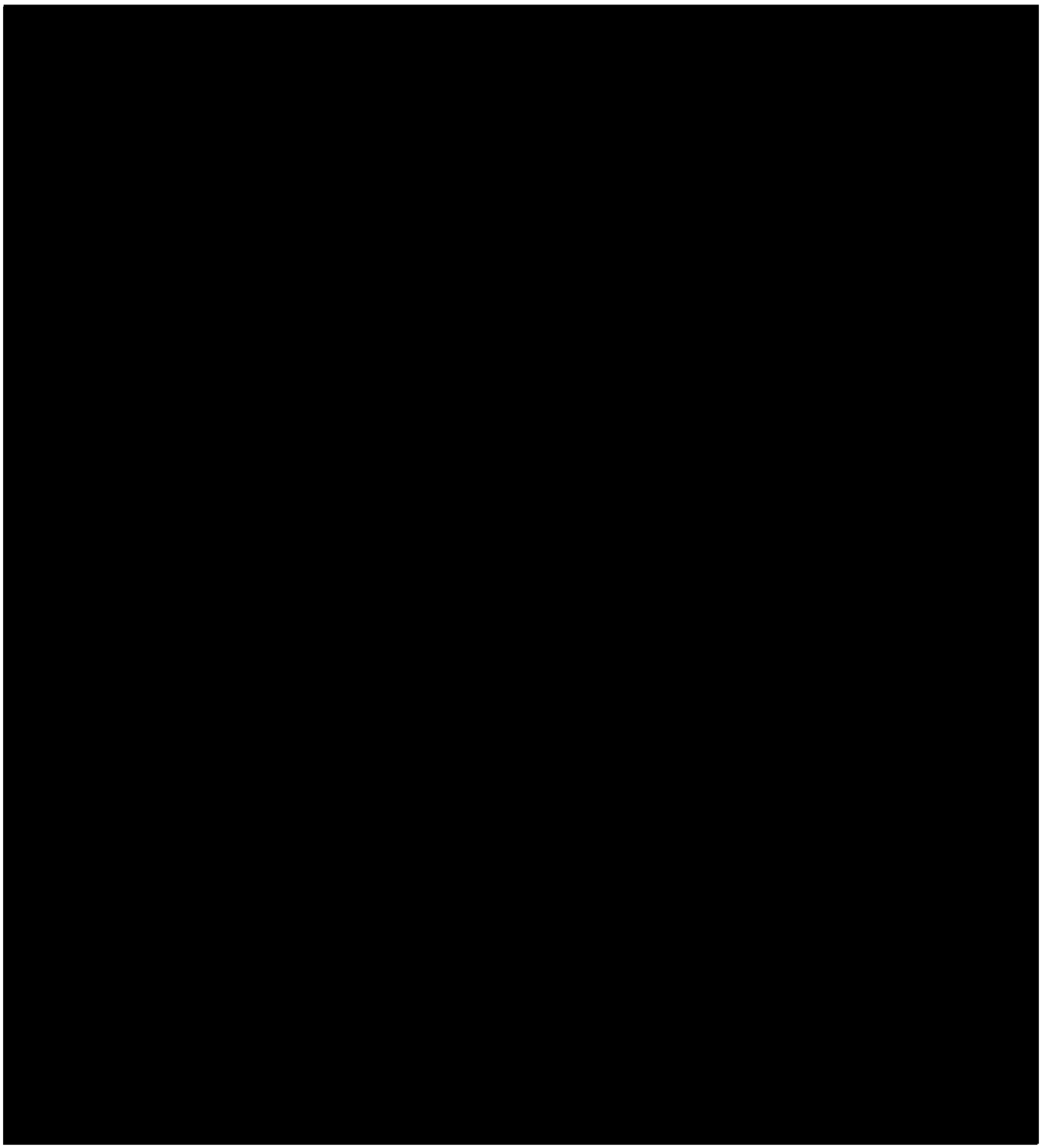
The government does not directly confront the statutory text on this point. It does argue, however, that an expansive, literal understanding of the prohibition on acquiring "contents" would lead to an absurd and unintended restriction on what PR/TT devices can do. Specifically, the government notes that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

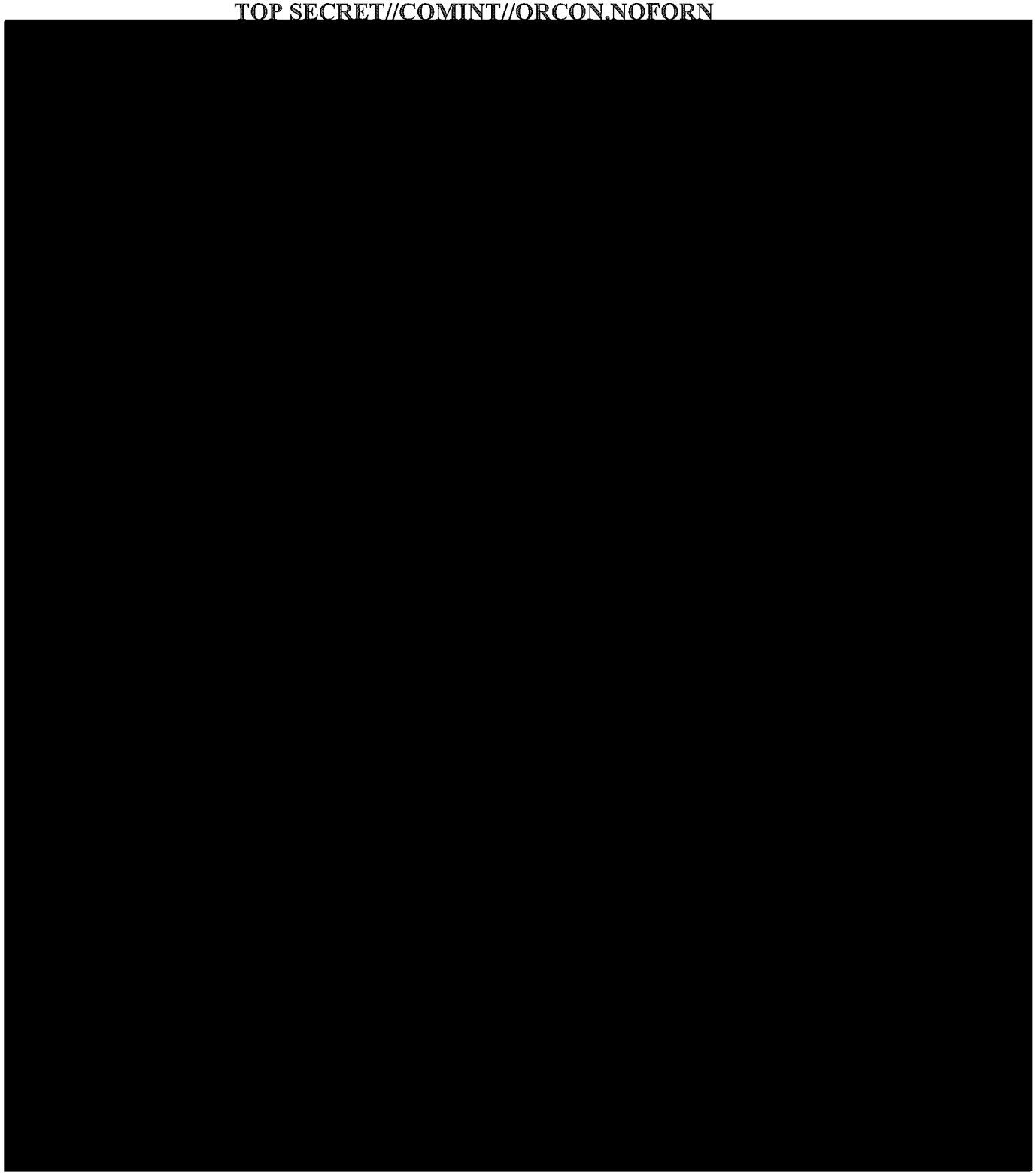
[49] The Court's understanding of "processing" and "transmitting" e-mail [redacted] is set forth below. See pages 63-64, infra.

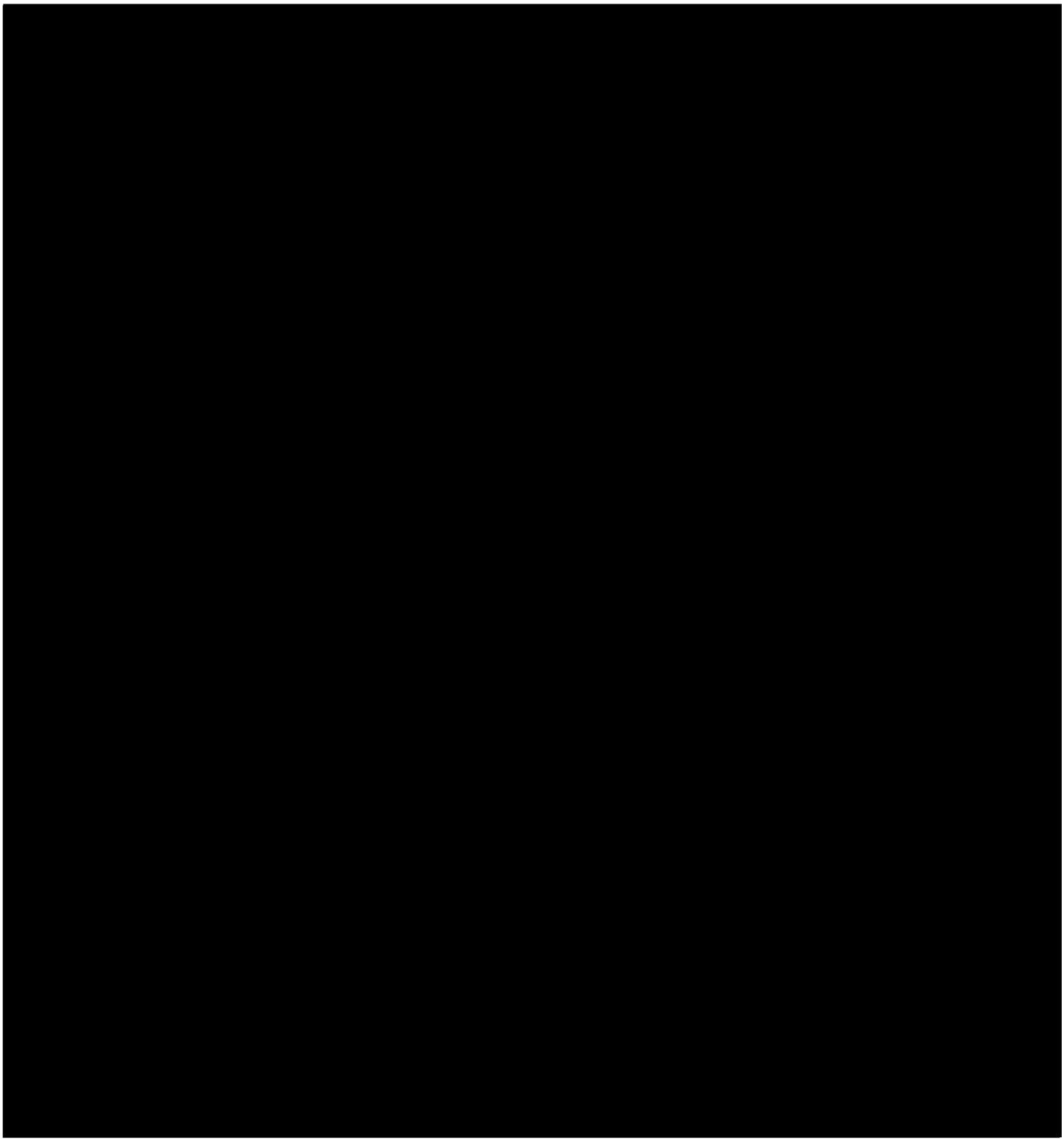
literally qualify as an "electronic communication" under Section 2510(12), but the "import" of that communication – i.e., "place a call from this telephone to the one whose number has been dialed" – has never been understood to be impermissible "contents" under the PR/TT statute. See [redacted] Response at 7.

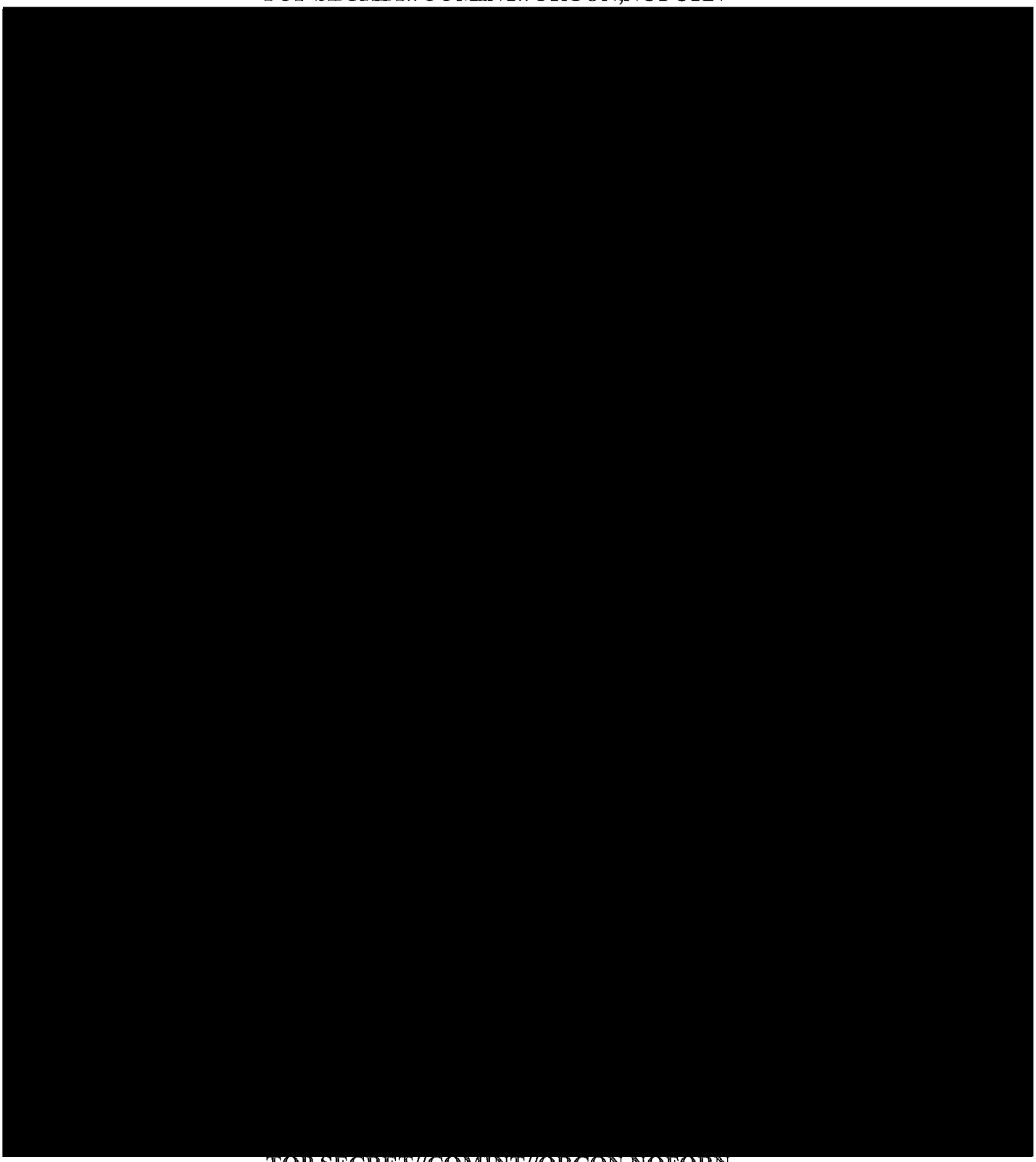
[redacted]

[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").

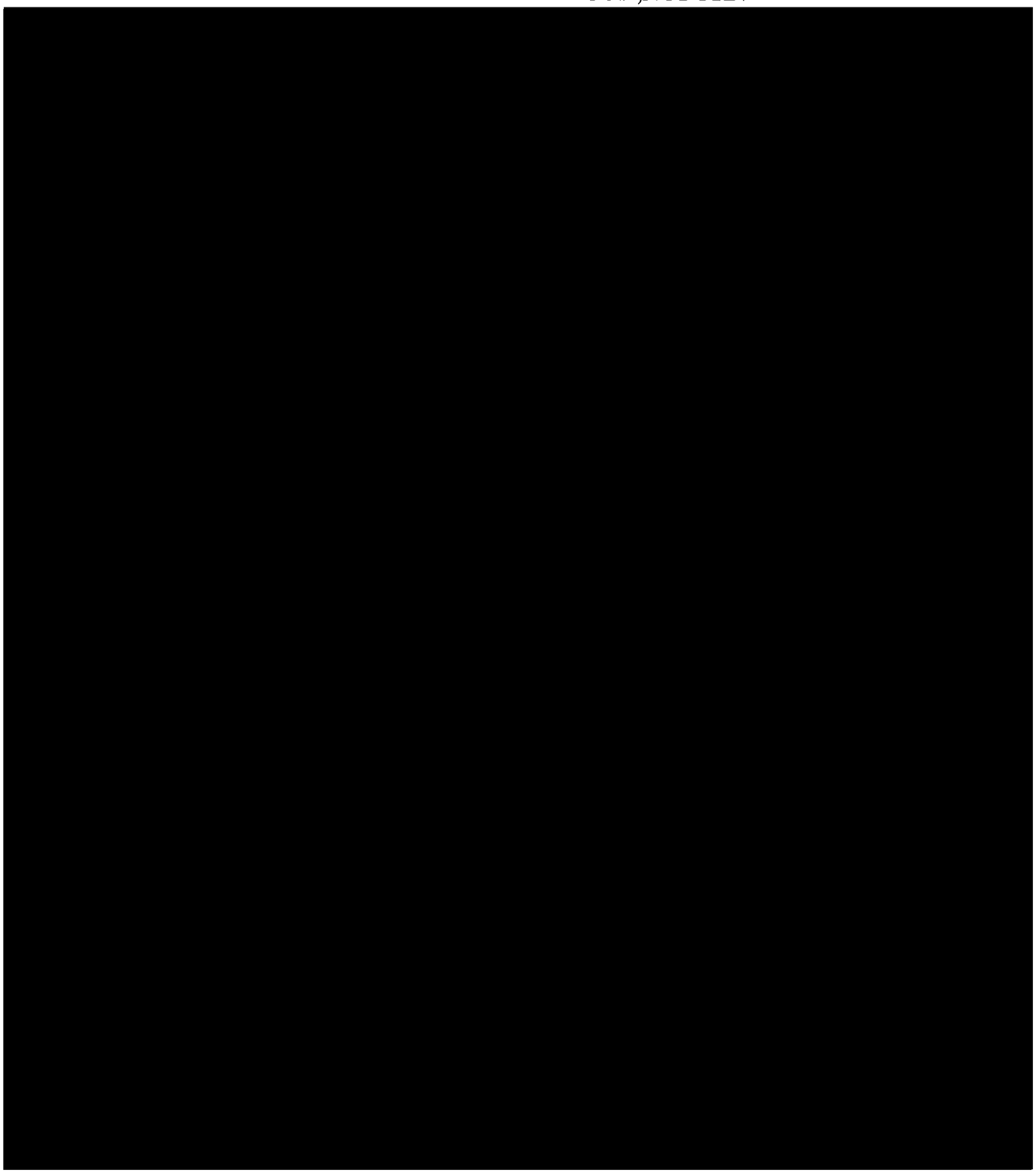


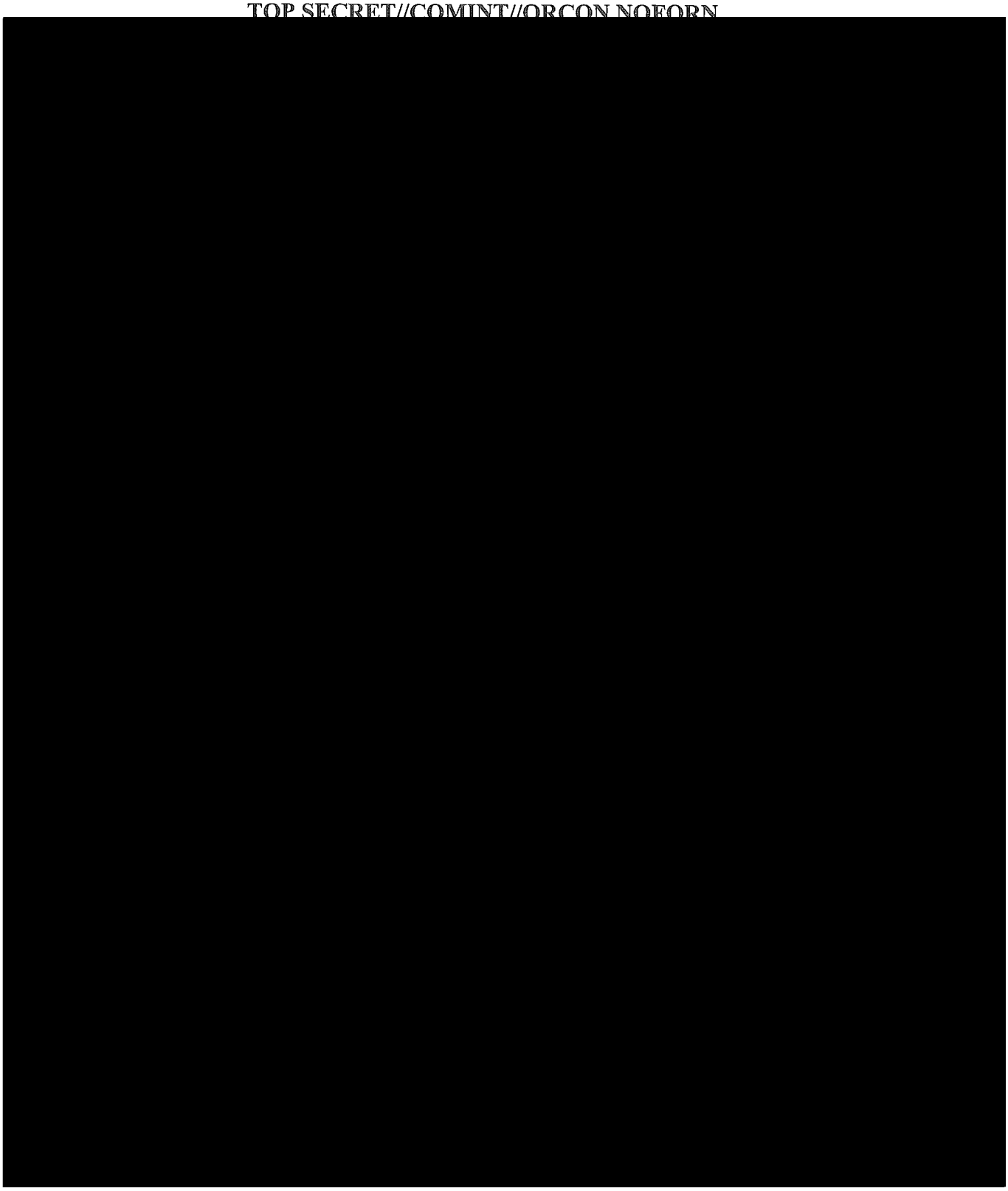


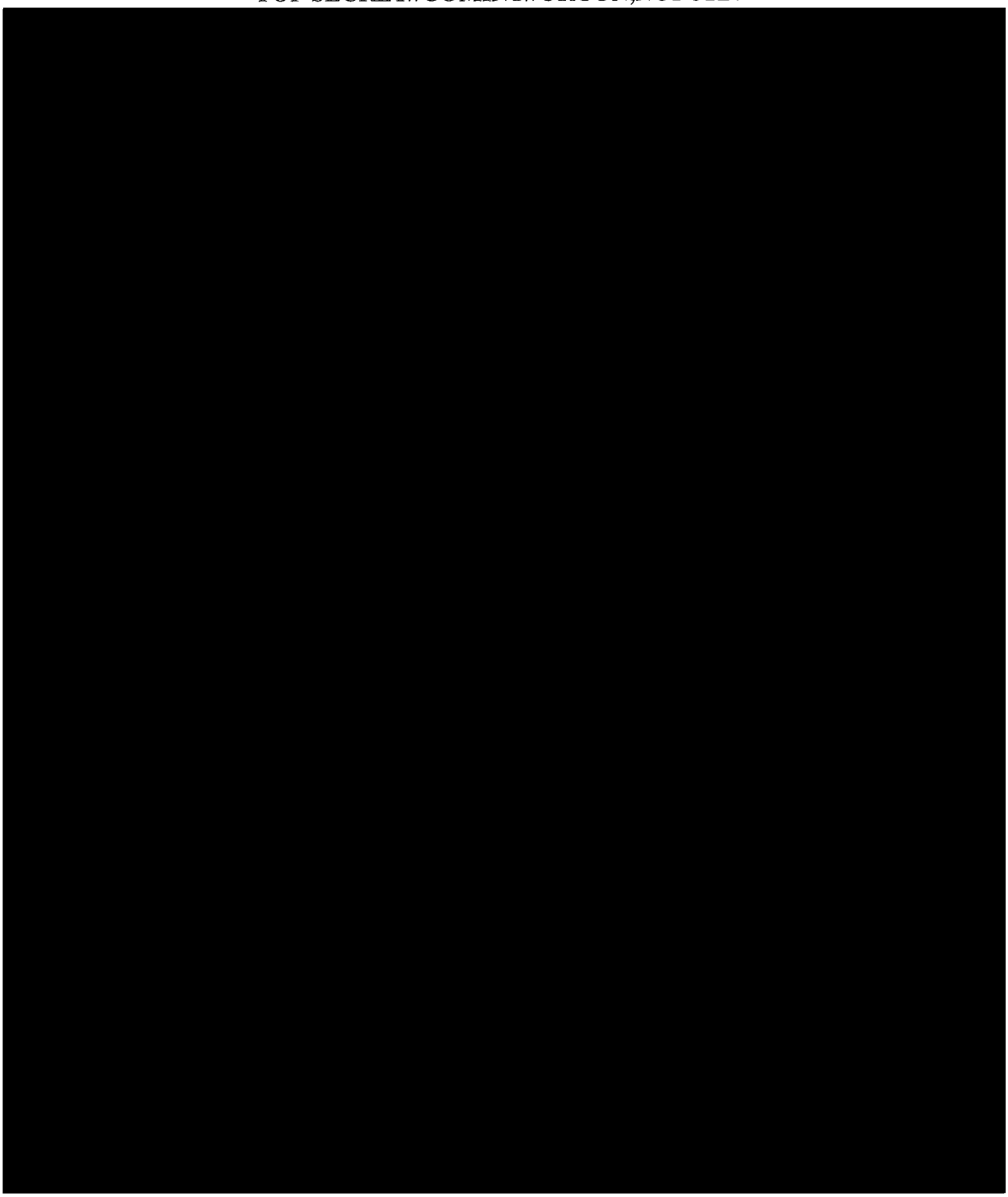


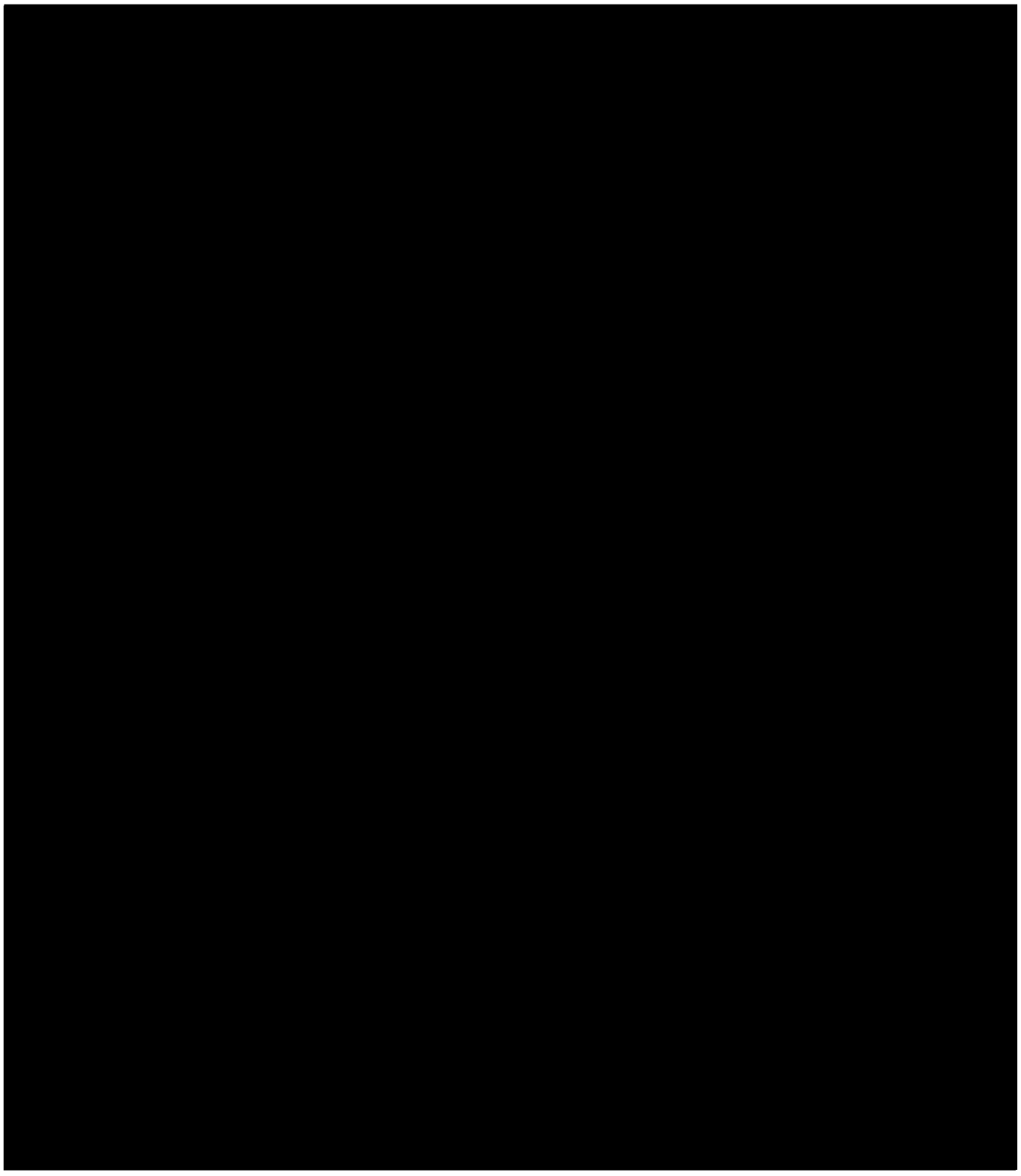


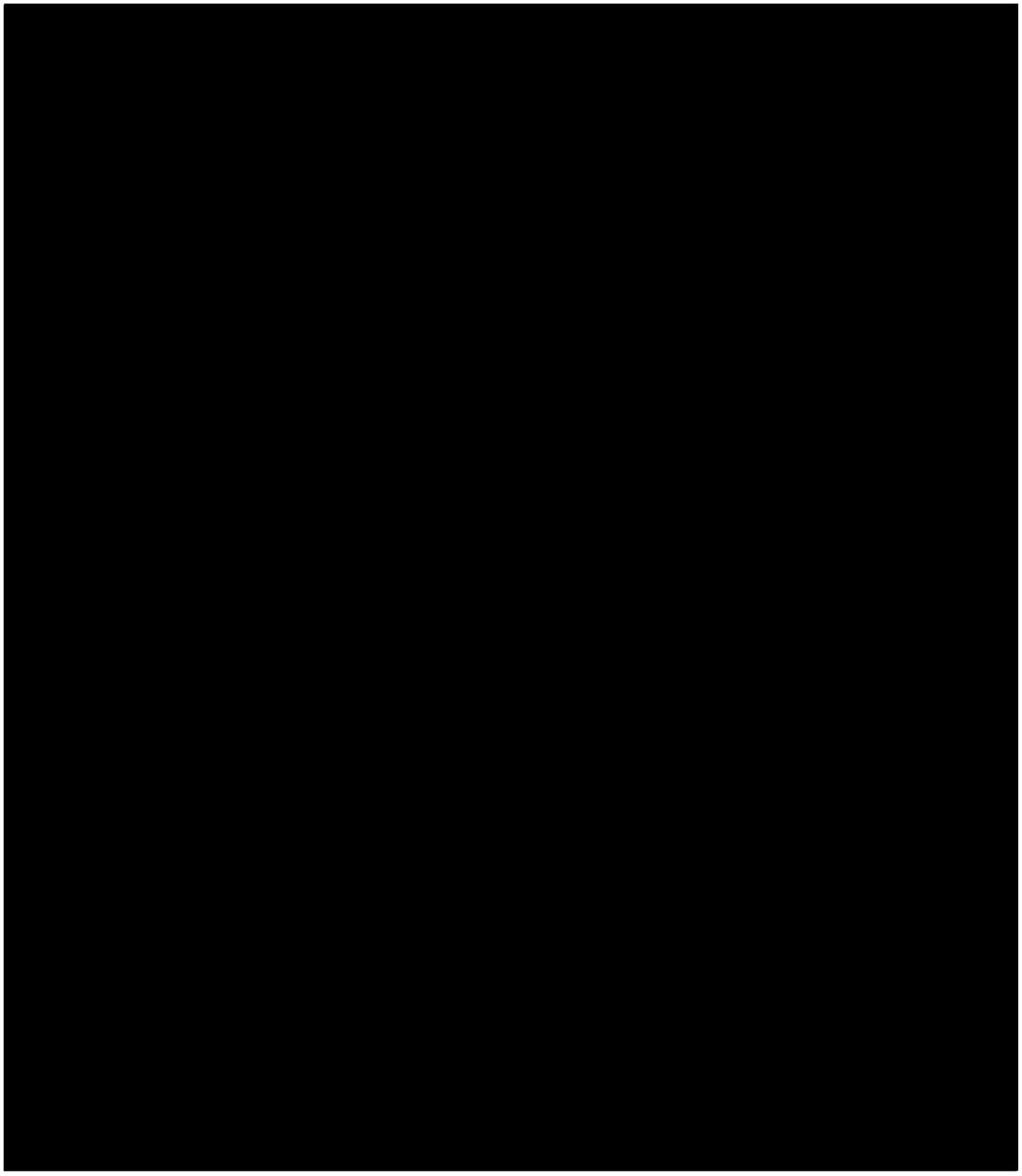
[53] See, e.g., TRW Inc. v. Andrews, 534 US. 19, 31 (2001) ("It is our duty to give effect, if possible, to every clause and word of a statute.") (citation and internal quotations omitted); accord Duncan v. Walker, 533 U.S. 167, 174 (2001).

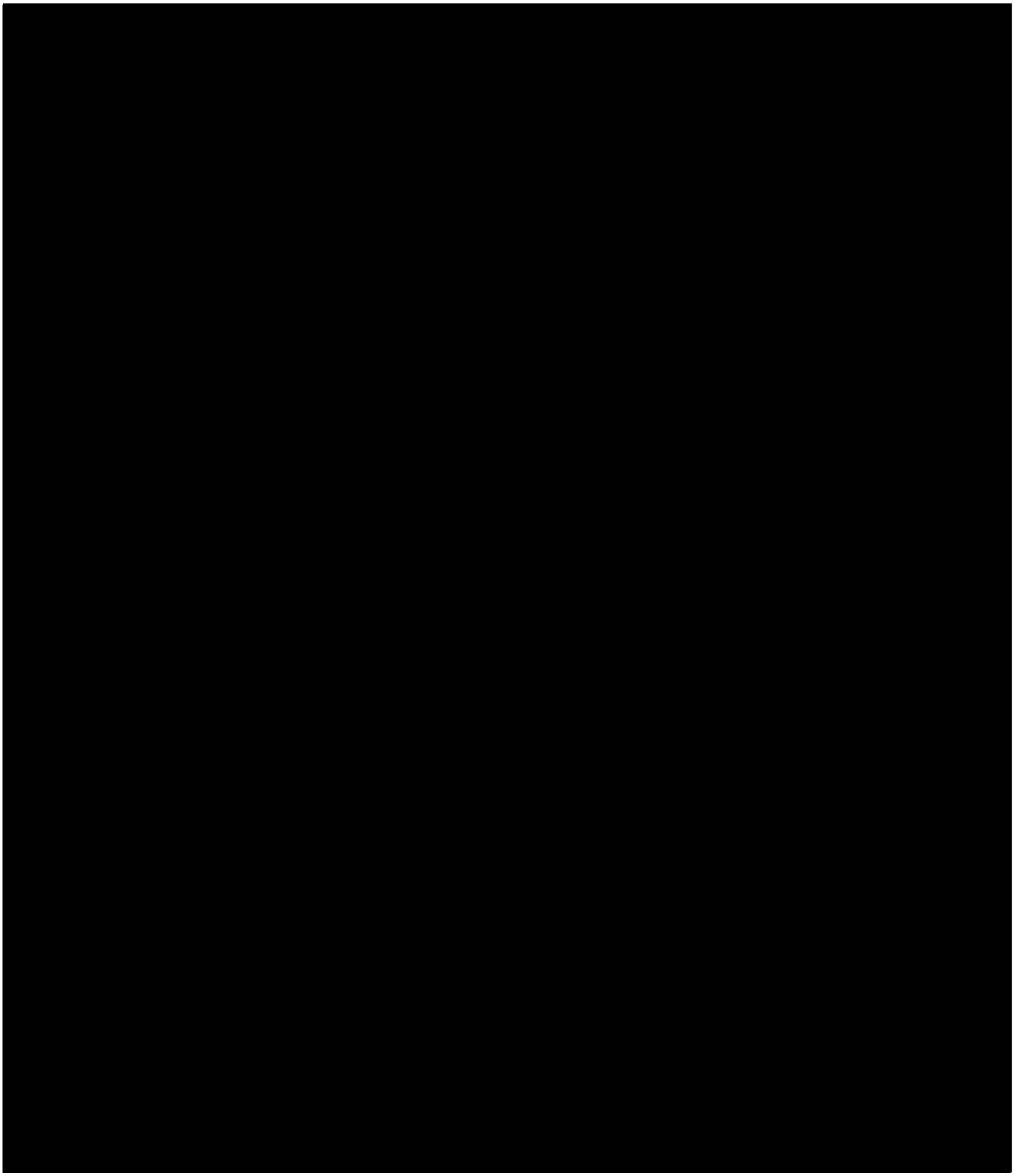


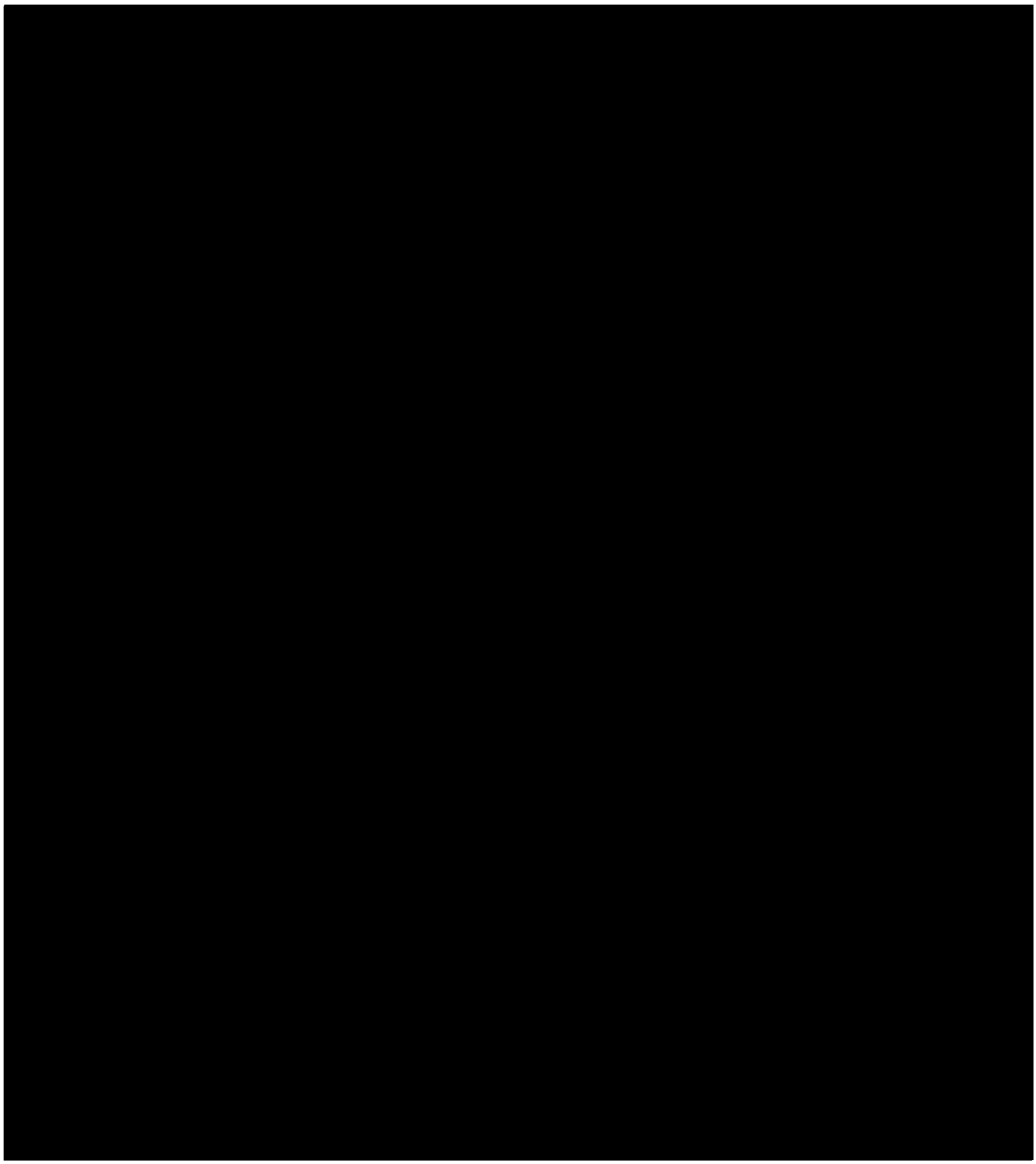












The foregoing analysis has involved difficult line-drawing. But the end-results correspond well with the evident legislative purpose of permitting the acquisition of DRAS information for e-mail [redacted] while avoiding the acquisition of the contents of electronic communications, [redacted] The Court believes that this approach is necessary to ensure that the authority sought by the government [redacted] is limited to non-content signaling information properly subject to collection by a PR/TT device. Given the challenges presented by this category of metadata, the Court's authorization will be limited to the [redacted] approved above. [redacted]

III. The Application Satisfies the Applicable Statutory Requirements

A. Request to Re-Initiate and Expand Collection

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

[redacted]

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

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

B. Relevance

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

[redacted]

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

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

---

[57] Under FISA, a PR/TT application requires

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

50 U.S.C. § 1842(c)(2).

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

NSA's efforts to acquire metadata that [redacted] 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.

[redacted] Primary Order issued on [redacted], 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." [redacted] Alexander Decl. at 18. There is credible testimony that terrorists affiliated with the Foreign Powers attempt to conceal operational communications by [redacted] 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 [redacted] Response at 3. The Court is satisfied that the increase in U.S. person communications does not undermine the basis for relevance, particularly in view of the specific safeguards for accessing and disseminating U.S. person information.

as e-mail accounts used by known terrorists that otherwise would be missed. Id. at 21-22.[62]

As the [redacted] Opinion recognizes, the relevance standard does not require "a statistical 'tight fit' between the volume of proposed collection and the much smaller proportion of information" that pertains directly to a Foreign Power. [redacted] Opinion at 49-50. Nor, in the Court's view, does the relevance standard necessarily require a PR/TT authorization to limit collection to [redacted] of Foreign Power communications. The circumstances that make bulk metadata relevant include [redacted] Alexander Decl. at 18. It follows that some Foreign Power communications [redacted]

[redacted]

C. Specifications of the Order

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

specify–

> (i) the identity, if known, of the person who is the subject of the investigation;
>
> (ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and
>
> (iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.[65]

[redacted]

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.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

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

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

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

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

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

[redacted]

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

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

---

[69] Section 1801(h) defines "minimization procedures" in pertinent part as follows:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]
>
> . . .

50 U.S.C. § 1801(h).

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

A. Storage and Traceability

NSA will continue to store the PR/TT data that it retains in repositories within secure networks under NSA's control. [redacted]lexander 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]esponse at 15, are designed to ensure that software and other controls (such as user authentication tools) can restrict access to the PR/TT data solely to authorized personnel who have received appropriate training regarding the special rules for using

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

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

Under the approach proposed by the government, "[t]rained and authorized technical personnel" will be permitted to access the metadata to ensure that it is "usable for intelligence analysis." Id. at 25. For example, such personnel may access the metadata to perform processes designed to prevent the collection, processing, or analysis of metadata associated with [redacted] 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]uery 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] Alexander Decl. at 25. After recognizing a [redacted]

(continued...)

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 Coordinators[72]) 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).

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] 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] Response at 16.

The government's proposed RAS-approval and querying process differs in two noteworthy respects from the approach previously approved by the Court. First, unlike RAS approvals made pursuant to the [redacted] 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. [redacted] 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 [redacted] NSA 90-Day Report to the Foreign Intelligence Surveillance Court filed on [redacted] at 6. The government had informed the Court on [redacted] 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 [redacted] Order on [redacted].

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 [redacted] 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; [redacted] 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." [redacted] 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 [redacted] 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 [redacted] 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." [redacted] Order at 11. The basis for such widespread sharing of query results

within NSA was the government's assertion that analysts throughout the agency address counterterrorism issues as part of their missions and, therefore, have a need for the information.[75] Presumably for the same reason, the government proposes in the application now before the Court that the results of RAS-approved queries be available to all NSA analysts for intelligence purposes, and that such analysts be allowed to apply "the full range of SIGINT analytical tradecraft" to the query results. [redacted] Alexander Decl. at 28 n.19.[76] The Court is satisfied

---

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

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

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

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

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

E. Dissemination Outside NSA

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

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

Id.

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

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

> NSA, the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operation Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.

Id.

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

---

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

(continued...)

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

---

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

[78] See, e.g., Holder v. Humanitarian Law Project, — U.S. —, 2010 WL 2471055, *22 (June 21, 2010) ("[W]hen it comes to collecting evidence and drawing factual inferences in [the national security] area, the lack of competence on the part of the courts is marked.") (citation and internal quotation marks omitted); Reno v. American-Arab Anti-Discrimination Comm., 525 U.S. 471, 491 (1999) ("a court would be ill-equipped to determine [the] authenticity and utterly unable to assess [the] adequacy" of the executive's security or foreign policy reasons for treating certain foreign nationals as a "special threat"); Regan v. Wald, 468 U.S. 222, 243 (1984) (giving the "traditional deference to executive judgment" in foreign affairs in sustaining President's decision to restrict travel to Cuba against a due process challenge).

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

F. Retention

Under the [redacted] Order, the PR/TT metadata was available for querying for four and one-half years, after which it had to be destroyed. [redacted] 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 [redacted] Opinion at 70-71. Pursuant to the government's proposal, the retention period would be extended to five years. [redacted] 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. [redacted] Response at 24. The Court is satisfied that the relatively small extension of the retention period that is sought by the government is justified by the administrative benefits that would result.

G. Oversight

The government proposes to employ an internal oversight regime that closely tracks the oversight provisions adopted by the Court in the [redacted] 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 [redacted] Order at 13-16, with [redacted] Alexander Decl. at 29-30. There is, however, one significant difference. The [redacted] 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." [redacted] 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 [redacted] 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 [redacted] 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. [redacted]

[redacted] 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 [redacted] Order. Compare [redacted] Alexander Decl. at 31, with [redacted] 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. Se[redacted] 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

[redacted] however, the 30-day reports will no longer include a discussion of "changes in the description of the [redacted] . . . or in the nature of the communications carried thereon." See [redacted] Order at 16. Like the [redacted] 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." [redacted] Alexander Decl. at 31.

The [redacted] 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 courterterrorism information or to assess its importance) had been followed. See [redacted] Order at 17. The government's proposal does not include such a requirement. In light of NSA's historical problems complying with the requirements for disseminating PR/TT-derived information, the Court is not prepared to eliminate this reporting requirement altogether. At the same time, the Court does not believe that weekly reports are still necessary to ensure compliance. Accordingly, the Court will order that the 30-day reports described in the preceding paragraph include a statement of the number of instances since the preceding report in which NSA has shared, in any form, information obtained or derived from the PR/TT metadata with anyone outside NSA. For each such instance in which United States person information has been

shared, the report must also include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand the counterterrorism information or to assess its importance.

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

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

A. The [redacted] Order

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

50 U.S.C. § 1809(a)(2).

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

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

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

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

---

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

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

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

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

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

pertinent part, as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States." 50 U.S.C. § 1801(f)(2).[83] For purposes of this definition of "electronic surveillance," "contents" is defined in Section 1801(n) to include, among other things, "any information concerning the identity of the parties" to a communication "or the existence . . . of that communication."[84] "Wire communication" is defined as "any communication while it is being carried by a wire, cable, or other like connection

---

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

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

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

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

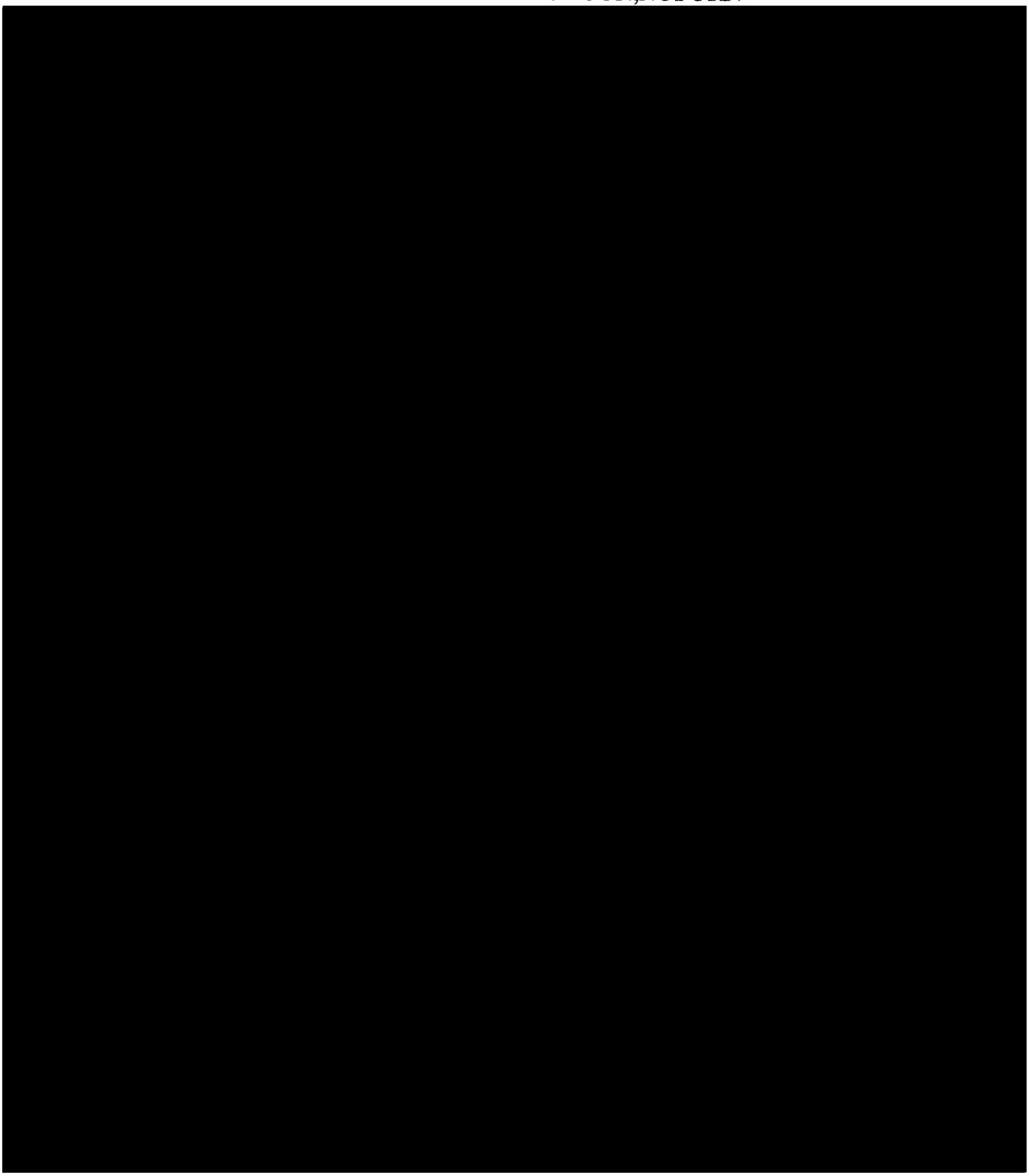
The unauthorized portion of the prior PR/TT collection includes some information that meets all four of these criteria. First, there is no question that the prior collection was acquired through the use of "electronic, mechanical, or other surveillance devices." See, e.g., [redacted] Decl. at 9 (describing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

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

the unauthorized collection included: [redacted] 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]

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(*l*). [redacted]



[redacted]

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

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

[redacted]

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

[redacted]

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

---

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

(continued...)

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

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

There is one additional category of information to consider – overcollected information that is not subject to Section 1809(a)(2). The Court is not well positioned to attempt a comprehensive description of the particular types of information that are subject (or not) to Section 1809(a)(2)'s prohibition, but it appears that some of the overcollected data is likely to fall outside its reach. For example, NSA may have no way to determine based on the available information whether a particular piece of data relates to a communication obtained from the [redacted] Similarly, it may not be apparent from available information whether the communication to which a piece of data relates is to or from a person in the United States, such that acquisition constituted electronic surveillance as defined at Section 1801(f)(2).

---

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

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

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

using the overcollected information. The Court has no basis to question that assertion. Furthermore, high-level officials at the Department of Justice and NSA have personally assured the Court that they will closely monitor the acquisition and use of the bulk PR/TT collection to ensure that the law, as reflected in the Court's orders, is carefully followed by all responsible officials and employees. In light of the government's assertions of need, and in heavy reliance on the assurances of the responsible officials, the Court is prepared – albeit reluctantly – to grant the government's request with respect to information that is not subject to Section 1809(a)(2)'s prohibition. Hence, the government may access, use, and disseminate such information subject to the restrictions and procedures described above that will apply to future collection.

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

VI. Conclusion

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

Signed [redacted] P02:37 _____ E.T.
Date Time

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

[redacted]