THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

HTTP://WWW.BLACKVAULT.COM

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

All redacted information exempt under b(1) and/ or b(3) except where otherwise noted.

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COU[redacted]

WASHINGTON, D.C.

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

PM 1:43

[redacted]

[redacted]

Docket Number: PR/TT

MEMORANDUM OF LAW AND FACT IN SUPPORT OF APPLICATION FOR PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES

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

Classified by: David S. Kris, Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: [redacted]

INTRODUCTION (U)

The nature of the Internet allows terrorists to conceal their communications within plain sight – commingled with the voluminous quantity of legitimate, non-terrorist related communications that occur every day. Analytic tools used in ongoing investigations enable the Government to sift through and identify terrorist communications. Use of such tools requires the collection of and access to bulk quantities of metadata associated with Internet communications (not including the substance, meaning, or purport of any communications).[1] The pen register and trap and trace provisions of Title IV of the Foreign Intelligence Surveillance Act of 1978, as amended, authorize the Government to obtain such access.[2] ~~(TS//SI//NF)~~

In a series of authorization orders issued between July 2004 and [redacted] this Court authorized bulk pen register collection under FISA. On [redacted] that authority expired, and the Court issued an order generally barring access to stored metadata that was collected during the preceding 4½ years. The current Application seeks authority to reinitiate bulk pen register collection on terms similar, but not identical, to those authorized in the prior orders, and to access the previously collected metadata. ~~(TS//SI//NF)~~

[redacted]

[2] For simplicity, we use the term "pen register" in this document to include both pen registers and trap and trace devices. (U)

1. Facilities. The Court's prior orders allowed NSA to conduct surveillance on [redacted] The attached Application for Use of Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes ("Application") seeks authority to conduct pen register surveillance on [redacted] This issue is discussed in more detail in Part I.C.2. of this Memorandum. ~~(TS//SI//NF)~~

2. Metadata. The prior authorization orders allowed NSA to acquire certain types of metadata from e-mail [redacted] although as described in the Report of the United States in docket number PR/TT [redacted], filed on [redacted] ("Compliance Report"), NSA was also collecting other types of metadata outside the scope of the prior orders. The new Application seeks authority to acquire all of the metadata NSA was previously acquiring, including metadata from [redacted] The Application also seeks access to all previously collected metadata now residing in NSA's databases, because that metadata, some of which was obtained in violation of the Court's prior orders, is nonetheless within the scope of the pen register statutes, the Fourth Amendment, and the current proposed authorization order, and is essential to the proper functioning of the pen register surveillance program. This issue is discussed in more detail in Parts I, II, and III of this Memorandum. ~~(TS//SI//NF)~~

3. Minimization. The prior authorization orders required adherence to certain minimization procedures, particularly with respect to the handling of query results that have been simplified or eliminated in the Application. We believe that certain of these procedures are unnecessary because query results represent a relatively small amount of information that is most relevant to foreign intelligence needs. In light of the requirement that analysts may query the bulk metadata only with an identifier[3] as to which there is reasonable, articulable suspicion ("RAS") that it is used by one of the identified targets, query results are effectively needles drawn from the haystack. Accordingly, this Application proposes adherence to the standards set out in United States Signals Intelligence Directive No. SP0018 (1993) ("USSID 18") to any results from queries of the metadata disseminated outside of NSA in any form. In addition, prior to disseminating any U.S. person information outside NSA, certain NSA officials must determine that the information identifying the U.S. person is in fact related to counterterrorism information and is necessary to understand the counterterrorism information or assess its importance. This issue is discussed in more detail in Part III.C.3. of this Memorandum. ~~(TS//SI//NF)~~

* * *

This memorandum has two main parts. It begins with a background discussion of [redacted] ("Foreign Powers") targeted in the Application, the threat they pose, their use of the Internet, and the relevance and value to U.S. national security of metadata collection in bulk. The background discussion also summarizes how the bulk data is analyzed and some of the

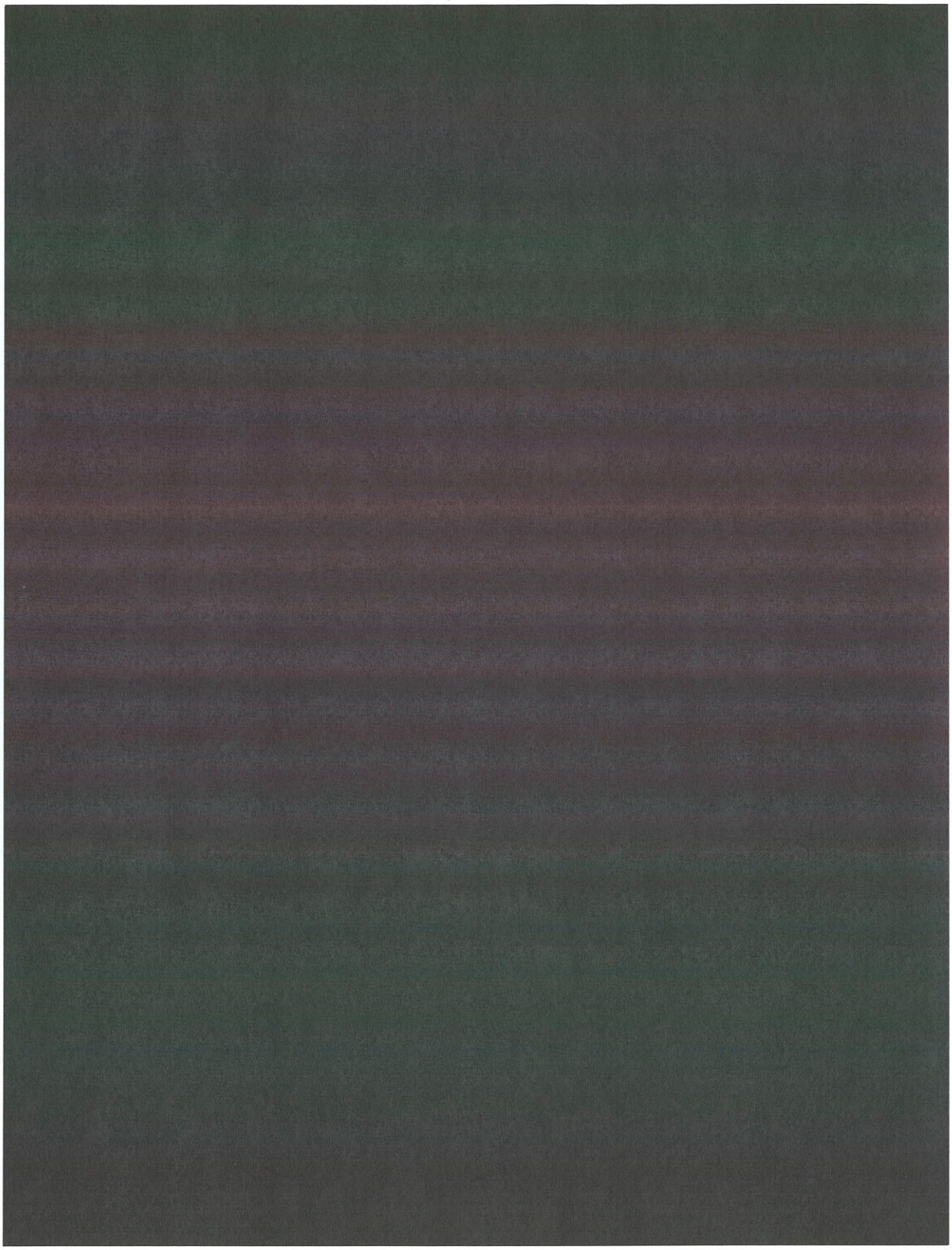
[redacted]

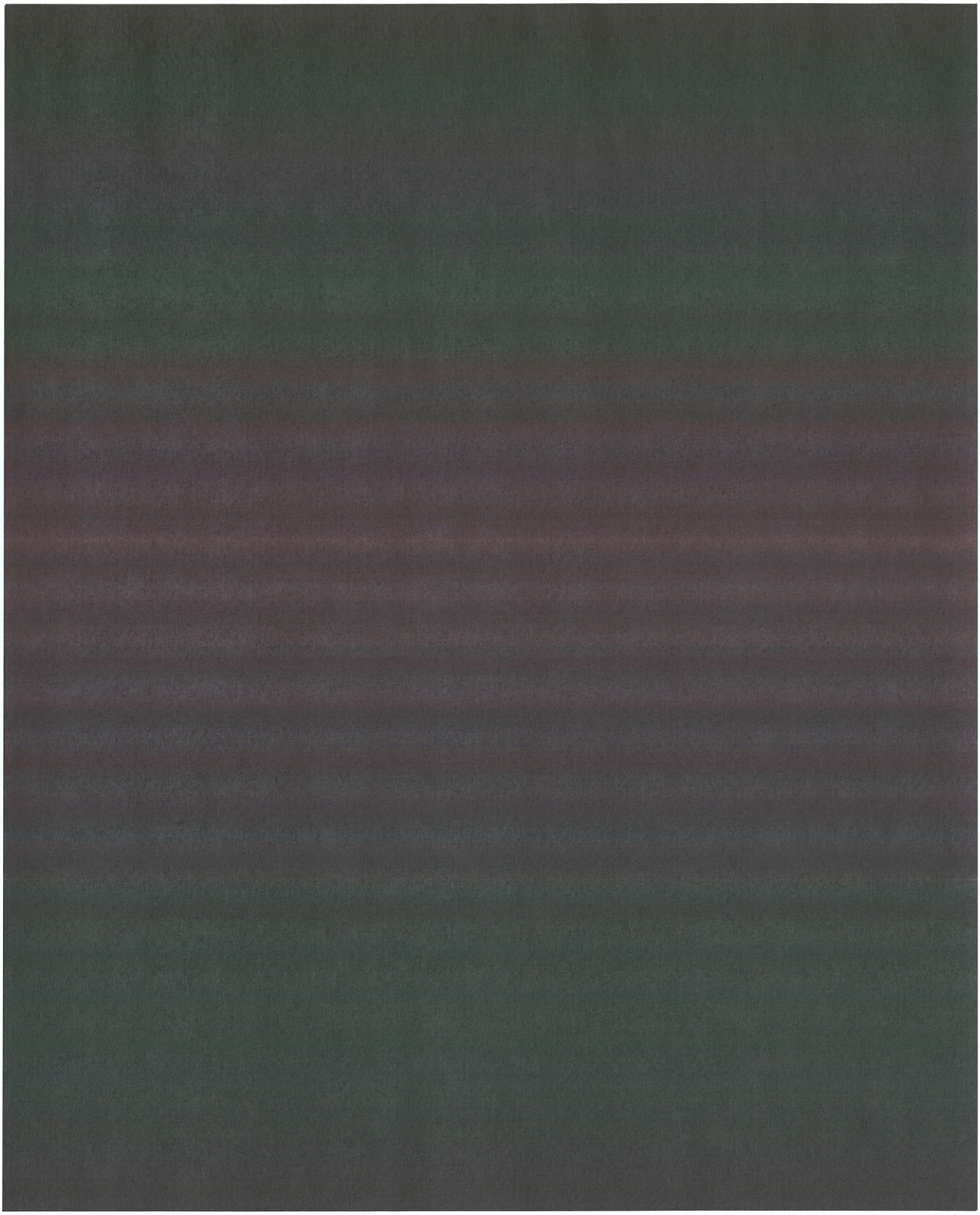
oversight mechanisms that apply to that analysis. The memorandum then sets out a legal analysis of the bulk metadata collection proposed in the Application, including a summary of argument and a detailed legal argument. The legal argument addresses, among other things, the scope of the applicable pen register statutes, the relevance of the data collected, the nature of the metadata proposed to be collected under those statutes, the constitutionality of such collection under the Fourth Amendment, and the issue of access to previously collected metadata that now resides in Government databases. ~~(TS//SI//NF)~~

BACKGROUND

I. Foreign Powers Threat (U)

As demonstrated in previous filings by the Government in matters before this Court, the Foreign Powers targeted in the attached Application present persistent, lethal, and long-term threats to the United States and its interests abroad. A document recovered from [redacted] Declaration of Michael E. Leiter, Director of the National Counterterrorism Center ("NCTC") (filed at docket number [redacted]) ("NCTC Declaration"), at 6. At the same time, according to the U.S. Intelligence Community (IC), [redacted] *Id.* at 89. [redacted] *Id.* The following summary of the threats posed by these Foreign Powers is supported by the NCTC Declaration, which provides greater detail on the targeted Foreign Powers' terrorist activities. ~~(TS//HCS//NF)~~





II. Foreign Powers' Use of the Internet ~~(S)~~

As explained in detail in the Declaration of General Keith B. Alexander, U.S. Army, Director of the NSA ("DIRNSA") in support of the Application (the "DIRNSA Declaration"), terrorists use Internet communications for many of the same reasons as the average person: [redacted]

[redacted]

[redacted] *Id.* Use by terrorists of the specific techniques noted above and detailed in the DIRNSA Declaration demonstrates why it is necessary for NSA to collect and maintain access to a repository of bulk metadata associated with Internet communications in order to best protect against acts of international terrorism against the United States and its interests. ~~(S//SI)~~

While all Internet communications are potentially the source of valuable foreign intelligence information, NSA believes that metadata associated with [redacted] is of particular importance. *Id.* ¶ 14 n.9. [redacted] *See* Declaration of Lieutenant General Keith B. Alexander, U.S. Army, Director of the NSA, Ex. A to the Compliance Report, at 20-23. ~~(TS//SI//NF)~~

NSA's experience has shown that terrorists use [redacted] DIRNSA Decl. ¶ 14 n. 9. [redacted]

A. Discovering the Enemy: Metadata Analysis ~~(TS//SI//NF)~~

While the Foreign Powers' exploitation of the Internet poses a daunting challenge to the IC, it also presents a great opportunity. As summarized above and described in greater detail in the DIRNSA Declaration, [redacted]

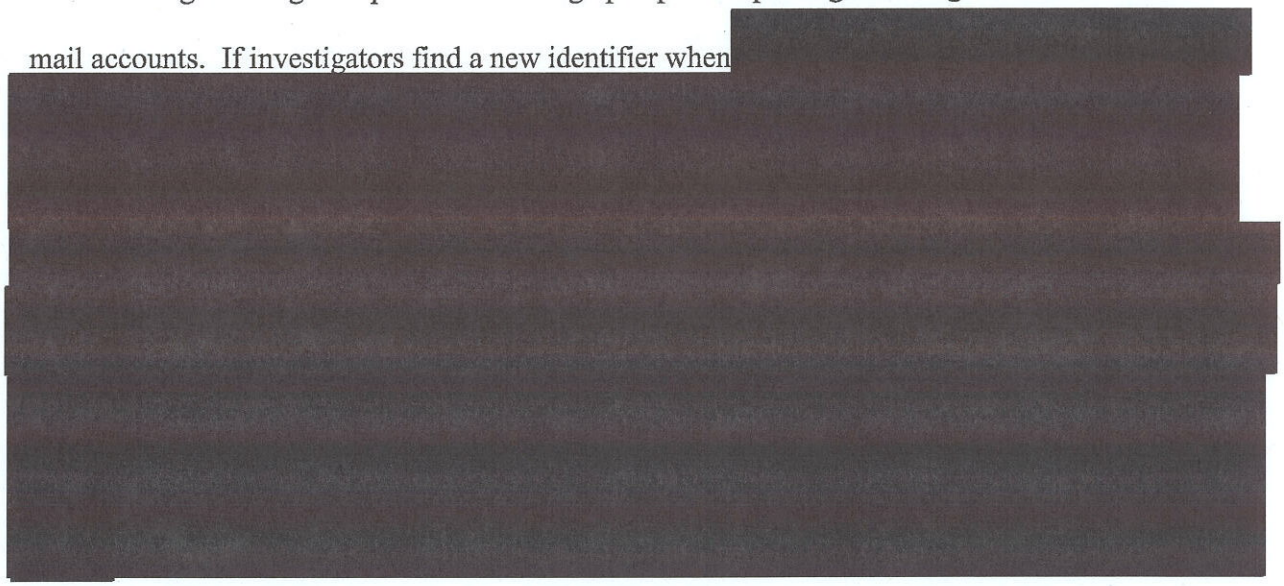
Analysis of the metadata from this Internet traffic can be a powerful tool for discovering enemy communications. However, Foreign Powers take affirmative and intentional steps to [redacted]

[redacted] *Id.* ¶ 21. Identifying these enemy communications in the billions of bits of Internet traffic, however, is like finding a needle in a haystack. For analysts to have the best chance at finding the terrorists, they need a mechanism to convert the Internet stream of communications traffic into something that can be searched in a targeted way. The mechanism for accomplishing that is the extraction of the metadata from the stream of Internet communications (without collecting the content of the communications) and storing it in a database for later analysis. Collecting metadata is the best avenue for solving this fundamental problem: although investigators do not know exactly where the terrorists' communications are hiding in the billions of bits of data flowing through the United States today, we do know that they are there, and if we place the metadata in a repository now, we will be able to use it in a targeted way to find the terrorists tomorrow. *See id.* ¶¶ 21-23. ~~(TS//SI//NF)~~

Collecting metadata from that stream creates invaluable capabilities for analysts that are otherwise unavailable. Most significantly, it allows for retrospective "contact chaining." *See id.* ¶ 26. [redacted] By examining metadata that has been collected over a period of time, analysts can search to find the contacts associated with that "seed" identifier. The ability to see who communicates with whom may lead to the discovery of other terrorist operatives, or it may help to identify hubs or common contacts between targets of interest whose relationships were previously unknown. Indeed, NSA's systems would automatically identify not only the first tier of contacts made by the seed, but also the contacts associated with the first tier identifiers. *Id.* ¶¶ 22-25, n.12. Going

out to the "second hop" enhances the ability of analysts to find additional terrorist connections. A seed e-mail address, for example, may be in touch with several e-mail addresses previously unknown to analysts. Following the contact chain out to the second hop to examine the contacts made by those e-mail addresses may reveal a contact that connects back to a different terrorist-associated e-mail address already known to the analyst. *Id.* ¶ 24 n.12. ~~(TS//SI//NF)~~

The capabilities offered by such searching of collected metadata are vastly more powerful than chaining that might be performed through prospective pen registers targeted at individual e-mail accounts. If investigators find a new identifier when



ability to trace terrorist connections by chaining two steps out from the original target. Instead, to find that second tier of contacts, a new individual pen register would have to be targeted at each e-mail account identified in the first tier. The time it would take to acquire the new pen registers would necessarily mean losing valuable data. And the data loss in the most critical cases would only be increased by terrorists' propensity for frequently changing their e-mail addresses. *Id.* ¶ 27. ~~(TS//SI//NF)~~

As proposed in the Application, analysts would query the bulk data with e-mail addresses or other identifiers as to which there is reasonable, articulable suspicion ("RAS") that the

identifier is associated with one of the targeted Foreign Powers or individuals. *Id.* ¶¶ 24, 31.

[redacted] Successful exploitation of the Internet communications of the Foreign Powers requires that NSA is in a constant state of development and discovery, as the terrorists [redacted] Metadata analysis contributes to this critical target monitoring, development and discovery by providing information that an analyst can use to determine various intelligence information, including but not limited to [redacted] *Id.* ¶ 25. Thus, the collected metadata provides an invaluable capability that could not be reproduced through any other mechanism because it allows analysts to bridge the gap between a known identifier and an unknown identifier, even where a terrorist has practiced strict operations security. ~~(TS//SI//NF)~~

B. Targeting the Relevant Data for Collection ~~(S)~~

Performing the metadata analysis described above necessarily requires collecting data in bulk. In other words, it entails collecting data on a significant number of communications that will not ever be found to have a connection with terrorists. The breadth of the collection, however, is necessary. The very reason for collecting the data to preserve it for later analysis is that it is [redacted]

[redacted] Effective metadata analysis requires broad collection and archiving of metadata. *See id.* ¶¶ 21-22. ~~(TS//SI//NF)~~

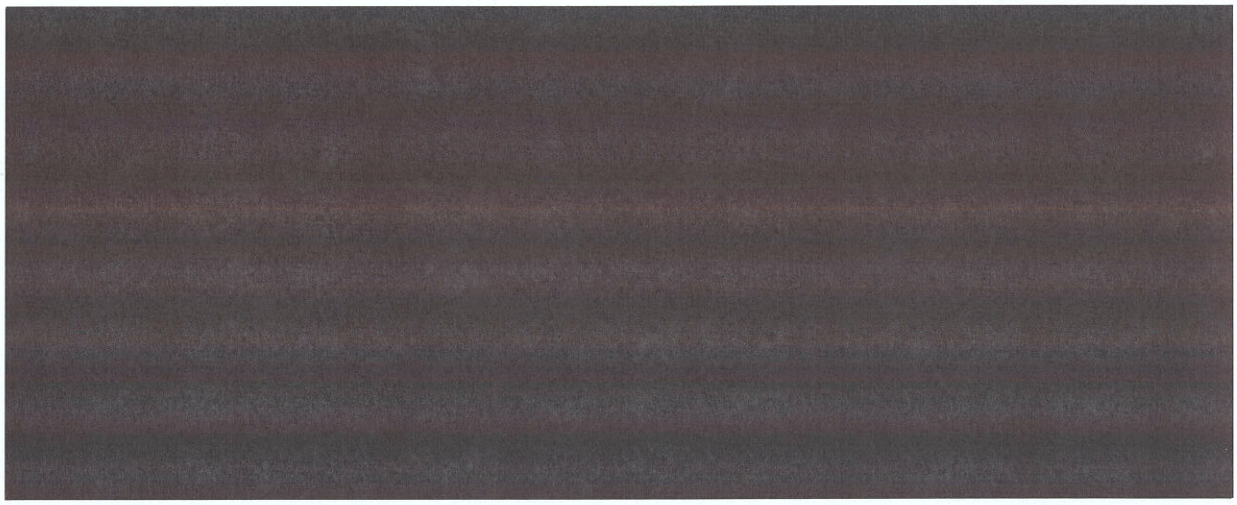
NSA will [redacted]

As discussed in more detail in Part II of this memorandum, that is consistent with the pen register statutes, which require specification of the "location" of relevant facilities, "if known." 50 U.S.C. § 1842(d)(2)(A)(iii). ~~(TS//SI//NF)~~

Under the Application, NSA's extraction of metadata would focus upon certain categories of data that are present [redacted] In particular, the NSA's current metadata collection efforts are focused on [redacted] types of data that fit in [redacted] categories. *Id.* Tab 2. Those [redacted] categories are communications addressing information, [redacted] The [redacted] types of metadata are [redacted] *Id.* These

types of metadata are useful in the investigation and analysis regarding the Foreign Powers through contact chain queries, a sophisticated means of identifying associations among individuals through exploitation of Internet communications metadata. *Id.* ¶¶ 23-24. ~~(TS//SI//NF)~~

All of the information collected by NSA's collection and retention systems would be subject to validation at collection and some of it would be subjected to multi-level validation before being stored in the NSA's repositories. An example of these validation checks are



The ability of NSA analysts to access the information collected under docket number PR/TT [redacted] and previous dockets is vital to NSA's ability to fully carry out its counterterrorism intelligence mission. *Id.* ¶ 13 n.6. Without access to that data, there would be [redacted]. *Id.* ~~(TS//SI//NF)~~

C. Searching the Metadata ~~(S)~~





[redacted] *Id.* ¶ 17. [redacted]

Id. ¶ 17. [redacted]

Id. ¶ 18. [redacted]

Id. ¶ 17. ~~(TS//SI//NF)~~

After the NSA has collected and retained the metadata, the use of that data will be subject to strict procedures and safeguards. First, NSA will store and process the collected metadata in repositories within secure networks under NSA's control. *Id.* ¶ 29. The metadata will carry unique markings such that software and other controls (including user authentication services) can restrict access to it to only authorized personnel. *Id.* NSA analytic personnel will query the metadata repository solely with RAS-approved identifiers (such as an e-mail address). *Id.* ¶¶ 24, 31.

The repositories will store, and the queries will address, metadata from the prospective collection proposed in the Application, as well as data obtained from the authority in docket number PR/TT [redacted] and previous dockets. The ability of NSA analysts to access the information collected under docket number PR/TT [redacted] and previous dockets is vital to NSA's ability to fully carry out its counterterrorism intelligence mission. *Id.* ¶ 13 n.6. Without access to that data, there will be a substantial gap in the information available to NSA. *Id.* ~~(TS//SI//NF)~~

Second, NSA will apply the procedures to ensure appropriate dissemination of the metadata. NSA will apply the minimization and dissemination requirements and procedures of Section 7 of USSID 18 to any results from queries of the metadata disseminated outside of NSA in any form. *Id.* ¶ 32. In addition, 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 Sharing 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.* ~~(TS//SI//NF)~~

Third, NSA's collection, access, and dissemination of information obtained pursuant to the authority requested in the Application will be subject to rigorous internal and external oversight. At NSA, the Office of the Director of Compliance (ODOC), the Office of the General Counsel (OGC), and the Inspector General (IG) will conduct oversight of the activities described in the Application and Declaration; oversight will also be conducted by the National Security Division (NSD) of the Department of Justice (DOJ). In addition, the Office of the Director of National Intelligence (ODNI) has independent responsibility over the IC and must ensure that NSA's intelligence activities are conducted in compliance with the law. Accordingly, ODNI personnel may participate in the oversight activities described below. Specifically:

(i) NSA's OGC and Office of the Director of Compliance (ODOC) will ensure that personnel with access to the metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the metadata and the results of queries of the metadata and will maintain records of such training. OGC will provide NSD/DoJ with

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

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

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

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives will meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of the metadata collected to ensure that only those categories or types of information described in Tab 2 are being collected. The results of this meeting will be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

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

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

(vii) Prior to implementation, all proposed automated query processes will be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

DIRNSA Decl. ¶ 34. ~~(TS//SI//NF)~~

Finally, approximately every thirty days, NSA shall file with the Court a report that includes a discussion of the queries made since the last report and NSA's application of the RAS standard. In addition, should the Government seek renewal of the requested authority, NSA shall also include in its report detailed information regarding any new facility proposed to be added to such authority and a description of any changes proposed in the collection methods, to include functioning and control of the pen registers and trap and trace devices. *Id.* ¶ 35. ~~(TS//SI//NF)~~

SUMMARY OF ARGUMENT

1. The pen register provisions in FISA authorize the Government to apply to the Court "for an order . . . authorizing or approving the installation or use of a pen register or trap and trace device" where two essential requirements are met. 50 U.S.C. § 1842(a)(1).[5] (U)

The first requirement is that the pen register be installed or used for certain specified investigations. *Id.* In particular, a pen register may be sought "for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order." *Id.* (U)

In this case, as explained in more detail in the Application, DIRNSA Declaration, and NCTC Declaration, the pen register order is sought for investigations to protect against international terrorism by [redacted] as well as other unknown persons in the United States and abroad who are affiliated with them. These investigations are being conducted by the FBI pursuant to guidelines approved by the Attorney General pursuant to Executive Order 12333, as amended, and to the extent the subjects of investigation are United States persons, the investigations are not being conducted solely on the basis of activities protected by the First Amendment. *See* 50 U.S.C. § 1842(a)(1). Thus, the

[5] The argument Section contains a more complete discussion of all requirements for issuance of a pen register order. This summary focuses only on the most significant requirements. (U)

first requirement in the statute is met. In this respect, the current Application is no different from Applications previously granted by this Court. ~~(TS//SI//NF)~~

The second requirement is that the pen register Application include 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." 50 U.S.C. § 1842(c)(2). In this case, as explained in more detail in the DIRNSA Declaration and elsewhere in the Application, the information sought by the pen register is "foreign intelligence information" which 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. Thus, the second requirement is met. The essential theory of relevance advanced in the current Application remains what it was in prior Applications granted by the Court – *i.e.*, that data collected in bulk is relevant to the ongoing investigations because of the analysis that bulk collection permits, even if the vast majority of the collected metadata does not in fact pertain to any terrorist. ~~(TS//SI//NF)~~

Where the requirements are met, the statute provides that a judge of this Court "shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device." 50 U.S.C. § 1842(d)(1). The Court's order itself must satisfy three main requirements that are set forth in the statute. (U)

First, the order "shall specify" the "identity, if known, of the person who is the subject of the investigation." 50 U.S.C. § 1842(d)(2)(A)(i). In this case, as discussed above and in the DIRNSA Declaration and elsewhere, the "persons" who are the subjects of the investigations are the Foreign Powers and unknown persons in the United States and abroad who are affiliated with

them. *See* 50 U.S.C. §§ 1801(a), (m), 1841(1) (definition of "person" includes foreign powers, such as international terrorist groups and foreign governments). Again, in this respect the current Application is no different than other Applications previously granted by the Court. ~~(TS//SI//NF)~~

Second, the Court's order must also specify "the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." 50 U.S.C. § 1842(d)(2)(a)(ii). In this case, as discussed in the DIRNSA Declaration, those persons are certain providers of telecommunications and related services, [redacted] *See* 50 U.S.C. §§ 1801(m), 1841(1) (definition of "person" includes corporations). Prior Applications likewise applied to telecommunications providers. ~~(TS//SI//NF)~~

Third and finally, the Court's order must 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 and, in the case of a trap and trace device, the geographic limits of the trap and trace order." 50 U.S.C. § 1842(d)(2)(a)(iii). The current Application proposes a different approach to this third and final element of the Court's order. ~~(TS//SI//NF)~~

a. At the outset, the current Application would expand the list of "attributes" of communications that may be collected. Prior orders authorized collection of [redacted] categories of metadata from e-mail [redacted] communications, and the current Application refers to [redacted] categories composed of [redacted] types. By way of illustration, [redacted] As

explained in Tab 2 to the DIRNSA Declaration, NSA will not collect any [redacted] without the Court's prior approval. ~~(TS//SI//NF)~~

As explained in Part I.C. of this Memorandum, all of the metadata to be collected under the current Application – including metadata types not previously authorized for collection – are within the scope of the pen register statutes, because all are "dialing, routing, addressing, and signaling information" and none is "contents."[6] Congress did not define the terms "dialing, routing, addressing, or signaling information," and these terms should be read in accordance with their broad ordinary meaning. Even if some of the metadata that is the subject of the Application is not "dialing, routing, addressing, or signaling" information, it may still be collected under the pen register statutes, because the statutes may be read to permit a pen register to acquire all communications information other than the "contents" of communications. That interpretation follows from the text of the statute and the legislative history of the USA PATRIOT Act. Pub. L. No. 107-56, § 206, 115 Stat. 272, 282 (2001). ~~(TS//SI//NF)~~

---

[6] As the Court is aware, the terms "pen register" and "trap and trace device" as used in FISA are defined in 18 U.S.C. § 3127, part of the U.S. Code chapter governing pen register surveillance in criminal cases. 50 U.S.C. § 1841(2). Under Section 3127(3), a "pen register" is 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." Similarly, a trap and trace device is a device or process which "captures the incoming electronic or other impulses which identify the originating number or other 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." 18 U.S.C. § 3127(4). ~~(TS//SI//NF)~~

It is difficult to provide a one-to-one comparison between what was collected in the past pen register program and in the current Application because the types of data have been re-organized in this Application to provide a better organizational framework. That said, the general description of data that is sought under this Application that was not the subject of any of the previous orders are metadata [redacted] *See* DIRNSA Decl. Tab 2. The Compliance Report filed in docket PR/TT [redacted] provides an exhaustive account of the specific types of metadata that were collected outside the authority of the previous pen register Orders. The authority sought in this Application includes the authority to collect that metadata, which the Government submits may be lawfully collected under the authority of the pen register statute. ~~(TS//SI//NF)~~

Congress intended the USA PATRIOT Act's amendments to "reinforce the statutorily prescribed line between a communication's contents and non-content information" – a line that it characterized as "identical to the constitutional distinction drawn by the U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979)." H.R. Rep. No. 107-236, at 53 (2001). In other words, "dialing, routing, addressing, and signaling information" and "contents" may be read as mutually exclusive categories that together define the universe of information that might be acquired (with the appropriate authorization) from a wire or electronic communication. Accordingly, a pen register may collect all non-content information from the communications passing through the transmission facility to which it is attached or applied, where "content" is defined as "any information concerning the substance, purport, or meaning of" a wire or electronic communication. 18 U.S.C. §§ 2510(8), 3127(1).[7] ~~(TS//SI//NF)~~

[redacted]

[7] Even if the Court were to disagree with this conclusion, and identify some intermediate data that are neither "contents" nor "dialing, routing, addressing, or signaling information," a pen register may collect that intermediate data. To qualify as a pen register, a device or process must capture, record or decode dialing, routing, addressing, and signaling information, but nothing in the statutory definition forbids the additional acquisition of other information transmitted by a wire or electronic communications facility, as long as that other information is not content or billing information. (U)

[redacted] Information that is both located in the appropriate field and is in the appropriate format for addressing is by definition "addressing information." ~~(TS//SI//NF)~~

Nothing in the pen register statutes requires "addressing information" to be used for the functional or technical purposes of addressing at the time of collection. The statute defines a pen register as a device or process that records or decodes addressing information "transmitted by an instrument or facility from which a wire or electronic communication is transmitted," as long as the information is not "contents," 18 U.S.C. § 3127(3). As proposed in the Application, NSA's pen registers will record and decode metadata only from Internet communications that are transmitted on the facilities identified in Tab 1 to the DIRNSA Declaration, including [redacted] sent e-mail [redacted]

b. The current Application also differs from its predecessors with respect to the "facilities" from which metadata will be collected. The Court's prior orders allowed NSA to conduct surveillance on [redacted]

[redacted] As explained in Tab 1 to the DIRNSA Declaration, the current Application treats [redacted] The statute requires nothing more. ~~(TS//SI//NF)~~

2. The collection and use of the bulk metadata sought in the Application is consistent with the Fourth Amendment. *See Smith v. Maryland*, 442 U.S. 735 (1979). In *Smith*, the Court held that "the installation and use of a pen register" was not a "search" under the Fourth Amendment. *Id.* at 736. Like the pen register in *Smith*, the pen register in this matter will acquire only the non-content attributes of communications indistinguishable from addressing information voluntarily conveyed to third parties. It therefore does not implicate the Fourth Amendment. ~~(TS//SI//NF)~~

Even if the Fourth Amendment protected some of the collected information [redacted] collection of that information would be reasonable, and therefore constitutional, in light of the unique protections governing the pen register bulk collection program, and under the "special needs" doctrine recognized by the Supreme Court and the Foreign Intelligence Surveillance Court of Review. *See, e.g., Griffin v. Wisconsin*, 483 U.S. 868,

[9] Even if the Court disagreed with that assertion, and concluded that there are [redacted] it would not affect the analysis, because FISA does not require specification of individual facilities for pen register surveillance, but only 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," and even then only if the location "is known." 50 U.S.C. § 1842(d)(2)(A)(iii) (emphasis added). In this respect, FISA's pen register provisions (Title IV) differ significantly from its provisions governing full-content collection (Title I), which require the Court to find probable cause that a foreign power or agent of a foreign power is using or about to use each of the facilities at which the surveillance will be directed, and the Court's orders to specify the nature as well as the location of each such facility. 50 U.S.C. § 1805(a)(2)(B), (c)(1)(B). ~~(TS//SI//NF)~~

873 (1987); *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002); *In re Directives*, 551 F.3d 1004, 1007 (FISA Ct. Rev. 2008). ~~(TS//SI//NF)~~

3. In addition to granting the Application for prospective collection, the Court should grant commensurate and continuing authority to query metadata previously collected. That is the case even though, as discussed in the Compliance Report, the prior pen register collection in certain ways exceeded the scope of the Court's orders. As detailed in the DIRNSA Declaration, without access to the previously collected information, the value of the pen register will be dramatically reduced. *See* DIRNSA Decl. ¶ 13 n.6. ~~(TS//SI//NF)~~

From the beginning, this Court has asserted a continuing jurisdiction over the bulk pen register program that is both prospective and retroactive, regulating in each authorization order the collection and querying of all data collected under all prior orders. The Government supported that assertion of jurisdiction in 2004, and continues to do so today in light of the unique nature of the bulk pen register program. That expansive jurisdiction, however, gives the Court authority to grant access to the stored metadata even though some of it exceeded the scope of the Court's prior orders. Indeed, the Court's rules give it discretion in this area, *see* FISC R. 10(c)(iv), and the Court should exercise that discretion to permit retention and querying of data that, although collected in violation of the Court's prior orders, is within the scope of the statute, Constitution, and the current proposed order, and is critical to the proper functioning of the bulk pen register surveillance program. The Court should not require destruction of the overcollected data, and should lift its [redacted] order generally barring access to the stored data. Additionally, NSA asserts that [redacted]

[redacted] DIRNSA Decl. ¶ 20 n.11. ~~(TS//SI//NF)~~

I. The Application Fully Complies with All Statutory Requirements. (U)

FISA provides a mechanism for the Government to obtain the metadata that is necessary to perform the type of contact chaining analysis described above that is vital for counterterrorism and foreign intelligence investigations. As this Court has previously ruled in docket number PR/TT [redacted] and subsequent orders renewing and modifying that authority, such data may lawfully be obtained using a pen register obtained pursuant to 50 U.S.C. § 1842.[10] The Government's Application satisfies all four statutory requirements of Section 1842(a)-(c), which are: (1) the device or process used to effect the surveillance must qualify as a "pen register"

---

[10] In docket number PR/TT [redacted] and subsequent applications renewing and modifying that authority, this Court authorized installation and use of pen registers similar to those described above. Those orders allowed NSA to collect, in bulk, metadata associated with e-mail [redacted] communications that traversed [redacted] In reliance on representations made by the Government since submission of the initial pen register application in 2004, the Court approved NSA's pen register collection as part of an effort to develop foreign intelligence on the activities of [redacted] The Court's [redacted] Order in docket number PR/TT [redacted] and preceding docket numbers extended authorization to target [redacted] The Court's [redacted] Order in docket number PR/TT [redacted] and preceding docket numbers extended authorization to target [redacted] (TS//SI//NF)

On [redacted] the Government orally notified the Court of a potential compliance problem. The compliance problem involved the collection of data that possibly fell outside the scope of the order, which permitted bulk collection of specified categories of information for e-mail [redacted] associated with investigations of the targeted Foreign Powers. A formal written notification to this Court followed on [redacted] On [redacted] this Court was informed of the Government's decision not to seek renewal at that time of the pen register collection in PR/TT [redacted] On [redacted] when the existing order expired, the Court entered an order directing that the Government not access for analytic or investigative purposes the information collected under the prior pen register orders unless the access was necessary to protect against an imminent threat to human life. Supplemental Order and Opinion, docket number PR/TT [redacted] at 5. This Court did authorize the Government to access the previously collected metadata for purposes of conducting non-analytic technical reviews. ~~(TS//SI//NF)~~

As detailed in the Compliance Report, the information collected included data that was not within the categories specified by the pen register orders. For the reasons stated herein, the data could lawfully have been collected under the pen register statute and the Fourth Amendment and indeed proposed for collection in the current Application. ~~(TS//SI//NF)~~

and/or "trap and trace device," 50 U.S.C. §§ 1841(2), 1842(a)(1); (2) the Application must have been approved by the Attorney General or a designated government attorney, 50 U.S.C. § 1842(c); (3) the Application must include the identity of the U.S. Government official seeking to use the pen register covered by the Application, 50 U.S.C. § 1842(c)(1); and (4) the Applicant must certify that the information "likely to be obtained" is foreign intelligence or is "relevant to an ongoing investigation to protect against international terrorism." 50 U.S.C. § 1842(c)(2). ~~(TS//SI//NF)~~

The second and third statutory requirements are clearly met. The Attorney General has approved the Application, and the Application specifies that the Director of the NSA is the government official seeking to use the pen register devices covered by the Application. The only requirements that merit further discussion are that the devices or processes used to effectuate the surveillance must qualify as pen registers and trap and trace devices and that the Application must contain a certification of relevance. This Court has previously found that bulk collection of metadata from e-mail [redacted] met the requirements of Section 1842, and should do so again here. ~~(S)~~

A. Scope of Review (U)

Section 1842(d) of FISA expressly limits the Court's discretion to consider an Application for a pen register. It states

> [u]pon an application made pursuant to this Section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device if the judge finds that the application satisfies the requirements of this Section. (U)

In keeping with the plain language of this provision, as the Government has argued to the Court in the past, judicial review of an Application for a pen register is limited.[11] In her Opinion and Order in docket number PR/TT [redacted] did not accept these arguments. *See* Opinion and Order, docket number PR/TT [redacted], at 26-27. Instead, Judge Kollar-Kotelly conducted an independent evaluation of the basis of the Certification of relevance, found it persuasive, and granted the Government's Application in docket number PR/TT [redacted]. The Government continues to believe that the language of the Certification should be determinative of this issue and incorporates those previously advanced arguments as if set forth more fully herein. However, acknowledging the Court's Opinion and Order in docket number PR/TT [redacted], this Memorandum of Law and Fact also discusses the relevance of the information sought to these ongoing investigations to protect against international terrorism. ~~(TS//SI//NF)~~

B. The Information Sought Through the Application is Relevant to an Ongoing Investigation to Protect Against International Terrorism. ~~(S)~~

The metadata sought through the Application is unquestionably relevant to an ongoing investigation to protect against international terrorism because it seeks to obtain non-content information relating to the Foreign Powers and those unknown individuals associated with them who may be plotting terrorist attacks and discover [redacted] as to how, and with whom, these Foreign Powers communicate while engaged in these terrorist conspiracies. The nature and volume of worldwide Internet communications provides a ready-made realm within which

[11] Section 1842(d)(1) directs that an order "shall" be entered by the judge if the Court finds that the Application satisfies Section 1842's requirements, one of which is that the Application contain a certification about the information likely to be obtained. 50 U.S.C. § 1842(c)(2). Like the criminal pen register provision upon which it is modeled (18 U.S.C. §§ 3121-27), FISA's pen register provisions limit judicial review to ensuring that the statutory requirements for an Application have been satisfied – *e.g.*, that the Application contains the required certification. *See United States v. Hallmark*, 911 F.2d 399 (10th Cir. 1990); *In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device*, 846 F. Supp. 1555 (M.D. Fla. 1994). The statute does not call for the Court to look behind the Certification or to conduct an independent review of the information likely to be acquired. ~~(S)~~

terrorists conceal their activities ostensibly within plain sight – through communications metadata processed through the same communications pathways as legitimate, non-terrorist related communications. That the majority of metadata collected previously, and that is proposed to be collected now, through this program will not be terrorist-related does not lessen the relevance of the information to these ongoing international terrorism investigations. Rather, when viewed in the context of the time span over which these terrorist groups conceptualize, plan, and carry out their terrorist attacks, the fact that the metadata relating to terrorist communications hides within the vast stream of otherwise legitimate Internet metadata only heightens the relevance of and necessity to collect the metadata sought in the Application. DIRNSA Decl. ¶¶ 14, 21-23. ~~(S)~~

Relevance here is not properly measured through scientific metrics or the number of reports issued over the course of a year and it does not require a statistical "tight fit" between the volume of proposed collection and the much smaller proportion of information that will be directly "relevant" to investigations of the Foreign Powers to protect against international terrorism. *See* Opinion and Order, docket number PR/TT [redacted], at 49-50. Rather, relevance here properly is measured in packets of metadata that, over an extended period of time, can help to fill in information that provides a more complete picture of the communications practices of these Foreign Powers and their agents. ~~(TS//SI//NF)~~

The metadata that has been and would be acquired through this collection is pertinent to the FBI's investigations into the Foreign Powers because, when collected and analyzed, the metadata provides assistance to investigators in putting together the complete picture of how these Foreign Powers and their agents communicate over extended periods of time. *See, e.g.*, 13 Oxford English Dictionary 561 (2d ed. 1989) ("relevant" means "[b]earing upon, connected

with, pertinent to, the matter in hand"); Webster's Third New Int'l Dictionary 1917 (1993) ("relevant" means "bearing upon or properly applying to the matter at hand . . . pertinent"); *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978) (noting that the phrase "relevant to the subject matter involved in the pending action" in Fed. R. Civ. Proc. 26(b)(1) has been "construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case"); Fed. R. Evid. 401 ("'Relevant evidence' means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."). ~~(TS//SI//NF)~~

Here, a substantial portion of the metadata that has been and will be collected does not relate to these Foreign Powers and their agents. That does not weigh against a determination that the information sought is relevant to an ongoing investigation to protect against international terrorism. To the contrary, as explained in the DIRNSA Declaration, this intelligence tool – one of many used by the Government in its efforts to counter the threat posed by these Foreign Powers – inherently requires collecting and storing large volumes of the metadata to enable later analysis -- analysis that may continue for years for it to be truly effective. Unless metadata is stored at the time of transmittal, it will be lost forever. DIRNSA Decl. ¶ 22. Therefore, all of the metadata collected is relevant because it is necessary for the success of the investigative tool. ~~(TS//SI//NF)~~

C. The Relevant Pen Register Statutes Are Satisfied. (U)

The collection devices[12] will record, decode, and capture data that is exchanged between Internet users The communications to be collected would fall into categories: sections I.C.3. and II.A. of this memorandum. ~~(TS//SI//NF)~~

1. The Proposed Collection Will Use "Pen Registers" and "Trap and Trace Devices" As Those Terms Are Defined By Statute. (U)

The devices described in the Application that will be used to accomplish the proposed collection satisfy the statutory definitions of "pen registers" and "trap and trace devices" in 18 U.S.C. §§ 3127(3) and (4) and incorporated into FISA by 50 U.S.C. § 1841(2). Title IV of FISA

[12] The pen register in the Application (TS//SI//NF)

authorizes the Attorney General or a designated attorney for the Government to apply to this Court

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

50 U.S.C. § 1842(a)(1). ~~(S)~~

Title IV of FISA expressly incorporates the definitions of the terms "pen register" and "trap and trace device" from 18 U.S.C. § 3127 for use under FISA's pen register provisions. 50 U.S.C. § 1841(2). That Section provides that a "pen register" is

> 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.[13]

18 U.S.C. § 3127(3).[14] Similarly, a "trap and trace device" is defined as

---

[13] The definition also states that devices or processes used for billing or recording as an incident to billing are not "pen registers." The devices the Government proposes using in its Application do not perform such billing services or collected related information. (U)

[14] "[W]ire communication" for purposes of this provision 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 (including the use of such connection in a switching station).

18 U.S.C. § 2510(1). "[E]lectronic communication" means "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 . . . but does not include . . . any wire or oral communication." 18 U.S.C. § 2510(12). The term "[c]ontents" includes "any information concerning the substance, purport, or meaning of [a particular] communication." 18 U.S.C. § 2510(8). These terms are incorporated into the chapter governing the use of pen registers and trap and trace devices. 18 U.S.C. § 3127(1). E-mail [redacted] "electronic communications" within the scope of the pen register statute. See S. Rep. 99-541 at 14 (1986) ("This term [electronic communications] includes electronic mail, digitized transmissions, and video teleconferences"); *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 461-62 (5th Cir. 1994). (U)

> 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.

18 U.S.C. § 3127(4). (U)

Pen registers historically were used to record the metadata associated with a particular telephone number. With the evolution in communications technology, some courts began to approve the installation and use of pen registers to collect metadata associated with an e-mail account. The USA PATRIOT Act amended Section 3127(3) and (4) of Title 18 to clarify that use of these devices was not limited to telephones[15] and could also be used on computers and cell phones.[16] Pub. L. No. 107-56, § 206, 115 Stat. 272, 282 (2001). Today, orders for use and installation of such devices for Internet communications are routinely granted by federal courts under 18 U.S.C. § 3123 (albeit not for bulk collection). Indeed, this Court has authorized the installation and use of devices substantially similar to the proposed collection devices here and did so after concluding that the collection devices satisfied the pen register statute. Opinion and Order, docket number PR/TT [redacted], at 13-17. ~~(TS//SI//NF)~~

2. The Pen Register Devices Will Collect Specified Attributes of Communications From Facilities [redacted] (U)

The Application explains how [redacted] devices will record, decode, and capture metadata in bulk for e-mail [redacted] communications transmitted by certain facilities. The Government is

---

[15] Prior to the amendment, a pen register was defined as "a device which records or decodes electronic or other impulses which identify the number dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3). Similarly, a trap and trace device was defined as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 18 U.S.C. § 3127(4). Thus, a pen register was generally used to record outgoing telephone numbers, and a trap and trace device was used to record incoming numbers. (U)

[16] *See* H.R. Rep. No. 107-236, pt. 1 at 53. (U)

not *required* to plead anything in its Application about the facility under Section 1842(c). However, Section 1842(d)(2) requires the Court's order approving the use of a pen register to specify the "identity, if known of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied" 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." 50 U.S.C. § 1842(d)(2)(A)(ii) & (iii). ~~(TS//SI//NF)~~

In the attached Application, the Government provides this Court with information sufficient to satisfy the statutory requirements for the issuance of an Order. Tabs 1 and 2 of the DIRNSA Declaration include: (1) [redacted] the facilities to which the pen registers and trap and trace devices are to be attached or applied – *e.g.*, [redacted] (2) the attributes of the communications to which the order applies, – *e.g.*, message addresses, such as badguy@[redacted] and (3) [redacted] facilities to which the pen registers and trap and trace devices are to be attached or applied. That level of specificity is ample for the type of collection conducted with a pen register. Use of a pen register does not constitute a search within the meaning of the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 220 (1979). Consequently, the Fourth Amendment's particularity requirement does not apply.[17] *Maryland v. Garrison*, 480 U.S. 79 (1987) (Warrant Clause of the Fourth Amendment

[17] Notably, the facilities requirement for Title IV is less substantial than for Title I of FISA. In contrast to Title IV, orders under Title I of FISA must specify, among other requirements, the "nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known." 50 U.S.C. § 1805(c)(1)(B) (emphasis added). Orders under Title IV of FISA require only "the location of the … facility" to which the pen register or trap and trace device is to be attached or applied and even that information only "if known." 50 U.S.C. § 1842(d)(2). Thus, the plain text of the requirements for orders under the two FISA provisions require differing degrees of descriptive detail for the facilities to which they apply, and the requirements of Title IV are less stringent than those required of Title I. ~~(S)~~

requires particularity describing the place to be search and the persons or things to be seized.).

~~(TS//SI//NF)~~

3. The Data That Would Be Collected Are Dialing, Routing, Addressing, or Signaling Information Properly Collected Under Section 1842. (U)

All of the data that would be obtained by the collection devices should be considered "dialing, routing, addressing, and signaling information" under a broad interpretation of those terms. That said, even under a narrow interpretation, the vast majority of the data that would be collected under the Application would properly be considered dialing, routing, addressing, and signaling information (and as discussed in the next part of this memorandum, all of the data would be properly collected because they are not the "contents" of a communication).

~~(TS//SI//NF)~~

No case law specifically addresses application of the terms "dialing, routing, addressing, or signaling" to all of the particular types of data that would be collected as proposed in the Application. But this Court has previously authorized the collection of most of the types of data in docket PR/TT [redacted] and previous dockets.[18] Some of these data, such as forms of message addresses like IP address and to/from information, have been found to be lawfully collected by a pen register. *See, e.g., United States v. Forrester*, 512 F.3d 500, 509-11 (9th Cir. 2008) (upholding pen register collection of to/from information, IP address, and total volume of data transmitted for e-mail messages). The remaining data should generally be viewed as the type of

[18] It is difficult to provide a one-to-one comparison between what was collected in the past pen register program and in the current Application because the types of data have been re-categorized in this Application to provide a better organizational framework. The data that are sought under this Application that was not the subject of any of the previous orders are metadata related to [redacted] *See, e.g.*, DIRNSA Decl. Tab 2. These are discussed at *infra*, 39-44. The Compliance Report provides an exhaustive account of the specific types of metadata that were collected outside the authority of the previous pen register Orders. The authority sought in this Application includes the authority to collect that metadata, which the Government submits may be lawfully collected under the authority of the pen register statute. ~~(TS//SI//NF)~~

[redacted] information transmitted in association with electronic communications that pen registers have traditionally collected. ~~(TS)~~

The terms "routing," "addressing," and "signaling" are not defined by Section 3127 and should be interpreted in light of their broad plain meanings.[19] "Routing" is technically defined as "the process of selecting the circuit path for a message." *Newton's Telecom Dict.* 786 (2006, 22nd Ed.). The term "route" is more generally defined as "an established or selected course of travel or action." *Webster's Collegiate Dict.* 1021 (1998, 10th Edition). Thus, "routing information" encompasses the path or means by which information travels or information about the path and means by which information travels. (U)

Similarly, "addressing information" is susceptible to broad interpretation. Newton's Telecom Dictionary describes an "address" as follows: "An address comprises the characters identifying the recipient or originator of transmitted data." *Newton's Telecom Dict.* 87. Webster's Collegiate Dictionary provides a similar definition of "address": "to identify (as a peripheral or memory location) by an address or a name for information transfer." *Webster's Collegiate Dict.* 13. Thus, "addressing information" may be understood to be information that identifies recipients of communications or participants in a communication. Moreover, addressing information may refer to people and/or devices. (U)

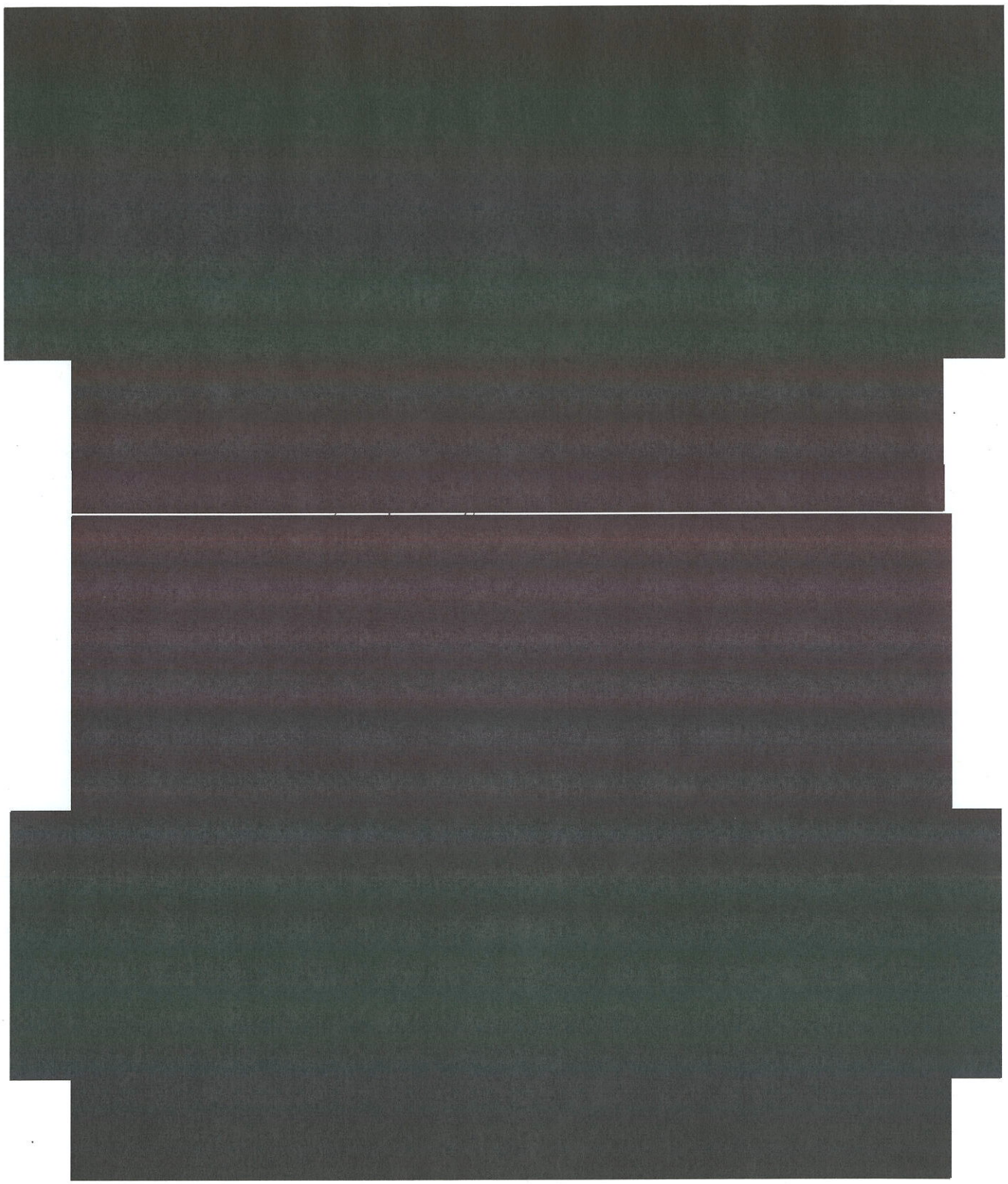
Lastly, "signaling information" also potentially has a broad meaning. "Signaling" information is generally understood to represent information transmitted by telephone systems to commence or terminate calls and to register the presence of a cell phone. *Newton's Telecom Dict.* 823. However, the meaning of that term should not be cabined to telephony and should be

[19] "Dialing" is much less ambiguous than the other terms. It presumptively relates to telephones, since the original version of the pen register provisions used that term since it was originally enacted to cover telephony. Accordingly, the Government does not believe that most of the data that would be collected could properly be considered "dialing information." ~~(TS)~~

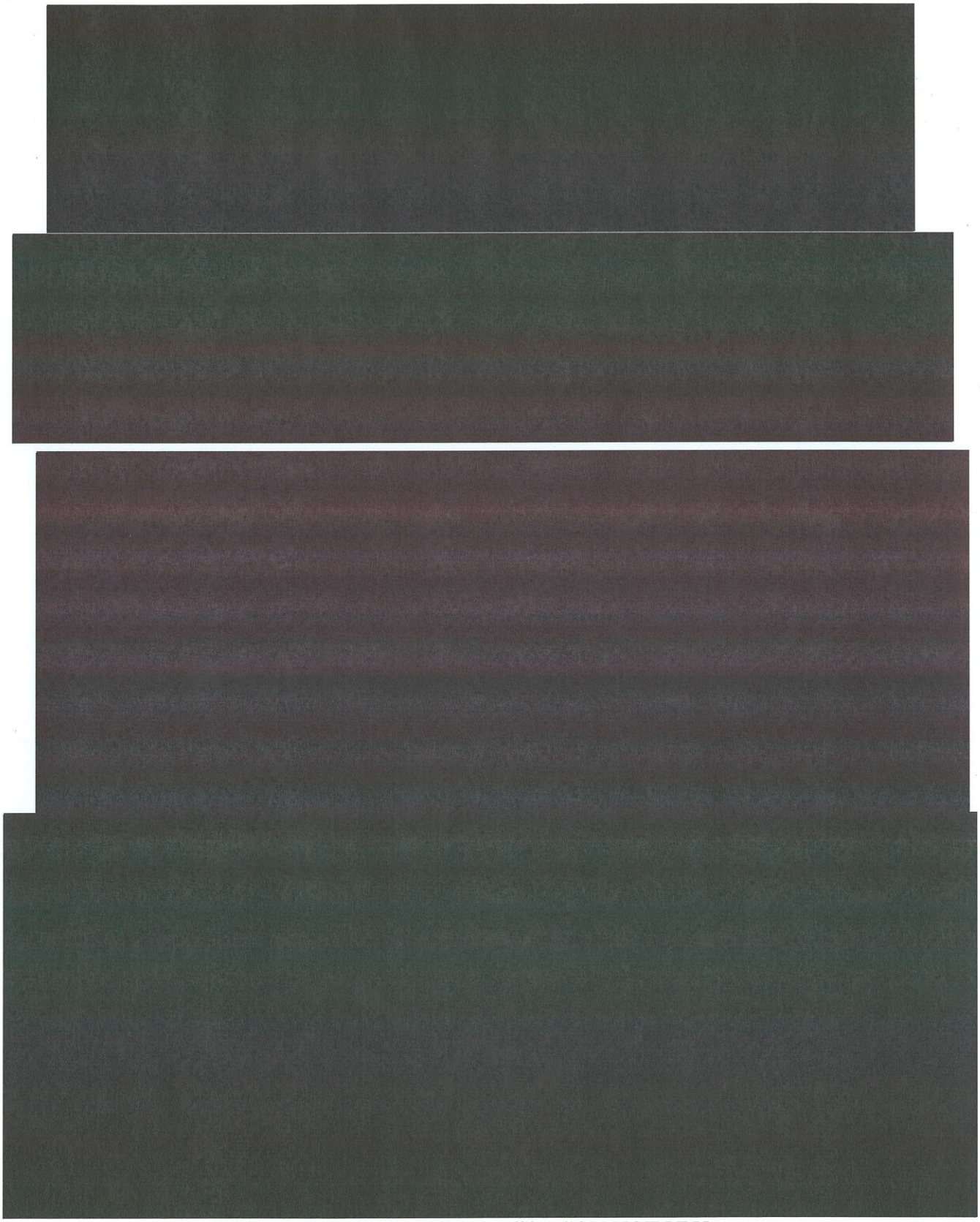
given broader application, because Congress intended each of these terms to apply to all forms of communications. H.R. Rep. No. 107-236 at 53 (terms were meant to apply "across the board to all communications, media, and to actual connections as well as attempted connections"). The less technical meaning of "signal" is "something that incites to action" or "conveys notice or warning." *Webster's Collegiate Dict.* at 1091. Thus, signaling information should be understood to include transmissions between communications devices (*e.g.*, the user's computer and an ISP's web server) that prompt certain actions or responses associated with a communication or register the presence of a device.[20] ~~(TS//SI//NF)~~

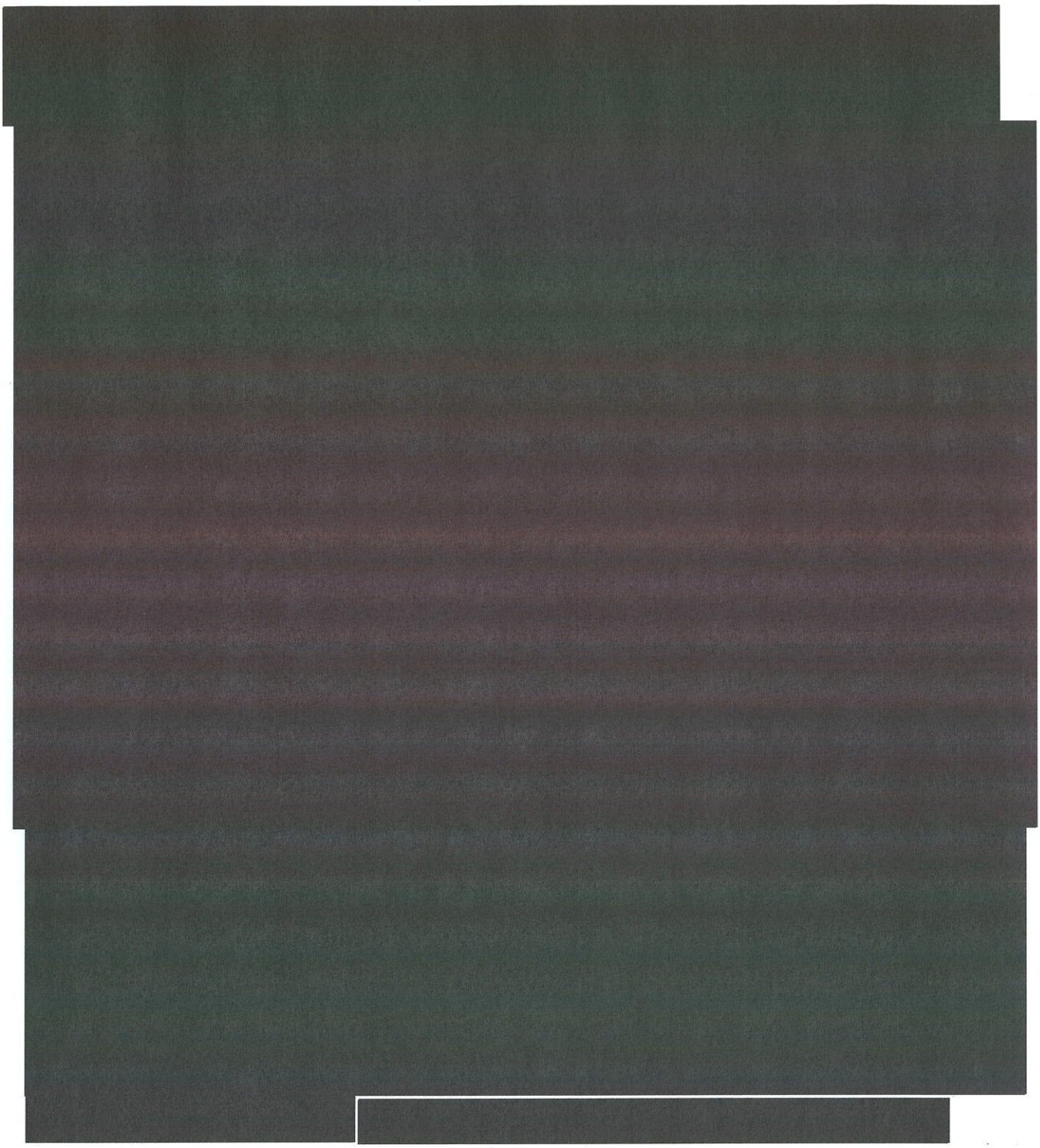
The legislative history suggests that Congress intended these undefined terms to be given broad effect, even beyond their conventional technical meanings. For example, the House Report states that "non-content information contained in the 'options field' of a network packet header constitutes 'signaling' information and is properly obtained by an authorized pen register or trap and trace device." H.R. Rep. No. 107-236 at 53 n.1. The options field of Internet packet header information does not conduct "signaling" in the conventional sense. Rather, it carries data used in the transmission of the packet such as time stamp, security, and routing information. Yet Congress made clear its intent in the legislative history that options field information is subject to collection as part of a pen register order. Accordingly, the Government submits that this Court should not rely on a narrow reading of these statutory terms and that all [redacted] of the attributes or data types specified in the DIRNSA Declaration are one or more of "routing," "addressing," or "signaling" information. ~~(TS//SI//NF)~~

[20] [redacted]



21



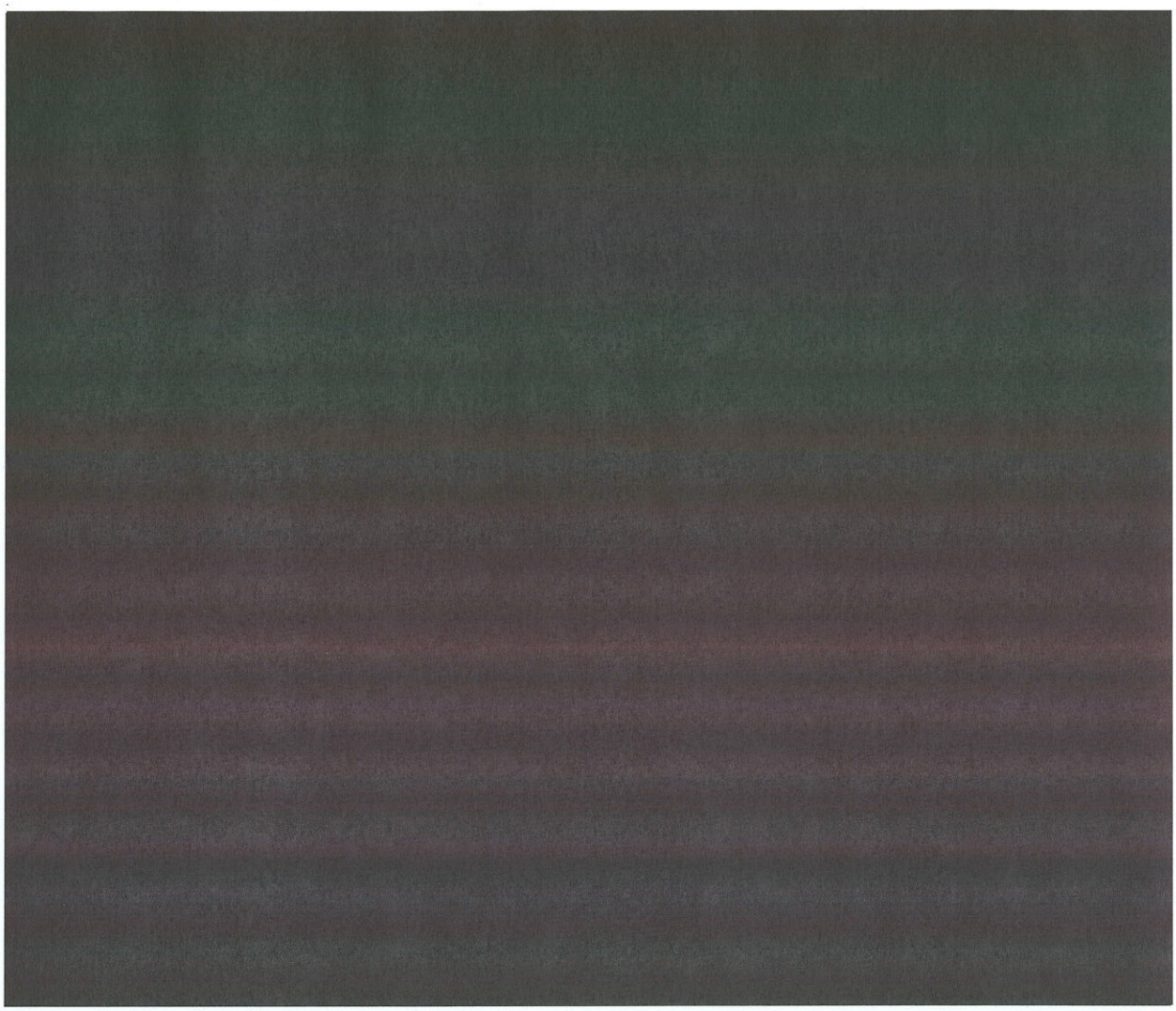


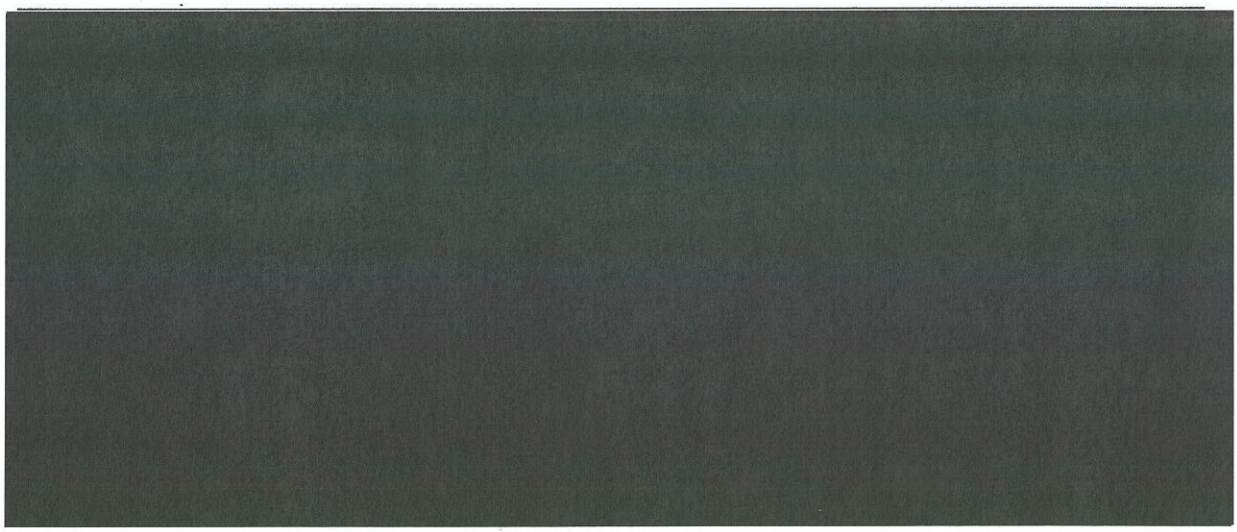
[redacted]

[redacted]

23 [redacted]

24 [redacted]





[redacted]

4. None of the Data That Would Be Collected by the Proposed Collection Devices Is Content. ~~(TS//SI//NF)~~

None of the data that would be collected under the Application are "contents," as defined by 18 U.S.C. § 2510(8). As this Court determined in docket number PR/TT [redacted], Section 2510(8) of Title 18, rather than Title I of FISA, supplies the operative definition of "contents" for purposes of FISA's pen register provision, 50 U.S.C. § 1842. When Congress added Section 1842 to FISA, it incorporated Title 18's definition of "contents" into FISA's pen register provision (Title IV) by expressly incorporating the Title 18 definitions of "pen register" and "trap and trace device," *see* 50 U.S.C. § 1841(2), which in turn rely on the definitions of "contents" in Title 18, *see* 18 U.S.C. § 3127. *See also* 50 U.S.C. 1801 (specifying the meanings of certain words, including "contents," "[a]s used in this title" – *i.e.*, title I of FISA).

~~(TS//SI//NF)~~

Section 2510(8) defines content to "include[] any information concerning the substance, meaning, or purport of the communication." The Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508 (1986), amended the definition of content under 18 U.S.C. § 2510(8) resulting in a narrower definition of content than under Title I of FISA. The FISA definition of content "includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 50 U.S.C. § 1801(n). Section 2510(8)'s amended definition omits any reference to "the identity of

the parties" or "the existence" of the communication. Thus, Section 2510(8)'s definition of content focuses only on information that reveals the meaning of a particular communication and specifically does not include information that identifies the parties to that communication. *See Jessup-Morgan v. Am. Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (holding that identifying information, such as identification of an account customer, is not content within Section 2510(8)); *see also Hill v. MCI WorldCom Commc'n, Inc.*, 120 F. Supp. 2d 1194 (S.D. Iowa 2000) (billing/invoice information and names, addresses and phone numbers of persons she called are not "contents" under Section 2510(8)). Further, Congress did not intend for transactional records to be considered content. S. Rep. No. 99-541 at 13 ("[T]he amended definition thus distinguishes between the substance, purport or meaning of the communication and the existence of the communication or transactional records about it.").[25] (U)

The data identified in Tab 2 of the DIRNSA Declaration are the type of [redacted] information that should not be considered "content," since they do not reveal the substance, purport, or meaning of the underlying communications. [redacted]

[redacted]

[25] The legislative history of the USA PATRIOT Act indicates that once pen registers were expressly made applicable to Internet communications, Congress had concerns about their potential to collect content information. H.R. Rep. No. 107-23 at 53. However, those concerns were focused on particular types of information that are [redacted]

[redacted]

Thus, the configuration of the pen register devices will help avoid concerns that have been identified by courts in other contexts about the collection of "content" information by devices that the Government has sought to install and use under Title 18's pen register provisions. For instance, in *Brown v. Waddell*, 50 F.3d 285 (4th Cir. 1995), the Court of Appeals found that a clone pager that collected phone numbers pursuant to the criminal pen register provision (18 U.S.C. §§ 3121-27) was not a "pen register device" because it intercepted alphanumeric characters that could constitute content. The court's concern was that such pagers could be used to capture sequences of numbers that went beyond the length of ordinary phone numbers and therefore were more likely to have a coded substantive meaning. *See, e.g.*, *id.* at 293 ("[T]he numbers capable of being so re-transmitted surely would have to be limited to raw telephone numbers to retain pen register status."). Here, however, [redacted] DIRNSA Decl. ¶ 18-19. [redacted] *Id.* at 19 n.10. [redacted]

The validation scheme also helps avoid concerns that have been raised about the use of a pen register to collect [redacted] which have been the subject of several district court opinions. [redacted]

[redacted] Nevertheless, [redacted] Moreover, the validation scheme is consistent with 18 U.S.C. § 3121(c), which mandates that the Government "use technology reasonably available to it" to prevent the capture of the contents of communications. ~~(TS//SI//NF)~~

Cases discussing the distinction between metadata and the content of communications are scarce.[26] Yet, the Court of Appeals' discussion of content in the Fourth Amendment context in *United States v. Forrester* is instructive on the issue of content for Internet communications. The Court of Appeals made an analogy between Internet communications and letters:

> [W]hen the government obtains the to/from addresses of a person's emails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the email to/from addresses and IP addresses-but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in [*Smith v. Maryland*] and [*Katz v. United States*] drew a clear line between unprotected addressing information and protected content information that the government did not cross here.

812 F.3d at 503, *citing* 495 F.3d 1041, 1049 (9th Cir. 2007). (U)

---

[26] In one case a magistrate held that information from the subject lines of e-mails, application commands, search queries, requested file names, and file paths were content. *In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxx@xxx.com]*, 396 F. Supp. 2d 45, 49 (D. Mass 2005). (U)

To extend this analogy to the physical world using the [redacted] types of data in Tab 2 of the DIRNSA Declaration, the metadata collected by the devices could be likened to information concerning a [redacted] It is information regarding [redacted]. While these pieces of information provide details about [redacted] they reveal nothing about *what* it actually says. ~~(TS//SI//NF)~~

The applicability of this reasoning to certain categories of metadata sought to be collected is uncontroversial. However, the [redacted] metadata discussed in detail above – [redacted] – also warrant in depth treatment here. ~~(TS//SI//NF)~~

[redacted] This metadata does not reveal the substance, meaning, or purport of the communication between user and provider. Rather, it consists of [redacted]

~~(TS//SI//NF)~~

Second, as previously discussed, [redacted] Accordingly, it also should not be considered content. ~~(TS//SI//NF)~~

Lastly, the "to," "from," "cc," and "bcc" information that would be collected is similarly not content of those communications. That information is indistinguishable from other addressing information used for purposes of identifying the parties to a communication; identifying information was removed from the definition of content by ECPA. S. Rep. No. 99-541 at 13. Moreover, as explained above, this information is obtained from [redacted] and should not be regarded as the "substance, purport, or meaning" of the communication [redacted] (TS//SI//NF)

Thus, considering the technical precautions that will be taken and the manner in which the definition of "contents" provided by Section 2510(8) as amended by ECPA has been interpreted, the metadata that would be collected would constitute non-content information permissibly obtained using a pen register device. ~~(TS//SI//NF)~~

5. Pen Registers May Collect Any Non-Content Data Associated With The Transmission of Electronic Communications, Regardless of Whether It Is Dialing, Routing, Addressing, and Signaling Information. (U)

Even if certain types of data that the Government proposes to collect under this Application are not dialing, routing, addressing, or signaling information, they still may lawfully

be collected by a pen register authorized under FISA because they are not "content." The text and legislative history of the pen register statute may be interpreted to permit a pen register to collect *any* non-content data, so long as the device or process used to collect it also records or decodes "dialing, routing, addressing, and signaling information and does not collect the content of any communications." In other words, to the extent that some communications data are neither dialing, routing, addressing, and signaling information nor "contents," a pen register can obtain them if it also records, decodes, or captures dialing, routing, addressing, and signaling information. ~~(TS//SI//NF)~~

The text of Sections 3127(3) and (4) do not limit pen register collection to dialing, routing, addressing, and signaling information.[27] Rather, Sections 3127(3) states that a pen register is 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 communications is transmitted, provided however, that such information shall not include the contents of any communication." The definition of a trap and trace device in Section 3127(4) is similar. While a pen register must perform those functions to qualify as a pen register, neither the definitions of a pen register or trap and trace device in 18 U.S.C. § 3127, nor Section 1842 of FISA, limits the information they may collect to dialing, routing, addressing, and signaling information. The only express limitation imposed on the type of information these devices may collect is the prohibition on the collection of the content of communications.[28] ~~(TS//SI//NF)~~

---

[27] This conclusion is not foreclosed by any other statute that might limit the Government's ability to collect information. Section 1842 of FISA provides that pen register may be obtained "[n]otwithstanding any other provision of law." Such language evidences Congress' intent to override any law that impeded that authority to obtain such a pen register. *See Liberty Maritime Corp. v. United States*, 928 F.2d 413, 416-17 and n.4 (D.C. Cir. 1991). (U)

[28] Section 3127(3) of Title 18 is also drafted to state that devices or processes used for billing or recording as an incident to billing are not "pen registers." [redacted] devices will not serve those purposes, so that provision is not germane to this analysis. ~~(TS)~~

The legislative history to the USA PATRIOT Act amendments to the pen register definition offers some support for this interpretation. As discussed above, in 2001, Congress amended the pen register statute to provide that a pen register is 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. *See* Pub. L. No. 107-56, § 216(c) (2001) (codified at 18 U.S.C. § 3127(3)). The definition of "pen register" previously had provided that a "pen register" is "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3) (2000).[29] One significant purpose of those amendments was to make the statute expressly applicable to computers and cell phone communications, as well as standard public switch telephone networks.[30] *Id.* at 47. In doing so, Congress broadened not only the nature of the device that may qualify as a pen register, but also the categories of information collected by a "pen register." (U)

The USA PATRIOT Act amendments used the term "dialing, routing, addressing, and signaling information" to cabin the information that a pen register must decode or record. While Congress used this term rather than "non-content," the legislative history suggests that Congress intended for "dialing, routing, addressing, and signaling information" to be synonymous with "non-content." The House Report states

---

[29] The USA PATRIOT Act similarly amended the definition of a trap and trace device to refer to "dialing, routing, addressing, and signaling information." Pub. L. No. 107-56, § 216(c). (U)

[30] The USA PATRIOT Act modified the definition of pen registers to explicitly apply to non-telephonic technology. Whereas the definition of a pen register device under Section 3127(3) previously only referred to "numbers dialed or otherwise transmitted through a telephone line," amended Section 3127(3) referred to "dialing, routing, addressing, and signaling information transmitted by an instrument or facility." Likewise, the definition of a trap and trace device was amended to refer to "dialing, routing, addressing, and signaling information." 18 U.S.C. § 3127(4). (U)

> [T]he section clarifies that orders for the installation of pen register and trap and trace devices may obtain *any non-content information* –"dialing, routing, addressing, and signaling information" – utilized in the processing or transmitting of wire and electronic communications. Just as today, such an order could not be used to intercept the contents of communications protected by the wiretap statute. The amendments reinforce the statutorily prescribed line between a communication's contents and non-content information, a line identical to the constitutional distinction drawn by the U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979). Thus, for example, an order under the statute could not authorize the collection of email subject lines, which are clearly content. Further, an order under the statute could not be used to collect information other than 'dialing, routing, addressing, and signaling' information, such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article. This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, applies across the board to all communications media.[31]

H.R. Rep. No. 107-236, at 53 (emphasis added). (U)

Here, regardless of whether the modified pen register provision was intended to permit the collection of all non-content – as the plain text of the statute appears to permit and the legislative history arguably supports – or only a subset of non-content that is dialing, routing, addressing, and signaling information, the Government submits that the non-content data identified in Tab 2 of the DIRNSA Declaration may be lawfully collected in either case under the authority of a pen register. All of the information to be collected is "dialing, routing, addressing, and signaling information" and, even if it is not, it may be collected because none of it is "content." ~~(TS//SI//NF)~~

[31] We acknowledge the existence of certain counter-arguments concerning the legislative history. The House Report quoted above, for instance, might arguably demonstrate that the reference in Sections 3127(3) and 3127(4) to "dialing, routing, addressing, or signaling information" was intended to specify the types of non-content information the collection of which had been approved in *Smith v. Maryland*. Similarly, the reference to particular types of content information – e-mail subject lines and URLs – might simply reflect Congress's attempt to underscore that pen registers may not collect content information. (U)

II. Operation of the Proposed Collection Devices Would Not Violate the Fourth Amendment. (U)

As argued above, all data that would be collected by the NSA's devices are non-content information constituting dialing, routing, addressing, and signaling information. It is well-established that information traditionally understood to be "dialing, routing, signaling, and addressing information" is not subject to the Fourth Amendment's protection. This was essentially the holding of *Smith v. Maryland* and the underpinning of the current pen register provisions, as modified by the USA PATRIOT Act: there is no legitimate expectation of privacy for such information. ~~(TS//SI//NF)~~

The information proposed to be collected under this Application falls within the phrase "dialing, routing, addressing, and signaling information," and in any event is non-content information voluntarily shared with a third party. Therefore, the information is not subject to a reasonable expectation of privacy. Moreover, even if certain categories of data are subject to a reasonable expectation of privacy, the collection program as a whole – particularly in light of the strict access and use limitations on the data once collected – would be reasonable under the Fourth Amendment in light of the "special needs" doctrine. ~~(TS//SI//NF)~~

A. The Proposed Collection Devices Would Be Consistent with *Smith v. Maryland*. (U)

Smith v. Maryland, the seminal case on the Fourth Amendment's application to use of pen registers for telephones, found that such devices could be operated without violating the Fourth Amendment to obtain non-content information that was given to a provider for purposes of completing a telephone call. In *Smith*, the Court rejected the argument that an individual can have a Fourth Amendment-protected "legitimate expectation of privacy regarding the numbers he dialed on his phone." 442 U.S. at 742 (internal quotation marks omitted). The Court

concluded that telephone subscribers know that they must convey the numbers they wish to call to the telephone company (because such conveyance is necessary for the company to complete their calls). Thus, the Court concluded, they cannot claim "any general expectation that the numbers they dial will remain secret." *Id.* at 743. Even if a subscriber could somehow claim a subjective intention to keep the numbers he dialed secret, the Court found that this was not an expectation that society would recognize as reasonable. To the contrary, the situation fell squarely into the line of cases in which the Court had ruled that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44. ~~(S)~~

The Supreme Court has not addressed the use of pen registers in the context of computer networks, but lower courts have reached the same conclusion about non-content information voluntarily provided for use in transmission of communications. *See, e.g.*, *Forrester*, 512 F.3d at 509. Indeed, this Court also arrived at that conclusion when it approved the Application for the previous bulk pen register collection in docket PR/TT [redacted]. This Court ruled, "[T]here is no reasonable expectation of privacy under the Fourth Amendment in the metadata to be collected ...." Opinion and Order, docket number PR/TT [redacted], at 59. ~~(TS//SI//NF)~~

The core of *Smith* and its progeny is the principle that non-content information that is voluntarily and knowingly provided to third parties is not protected by the Fourth Amendment. Users of communications systems understand that they are voluntarily exposing that information to third parties when they engage in communications requiring such disclosure. Therefore, that information is no longer subject to a legitimate expectation of privacy. *Smith* at 743-44, *citing* *United States v. Miller*, 425 U.S. 435, 442-44 (1976); *United States v. White*, 401 U.S. 745, 752 (1971). That is the case, moreover, regardless of whether the third party (*e.g.*, an ISP) records

the information. *See Smith*, 442 U.S. at 745 ("The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference"). (U)

As argued *supra*, 44-49, all of the data that would be collected by the proposed devices are not the content of communications. They are information about and related to the transmission of communications. Consistent with this fact, the data would be collected from the portions of communications in which non-content information is generally found. DIRNSA Decl. ¶¶ 17-19. The e-mail validation scheme that ensures that [redacted] also prevents the unintended collection of content as analogous to PCTDD information. Moreover, the [redacted] information [redacted] of e-mail [redacted] – essentially, all of the dialing, routing, addressing, and signaling information – are data that fall under *Smith* and are not protected by the Fourth Amendment. ~~(TS//SI//NF)~~

The users of Internet communications such as e-mail [redacted] should be cognizant of the fact that they are conveying their information to a third-party provider. Indeed, the convenience [redacted] (TS//SI//NF)

[redacted]

[redacted] *See* DIRNSA Decl. ¶ 14 n.9. Nevertheless, the Government submits that under the circumstances relevant to this collection, such information is not subject to a legitimate expectation of privacy. It is non-content information knowingly exposed to the provider and collected in a manner consistent with addressing information. ~~(TS//SI//NF)~~

Smith rests on the notion that a legitimate expectation of privacy is lost when one voluntarily exposes transmission (non-content) information to the third party communication provider; it should not be understood to be limited to information that is surrendered be used for purposes of actually transmitting the data. Instead, it merely requires that the information be surrendered knowing that the information is transmitted to the ISP. Furthermore, the non-content information that would be collected from [redacted]

Case law governing the use of mail covers is instructive on the issue of an expectation of privacy for such information. It is well established that the Fourth Amendment is not implicated by "mail covers," through which postal officials monitor and report for regular letter mail the same type of information contained in e-mail meta data – *i.e.*, information on the face of the envelope, including the name of the addressee, the postmark, the name and address of the sender (if it appears), and the class of mail. *See, e.g., United States v. Choate*, 576 F.2d 165, 174-77 (9th Cir. 1978); *cf. United States v. Charbonneau*, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) ("Email is almost equivalent to sending a letter via the mails."); *United States v. Maxwell*, 45

M.J. 406, 418 (C.A.A.F. 1996) ("In a sense, email is like a letter."). Courts have reasoned that "[s]enders knowingly expose[] the outsides of the mail to postal employees and others," *Choate*, 576 F.2d at 177, and therefore have "no reasonable expectation that such information will remain unobserved," id. at 175; *see also Vreeken v. Davis*, 718 F.2d 343, 347-48 (10th Cir. 1983) (concluding the "mail cover at issue in the instant case is indistinguishable in any important respect from the pen register at issue in *Smith*"); *United States v. DePoli*, 628 F.2d 779, 786 (2d Cir. 1980) ("[T]here is no reasonable expectation of privacy with regard to the outside of a letter . . . ."); *United States v. Huie*, 593 F.2d 14, 15 (5th Cir. 1979) (per curiam) ("There is no reasonable expectation of privacy in information placed on the exterior of mailed items . . . .").

~~(TS//SI//NF)~~

B. Use of the Proposed Collection for the Devices to Protect Against Terrorist and Foreign Intelligence Threats Would Not Violate the Fourth Amendment Because Their Use Is Reasonable Under the "Special Needs" Doctrine.[32] (U)

The overarching Government effort to collect non-content information, for which there is no reasonable expectation of privacy, in support of vital national security objectives, does not implicate the Fourth Amendment. Even assuming, however, that Fourth Amendment protections applied to some of the collected information [redacted] collection of that information is consistent with the Fourth Amendment. The Fourth Amendment requires no warrant here, only that the collection be reasonable. ~~(TS//SI//NF)~~

The collection of data arguably protected by the Fourth Amendment does not require a warrant because the collection program as a whole – in light of the strict restrictions on accessing

[32] The discussion of the Fourth Amendment assumes that the collection of metadata would occur lawfully under the pen register statute. We believe that even if that statute allows collection beyond what is described in *Smith*, such that the Fourth Amendment is implicated, it is still permissible under the Fourth Amendment's "special needs" doctrine, at least under the totality of circumstances surrounding the collection proposed in the Application. ~~(S)~~

and querying the database and disseminating collected information; the governmental interest; and the limited nature of the intrusion on privacy – is reasonable under the Fourth Amendment. The "nature and immediacy of the governments concerns," which are to identify and track foreign power operatives and thwart terrorist attacks, implicates governmental concerns that are at their most extreme. *Board of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie County v. Earls,* 536 U.S. 822, 833 (1976). The Supreme Court has recognized exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal citations omitted); *see also Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995). The Government's foreign intelligence collection through use of the devices is just such a special need, justifying an exception to the warrant requirement. *See In re Sealed Case*, 310 F.3d at 742 ("[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."). *See also In re Directives*, 551 F.3d at 1007 ("[W]e hold that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when the surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States."). ~~(TS//SI//NF)~~

Equally clearly, "the imposition of a warrant requirement [would] be a disproportionate and perhaps even disabling burden" on the Government's ability to obtain foreign intelligence information effectively. *Cf. United States v. Bin Laden*, 126 F. Supp. 2d 264, 273 (S.D.N.Y. 2000), *aff'd on other grounds*, 552 F.3d 157, 171 (2d Cir. 2008)(discussing activity abroad). The Government's foreign intelligence purposes for the overall effort to identify, track, and thwart

agents of Foreign Powers require that the devices collect metadata in bulk; such collection is necessary to make connections between terrorists and their associates. An individualized warrant requirement is a threshold, disabling requirement for such a collection. In terms of process alone, because the Government cannot identify the persons whose communications the devices will collect, it could not apply for a warrant. Furthermore, as the Fourth Circuit has explained, "attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy"; accordingly, "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations." *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) *quoted in In re Directives*, 551 F.3d at 1011-12. ~~(TS//SI//NF)~~

To the extent there is a reasonable expectation of privacy in some information, collection of such information complies with the Fourth Amendment's reasonableness requirement. In evaluating the constitutional reasonableness of a government search, a court must look to the totality of the circumstances, *United States v. Knights*, 534 U.S. 112, 118 (2001), "balancing [the individual's] Fourth Amendment interests against [the search's] promotion of legitimate governmental interests," *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 619 (1989) (citations and internal quotation marks omitted). (U)

The Government has a compelling interest in obtaining foreign intelligence information to protect national security. "[I]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981) (internal citations omitted). The overall collection effort aims to protect the nation from terrorist threats, which is a "governmental interest . . . of the highest order of magnitude." *In re*

Directives, 551 F.3d at 1012. *See also In re Sealed Case*, 310 F.3d at 746 (holding terrorist threats "may well involve the most serious threat our country faces."). ~~(TS//SI//NF)~~

The privacy interests at stake are limited. Most of the information collected by the devices is the type of information that clearly enjoys no Fourth Amendment protection under *Smith*. Insofar as certain categories of information might arguably be subject to a reasonable expectation of privacy, that expectation may well be diminished in light of the nature of e-mail communications and the need to share the information with the service provider for purposes of transmitting the communication. *Cf. United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002); Orin S. Kerr, *Internet Surveillance After the USA PATRIOT Act: The Big Brother that Isn't*, 97 NW. U.L.R. 607, 628-29 (2003) ("[B]ecause the contents of Internet communications are mixed together with envelope information and disclosed to the ISP, it is at least possible that courts will find that Internet users cannot have a reasonable expectation of privacy in Internet content information, much like postcards or cordless phone calls."). In addition, the Government's Application proposes numerous safeguards and procedures that reasonably protect the interests of United States persons. Access to the metadata requires a particularized showing that there is a reasonable, articulable suspicion that the seed identifier is associated with a Foreign Power. RAS determinations, moreover, are made by supervisors and are reviewed periodically by the Department of Justice's National Security Division and NSA's OGC. The supervisor and oversight reviews are a sufficient internal check against arbitrary action. ~~(TS//SI//NF)~~

The protections extend to the use and dissemination of the results of metadata queries. The Government's minimization procedures are incorporated from USSID 18 and FISA and require, among other things, that the identity of U.S. persons be redacted from intelligence reports prior to dissemination unless the information is in fact related to counterterrorism

information and is necessary to understand the counterterrorism information or assess its importance. This dissemination standard is virtually identical to that used by the Court in approving applications for electronic surveillance, and to the minimization procedures that were an important factor in the Court of Review's decision holding traditional FISA surveillance to be reasonable under the Fourth Amendment. *In re Sealed Case*, 310 F.3d at 740. ~~(TS//SI//NF)~~

C. The Proposed Collection Is Reasonable Because It is Appropriately Tailored to Balance the Overwhelming National Security Interest with the Minimal Intrusion to Privacy Interests. (U)

All of the metadata collected is properly collected under the Fourth Amendment because all of it is relevant to the FBI's investigations into these Foreign Powers, in the sense that full collection of all the metadata is vital for the use of the analytic tools the NSA will bring to bear to find the communications of these Foreign Powers. Neither the Fourth Amendment nor Title IV of FISA expressly imposes any requirement to tailor collection precisely to obtain solely communications that are strictly relevant to the investigation. While it is true that the overwhelming majority of communications from which metadata have been and will be collected will not be associated with these Foreign Powers, this does not present any infirmity under the Fourth Amendment or Section 1842. The collection program here is and has been appropriately tailored to balance the overwhelming national security interest at stake here and the minimal intrusion into privacy interests that will be implicated by collecting metadata, much of which will never be seen by a human being unless a connection to a terrorist-associated identifier is found. It is, therefore, reasonable under the Fourth Amendment. ~~(TS//SI//NF)~~

1. FISA Does Not Require Pen Registers or Trap and Trace Devices to Collect Only Narrowly Tailored Information and Any Application of Fourth Amendment Balancing Factors Demonstrates that the Collection is Reasonable. (U)

Title IV of FISA does not require that pen registers acquire only narrowly tailored information. The only statutory requirement is that "the information likely to be obtained" be "relevant to an investigation to protect against international terrorism." 50 U.S.C. § 1842(c). That standard does not require that all of the information likely to be obtained by a pen or trap be directly connected with the underlying investigation. The Government could never make such an absolute certification. Even in FISA pen register cases targeting individuals, many communication events are recorded that do not directly bear upon the investigation at issue.[33] ~~(S)~~

The Government cannot identify precisely which communications from the stream of billions are carrying the messages of these Foreign Powers, a challenge that may remain relatively constant given the worldwide nature of Internet communications. The Government therefore seeks to collect solely the e-mail metadata from these Internet communications – not their contents – so that it can use the metadata over an extended period of time to trace or determine connections between known terrorist identifiers and other identifiers (such as e-mails [redacted]). (TS//SI//NF)

---

[33] The same is true in cases where greater privacy interests are at stake and where the terms of the statute reflect a concern for tailoring the collection. For example, in cases where this Court authorizes electronic surveillance of Foreign Powers or agents of Foreign Powers pursuant to Title I of FISA, 50 U.S.C. §§ 1801-1812, [redacted] Instead, communications of that nature are minimized in accord with minimization procedures that the agencies conducting the electronic surveillance are ordered to follow by the Court. Here, although Title IV of FISA does not impose a requirement for minimization procedures, the Government has (as discussed in the Application and proposed orders) tailored this collection program and the Court has imposed processes and controls on it that the Government believes will limit the already minimal intrusion to privacy interests. ~~(TS//SI//NF)~~

Although the Government is not required by Title IV of FISA to tailor this collection to limit the intrusion to privacy interests, the Government's structuring of this collection program has and will limit any such intrusion. Thus, the collection clearly is appropriate and meets any examination that the Court would conduct by balancing Government's interests in conducting the collection against the potential intrusion into individual privacy interests. The collection therefore is consistent with one of the principal objectives of the entire statutory scheme under FISA – to achieve the appropriate balance between those interests. *See, e.g.*, H.R. Rep. No. 95-1283, pt. 1, at 47 (1978) ("The primary thrust of [FISA] is to protect Americans both from improper activities by our intelligence agencies as well as from hostile acts by Foreign Powers and their agents."); *id.* (discussing circumstances where "the countervailing privacy considerations militating against seeking [foreign intelligence] information through electronic surveillance are outweighed by the need for the information"); *id.* at 70 (discussing the "balance between security and civil liberties" to explain a particular provision in FISA). ~~(S)~~

The use of a balancing analysis, moreover, is supported by analogy to the method of analysis used to assess the reasonableness of a search under the Fourth Amendment – an approach that Judge Kollar-Kotelly explored and found persuasive in her Opinion and Order in docket number PR/TT [redacted] *See, e.g.*, Opinion and Order, docket number PR/TT [redacted], at 50-54. The reasons underlying Judge Kollar-Kotelly's discussion in her Opinion and Order have not changed in the past five years, for there is no Fourth Amendment-protected interest in the metadata at issue here. *See supra* at 53-57. As a result, the standards applied under Fourth Amendment balancing are far more rigorous than any that the Court should read into the statutory requirement that collection under Section 1842 be likely to obtain "relevant" information. Nevertheless, the balancing methodology applied under the Fourth Amendment –

balancing the Government's interest against the privacy interest at stake – demonstrates the reasonableness of the collection. ~~(TS//SI//NF)~~

It is well-established that determining the reasonableness of a search or seizure under the Fourth Amendment requires "balancing the nature of the intrusion on the individual's privacy against the promotion of legitimate governmental interests." *Board of Educ. v. Earls*, 536 U.S. at 829. Even where constitutionally protected interests are at stake (and they are not at stake here), the Fourth Amendment does not require the "least intrusive" or most "narrowly tailored" means for obtaining information. *See, e.g., id.* at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal citation and quotation marks omitted); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. at 663 ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."). Instead, the Supreme Court has indicated that any tailoring of the search should be considered as part of the reasonableness analysis in considering the "efficacy of [the] means for addressing the problem." *Id.* (U)

Even under the more exacting standards imposed by the Fourth Amendment, if the Government's interest is great and the intrusion into privacy is relatively minimal, the measure of efficacy required to make a search "reasonable" is not a numerically demanding success rate for the search. For example, in considering the use of warrantless and suspicionless roadblocks to temporarily seize automobiles and screen for drunken drivers, the Supreme Court found that an arrest rate of only 1.6 percent of drivers passing through drunk driving roadblocks established sufficient "efficacy" to sustain the constitutionality of the practice. *See Michigan Dep't of State*

Police v. Sitz, 496 U.S. 444, 454-55 (1990). Similarly, the Court has approved the use of suspicionless roadblocks near the border to find illegal aliens even when the roadblocks successfully detected illegal immigrants in only 0.12 percent of the vehicles passing through the checkpoint. *See United States v. Martinez-Fuerte*, 428 U.S. 543, 554 (1976). In sum, "[t]he effectiveness of the [state's] plan, in terms of percentage, need not be high where the objective is significant and the privacy intrusion limited." *Jones v. Murray*, 962 F.2d 302, 308 (4th Cir. 1992). (U)

Here, the Government's interest is at its zenith. As the Supreme Court has recognized, "[i]t is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." *Haig*, 453 U.S. at 307 (citations and internal quotation marks omitted). Tracking down agents of these Foreign Powers remains essential to safeguarding the Nation from the grave threat of further terrorist attacks that these Foreign Powers continue to plan and make efforts to carry out. Acquiring bulk metadata is an important step among several in the process of locating terrorists. Archiving the metadata has and will continue to enable historical chaining [redacted] of Internet communications. Those methods of analysis (among others) are invaluable tools in efforts to identify the broad scope of the terrorist activities of these Foreign Powers and their agents. The Government cannot rely solely on targeted metadata collection because it cannot know [redacted] exactly which communications will show the connections among terrorists. *Cf. Martinez-Fuerte*, 428 U.S. at 557 (upholding suspicionless roadblocks to search for illegal aliens in part because a "requirement that stops on major routes inland always be based on reasonable suspicion would be impractical because the flow of traffic tends to be too heavy to allow the particularized study

of a given car that would enable it to be identified as a possible carrier of illegal aliens"). ~~(TS//SI//NF)~~

Balanced against this extraordinarily strong governmental interest is the minor intrusion into the privacy interests of innocent Internet users in the metadata associated with their electronic communications. There is, of course, no constitutionally protected privacy interest in such metadata. Rather, it is analogous to the dialed-number information for telephone calls considered by the Supreme Court in *Smith v. Maryland*, 442 U.S. 735 (1979) (discussed above). In *Smith*, the Court squarely rejected the view that an individual can have a Fourth Amendment protected "legitimate expectation of privacy regarding the numbers he dialed on his phone." *Smith*, 442 U.S. at 742 (internal quotation marks omitted). Just as telephone users who "voluntarily convey[]" information to the phone company "in the ordinary course" of making a call "assum[e] the risk" that this information will be passed on to the government or others, *Smith*, 442 U.S. at 744 (internal quotation marks omitted), so too do e-mail [redacted] users assume the risk that the addressing information on their communications may be shared. ~~(S)~~

2. The Application of the RAS Standard Has and Will Function to Significantly Limit the Actual Amount of Metadata that is Viewed by the NSA. ~~(TS//SI//NF)~~

In weighing the intrusion into privacy that the proposed collection would involve, it is also significant that, while the Government will collect a large volume of metadata, only a tiny fraction of that information has been and will ever be seen by any human being, and then only on the basis of a targeted inquiry. As described herein, the Government will search the metadata only in prescribed ways designed to uncover communications identifiers associated with these Foreign Powers. Metadata concerning an individual's communications that is collected will be [redacted] but the information pertaining to that individual's

communications will never be presented to a human being unless the computer program identifies a terrorist connection in the form of contact with a terrorist-associated identifier that has been determined to satisfy the RAS standard. The fact that no person will ever view the overwhelming majority of the information collected here reduces even further the weight to be accorded any intrusion into privacy. ~~(TS//SI//NF)~~

Here, as in the predecessor collections to the attached Application that this Court has granted, the actual amount of raw metadata that will ever be seen by an NSA analyst is substantially less than the total amount of metadata collected. That is because any search or analysis of the collected data will occur only after the Government has identified a particular Internet communications identifier (*e.g.*, an address that is associated with these Foreign Powers or their or affiliated terrorist organizations). In identifying such identifiers, the Government will consider an identifier to be terrorist-associated only when "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion" that the identifier is associated with agents of [redacted] DIRNSA Decl. ¶¶ 24, 31. For example, [redacted] This is, in effect, the standard applied in the criminal law context for a "Terry" stop. *See Terry v. Ohio*, 392 U.S. 1, 21, 30 (1968); *see also Illinois v. Wardlow*, 528 U.S. 119, 123 (2000) (police officer may conduct a brief, investigatory Terry stop "when the officer has a reasonable, articulable suspicion that criminal activity is afoot"). The determination that an identifier satisfies that standard must be approved by one of the following people: the Chief or Deputy Chief, Homeland Security

Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. DIRNSA Decl. ¶ 31. In sum, the application of this standard further reinforces the reasonableness of the collection as it, in effect, significantly reduces the total amount of metadata that will ever be analyzed by NSA. ~~(TS//SI//NF)~~

When the Government's need for the metadata collection at issue is balanced against the minimal intrusion on the privacy interests of those innocent users of the Internet whose metadata would be collected, the balance tips overwhelmingly in favor of the Government. If, as the Supreme Court concluded in *Martinez-Fuerte*, the Government's interest in stemming the flow of illegal immigration is sufficient to sustain suspicionless seizures of motorists as constitutionally reasonable even when the seizures yield a success rate of only 0.12 percent in finding illegal aliens, then the Government's interest in finding a terrorist plotting the deaths of thousands should easily sustain a collection program that implicates no constitutionally protected interests even if its success rate in identifying terrorists is substantially lower than that. The statutory standard of relevance certainly cannot be construed to impose a more demanding tailoring requirement than the Fourth Amendment.[34] ~~(S)~~

[redacted]

The exploitation of the metadata information described in the attached Application is appropriate under these circumstances. It involves solely information in which there is no constitutionally protected privacy interest (as opposed to the contents of communications), and application of the reasonably articulable suspicion standard will substantially limit the amount of metadata that actually is seen by one of only a limited number of NSA analysts. There is no attempt to censor the communications from which metadata will be acquired.[35] Thus, the collection the Government proposes here –collection that will take place under the FISA statute and with judicial oversight – does not strike any more aggressive balance between the Government's interest in intelligence and individual privacy than the overall balance that Congress itself struck in the statute with respect to non-content metadata that is appropriately collected through a pen register. ~~(TS//SI//NF)~~

3. The Government's Use of the Collected Metadata Will Be Strictly Circumscribed, and the Government Will Apply Procedures To Protect U.S. Person Information. ~~(S)~~

The Government represents to this Court that, although the data collected under the attached Application will necessarily be broad in order to achieve the critical intelligence

---

[35] The First Amendment similarly presents no concerns regarding the proposed collection, as this Court previously has found. *See* Opinion and Order, docket number PR/TT [redacted] at 66-69. As Judge Kollar-Kotelly acknowledged in her Opinion and Order, "[t]he weight of authority supports the conclusion that Government information-gathering that does not constitute a Fourth Amendment search or seizure will also comply with the First Amendment when conducted as a part of a good-faith criminal investigation." *Id.* at 66. Here, the proposed collection will not be for ordinary law enforcement purposes, but rather for the extraordinarily compelling purposes of protecting against the terrorist activities of the Foreign Powers. This interest clearly satisfies any "good faith" standard that would be applicable. *See United States v. Aguilar*, 883 F.2d 662, 705 (9th Cir. 1989); *Reporters Comm. For Freedom of the Press v. AT&T*, 593 F.2d 1030, 1051 (D.C. Cir. 1978); *see also* Opinion and Order, docket number PR/TT [redacted] at 66-67. Further, the Government has certified that the investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution, and the proposed Primary Order further directs, as to any seed identifiers reasonably believed to be used by or associated with a United States person, *that NSA's Office of General Counsel (OGC) shall first determine that any identifier so believed is not regarded as associated with a Foreign Power solely on the basis of activities that are protected by the First Amendment to the Constitution*. As such, the proposed collection poses no First Amendment concern here. ~~(TS//SI//NF)~~

objectives of metadata analysis, the use of that information for analysis will be strictly tailored to identifying terrorist communications and will occur solely according to stringent procedures, including minimization procedures designed to protect U.S. person information. ~~(TS//SI//NF)~~

When such a communication is identified, as outlined above, the NSA may perform several types of analysis with the metadata it has collected. For example, it may perform contact-chaining – that is, it may search the metadata to determine what other identifiers the target identifier has been in contact with. In addition, the results of such a query may be subjected to other forms of SIGINT analysis. DIRNSA Decl. ¶ 25. It bears emphasis that, given the types of analysis the NSA will perform, no information about an identifier will ever be accessed by or presented in an intelligible form to any person unless that identifier has been in direct contact (within two hops) of an identifier for which NSA has satisfied the RAS standard. ~~(TS//SI//NF)~~

Second, the Government will follow strict procedures ensuring the limited use of the metadata and protecting U.S. person information. These procedures will include ensuring adherence to the requirements that access to the data generate auditable records; analytic queries of the data are limited to RAS-approved seed identifiers; and that the underlying metadata is destroyed within five years of collection. DIRNSA Decl. ¶¶ 31, 33. In particular, NSA will apply the minimization and dissemination requirements and procedures of Section 7 of USSID 18 to any results from queries of the metadata disseminated outside of NSA in any form. *Id.* ¶ 32. In addition, 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 SID, the Deputy Director of the SID, the Chief of the 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.* In this regard, the procedures the Government proposes to use are more exacting than is required by statute. In contrast to other provisions in FISA, Title IV does not require any minimization procedures to be followed when the Government obtains approval for pen registers or trap and trace devices, and indeed applications under Title IV of FISA do not normally stipulate that minimization procedures will be followed. *Cf.* 50 U.S.C. § 1805(c)(2) (FISA order approving electronic surveillance must direct that minimization procedures be followed). ~~(TS//SI//NF)~~

Finally, to ensure that the Court can understand the way the above-described standards and procedures are applied, and the way the Government is accessing the information collected under the attached Application, when and if the Government seeks a reauthorization of the pen registers and trap and trace devices in the Application, it will provide the Court with a report about the searches that have been conducted of the acquired bulk metadata. DIRNSA Decl. ¶ 35. ~~(S)~~

III. The Government Requests Authorization under 50 U.S.C. § 1842 to Access, Process, and Use Metadata Previously Obtained [redacted] (S)

As discussed above, the attached Application seeks authorization from the Court to install and use pen registers on a prospective basis. In addition, and in accord with that request, the Court also should grant commensurate and continuing authority to query metadata previously collected. That is the case even though, as discussed in the Compliance Report, the prior pen register collection in certain ways exceeded the scope of the Court's orders. For the reasons set forth above, however, such collection did not exceed *the scope of the pen register statute, the*

Constitution, or the current proposed order. As detailed in the DIRNSA Declaration, without access to the previously collected information, the value of the pen register will be reduced. *See* DIRNSA Decl. 13 n.6. ~~(TS//SI//NF)~~

Beginning in its first order in July 2004, the Court has recognized the unique nature of bulk pen register and has regulated it at two critical stages: a collection stage, in which metadata is extracted from the Internet and stored in NSA databases; and at the querying stage, in which the metadata is extracted from the databases if responsive to a identifier as to which there is reasonable articulable suspicion that it is used by one of the Foreign Powers specified in the Court's orders. This regulatory framework differentiates the bulk pen register orders from traditional FISA pen register orders in two important ways. ~~(TS//SI//NF)~~

First, the bulk orders have regulated both collection and use, where a traditional pen register order regulates collection only. *Cf.* 50 U.S.C. § 1845(a)(2) (requiring that pen register information be used lawfully). Second, each bulk pen register order has regulated not only querying of the information acquired during the 90 days following entry of the order, but also the information acquired pursuant to all of its predecessor orders.[36] In that sense, the Court has asserted a continuing jurisdiction over the bulk pen register program that is both prospective and retroactive. The Government supported that assertion of jurisdiction in 2004, and continues to do so today in light of the unique nature of the bulk pen register program. ~~(TS//SI//NF)~~

[36] In a way, this difference in the bulk pen register orders is similar to the Government's obligations pursuant to minimization procedures that the Government is ordered to follow where this Court authorizes electronic surveillance of Foreign Powers or their agents pursuant to 50 U.S.C. §§ 1801-1812. *See also* note 34, *supra* (discussing how tailoring of this collection through the regulation of queries minimizes the already minimal potential intrusion to privacy interests). In those cases, the Government affirmatively pleads and is ordered to follow those minimization procedures "as to all information acquired through the authorities" requested in those Applications – a limitation on how the Government deals with that information even well after the effective period of surveillance ends. Here, even though the pen register statute does not require minimization procedures for pen registers, in this Application and in the prior Applications and orders in the bulk pen register collection, similar controls on the Government's querying of the information are imposed. ~~(TS//SI//NF)~~

The Court's continuing jurisdiction under Section 1842 justifies an order granting access to the stored metadata, even though some of that metadata exceeded the scope of the Court's prior orders. In effect, the Court has treated the "installation and use" of the bulk pen register as embracing not only current collection but also querying and related actions, whether the data being queried are newly collected or old. *See generally In the Matter of Application of the United States*, 416 F. Supp. 2d 13, 16 & n.5 (D.D.C. 2006). As such, it is within the Court's Section 1842 authority to permit querying of all accumulated metadata, as long as that metadata is within the scope of the statute and the Constitution, as it is for reasons discussed above. And as noted above, the value of the bulk pen register would be dramatically reduced without access to the years of accumulated data that resides in the NSA's databases pursuant to the prior orders. ~~(TS//SI//NF)~~

There is no independent limitation that would prohibit the Court's authorization of access to the stored metadata under Section 1842. The Court's rules give it discretion to enter this requested order lifting the current embargo on the NSA's ability to query this data, *see* FISC R. 10(c)(iv), and there is precedent for similar actions, although in light of the unique nature of the bulk pen register it should not be surprising that there are no cases directly on point. *See, e.g.*, *In re* [redacted] docket numbers [redacted] (seeking authority to index and log a communication that was previously indexed and logged in violation of the known or extended absence provision of the FBI's Standard Electronic Surveillance Minimization Procedures); *In re* [redacted] docket number [redacted] (authorizing retention of information previously obtained from pen register surveillance of a location not specified in the Court's authorization order because of the government's "good-faith implementation" of the pen

register order concerning the correct telephone numbers used by the correct target).[37] For these reasons, we believe the Court may affirmatively authorize access to and use of the stored metadata under Section 1842. ~~(TS//SI//NF)~~

--- Remainder of page intentionally left blank ---

[37] Section 1809 of Title 50, the criminal provision of FISA, is not to the contrary. Section 1809 is a provision that penalizes certain intentional violations of the Court's orders. That is consistent with Section 1809's requirement of an intentional violation of a known legal duty and its inclusion of an affirmative defense for officers who act in any manner authorized by court order. Here, of course, we are seeking an order expressly authorizing access to the previously collected data. If indeed the Court enjoys authority to issue such an order, as we argue it does, then Section 1809 should not be read to restrict that authority, given that FISA's pen register provisions apply "[n]otwithstanding any other provision of law," including Section 1809. 50 U.S.C. § 1842(a)(1). In light of that proviso and the requirement that the conduct be willful, the existence of the order would of course preclude any criminal penalty for conduct in conformity with it. ~~(TS//SI//NF)~~

IV. Conclusion (U)

For the foregoing reasons, the Government submits that this Court should authorize the Government to use and install pen registers and trap and trace devices as proposed in the Application and be permitted to access and prospectively use the data that is the subject to Supplemental Order and Opinion in PRTT [redacted] (TS//SI//NF)

Respectfully submitted,

Eric H. Holder, Jr.
Attorney General of the United States

David S. Kris
Assistant Attorney General
for National Security
U.S. Department of Justice