

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](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//NOFORN~~

FILED
KAREN E. SUTTON, CLERK

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

U.S. Foreign Intelligence
Surveillance Court

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//NOFORN~~

Derived from Application of the United States to the Foreign
Intelligence Surveillance Court in the above-captioned
matter filed _____

~~Declassify only upon the determination of the President.~~

~~TOP SECRET//ICS//COMINT//NOFORN~~

INTRODUCTION (U)

One of the greatest challenges the United States faces in the ongoing conflict with [REDACTED]

[REDACTED] is finding operatives of the enemy. As the Court is aware, that task is complicated by terrorists' exploitation of Internet e-mail as a favored means of communication. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] See Declaration of

~~TOP SECRET//ICS//COMINT//NOFORN~~

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

Lt. Gen. Michael V. Hayden, USAF, Director, NSA ¶ 6 [REDACTED] (Attachment A to the Application) (hereinafter "DIRNSA Decl."). Unless the United States finds a way to sort through that data to identify terrorists' communications, [REDACTED] [REDACTED] will be losing vital intelligence that could prevent another deadly terrorist attack. ~~(TS//SI//NF)~~

The attached Application for pen registers and trap and trace devices works within the traditional authorities provided by the Foreign Intelligence Surveillance Act to capitalize upon the unique opportunities the United States has for identifying communications of [REDACTED] [REDACTED] The collection sought here will make possible one of the most powerful tools that the Government can bring to bear to discover enemy communications: meta data analysis. Meta data essentially consists of the header/router/addressing information on an electronic communication that identifies the addresses of the communicants. It does not include the substance of the communication. Relying solely on such meta data, the Government can analyze the contacts made by an e-mail account believed to be associated with a terrorist, and thereby identify other, previously unknown, terrorists. A form of such "contact analysis" is regularly used in both criminal and intelligence cases when a pen register is placed, for example, on a single e-mail account. Such individually targeted collection of meta data, however, is inadequate for tracking the communications of terrorists [REDACTED]

[REDACTED] [REDACTED] Given that challenge, meta data analysis offers its fullest advantage as an intelligence tool only if the Government can analyze *past* connections [REDACTED] That analysis is possible, however, only if the Government has collected and archived a broad set of meta data that contains within it

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

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

the subset of communications that can later be identified as terrorist-related. If that broad data set is not collected and archived by the Government on an ongoing basis at the time e-mails are sent, it disappears and is lost forever, and the data can never be analyzed to find the terrorist connections hidden within it. ~~(TS//SI//NF)~~

In the attached Application, therefore, the Government seeks the Court's approval to use pen registers and trap and trace devices to collect, in bulk, the meta data associated with large volumes of electronic communications transiting [REDACTED] on the Internet. The Application fully satisfies all requirements of Title IV of FISA, 50 U.S.C. §§ 1841-1846, as amended. Most importantly, the Application certifies that the "information likely to be obtained" by bulk collection of e-mail meta data at these [REDACTED] is "relevant to an ongoing investigation to protect against international terrorism." As described in more detail below, the

[REDACTED]

[REDACTED]

[REDACTED]

Nevertheless, because [REDACTED] carry large volumes of traffic, the vast majority of communications transiting [REDACTED] (and hence the vast majority of meta data collected) will not be terrorist-related. That, however, presents no infirmity under the statute for several reasons. First, once the Government certifies, as it has here, that the "information likely to be obtained" is relevant to the investigation, the Court's inquiry is properly at an end and the Application should be approved. Congress made the Government's certification on this point dispositive. Second, in any event, all of the meta data to be collected here is relevant to FBI

[REDACTED] DIRNSA Decl. ¶ 7 & n.6. ~~(TS//SI//NF)~~

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

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

investigations into [REDACTED] because it is necessary to have the data in bulk for the NSA to be able to bring to bear its intelligence tools for analyzing the data.

Third, even if non-terrorist communications were not deemed relevant, nothing in Title IV of FISA demands that a pen register or trap and trace device collect *only* information that is strictly relevant to the international terrorism investigation at hand. Even if the Court were to look behind the Government's certification, therefore, and were to require some tailoring of the breadth of the proposed collection to fit the information that will actually be terrorist-related, the collection proposed in the Application would meet any proper test for reasonable tailoring. Any tailoring standard must be informed by a balancing of the government interest at stake against the degree of intrusion into any protected privacy interests. Here, the Government's interest is the most compelling imaginable: the defense of the Nation in wartime from attacks that may take thousands of lives. On the other side of the balance, the intrusion is minimal. There is certainly no constitutionally protected interest in the meta data from e-mails, just as there is no such interest in the numbers dialed on a telephone. Any intrusion is even further reduced, moreover, because any data that is ultimately unrelated to terrorists will never even be viewed by any human being. Under the procedures the Government will apply, meta data reflecting the activity of a particular e-mail contact will never even be presented to a human analyst until a computer search has established a connection to a known, terrorist-associated e-mail address. ~~(TS//SI//NF)~~

It is true that the Application presents a somewhat novel approach to pen registers and trap and trace devices. Nevertheless, it involves nothing more than adapting the traditional tools of FISA to meet an unprecedented challenge and does so in a way that promotes both of the twin goals of FISA: facilitating the foreign-intelligence collection needed to protect American lives while at the same time providing judicial oversight to safeguard American freedoms. ~~(S)~~

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

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

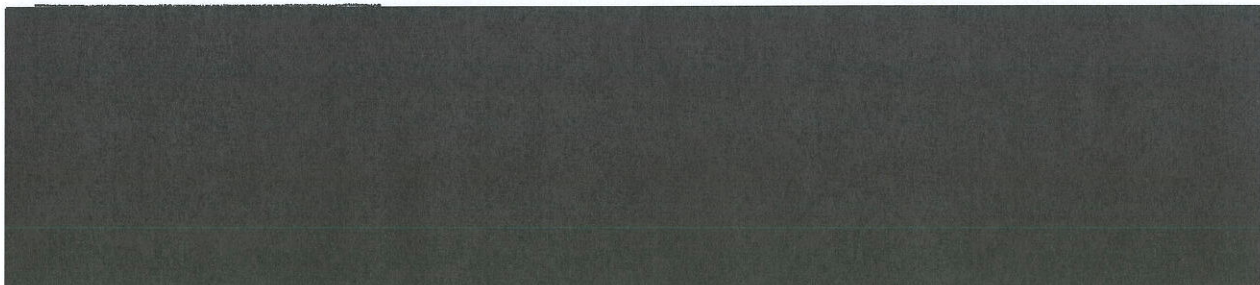
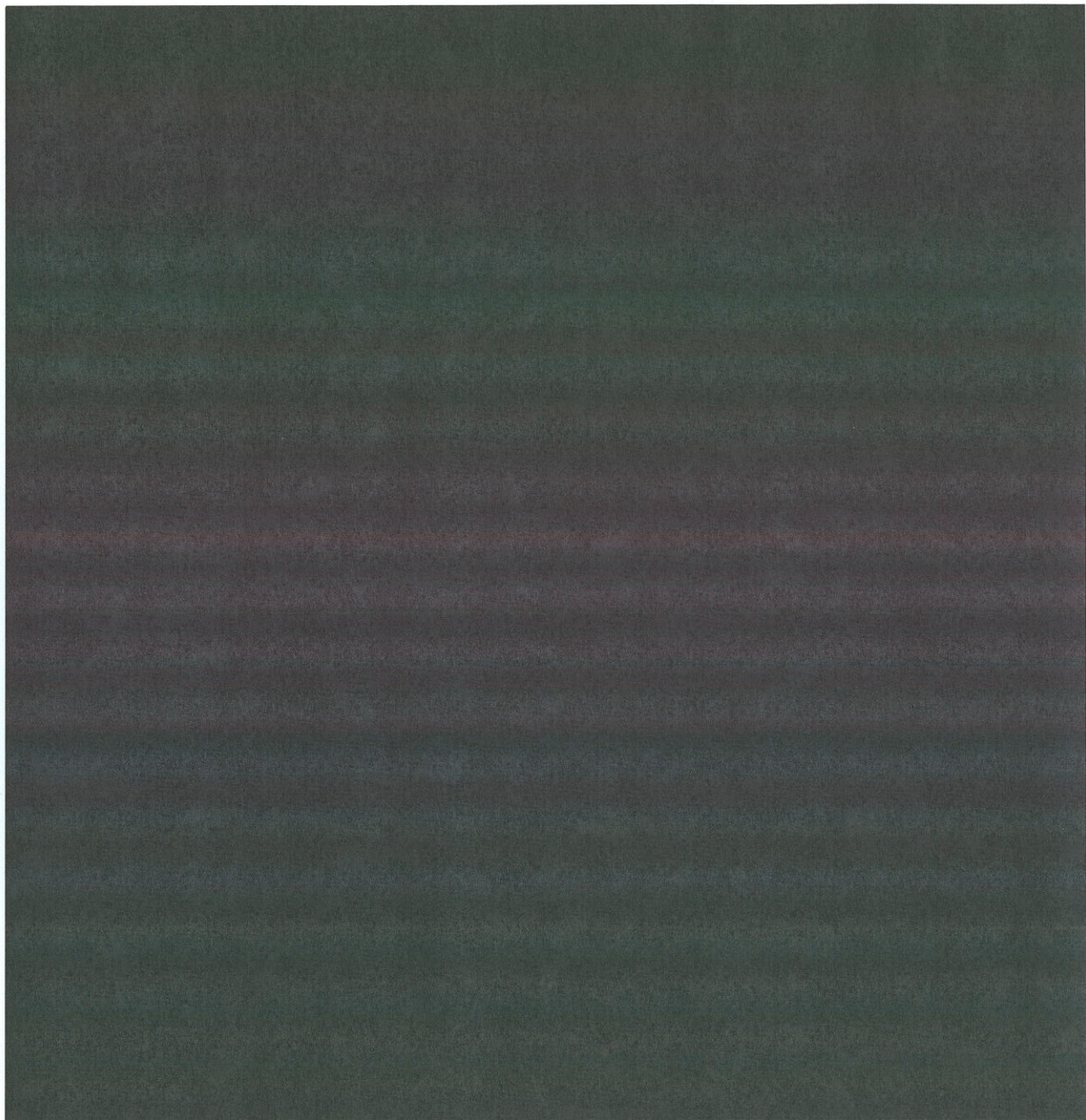
BACKGROUND (U)

A. 



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

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



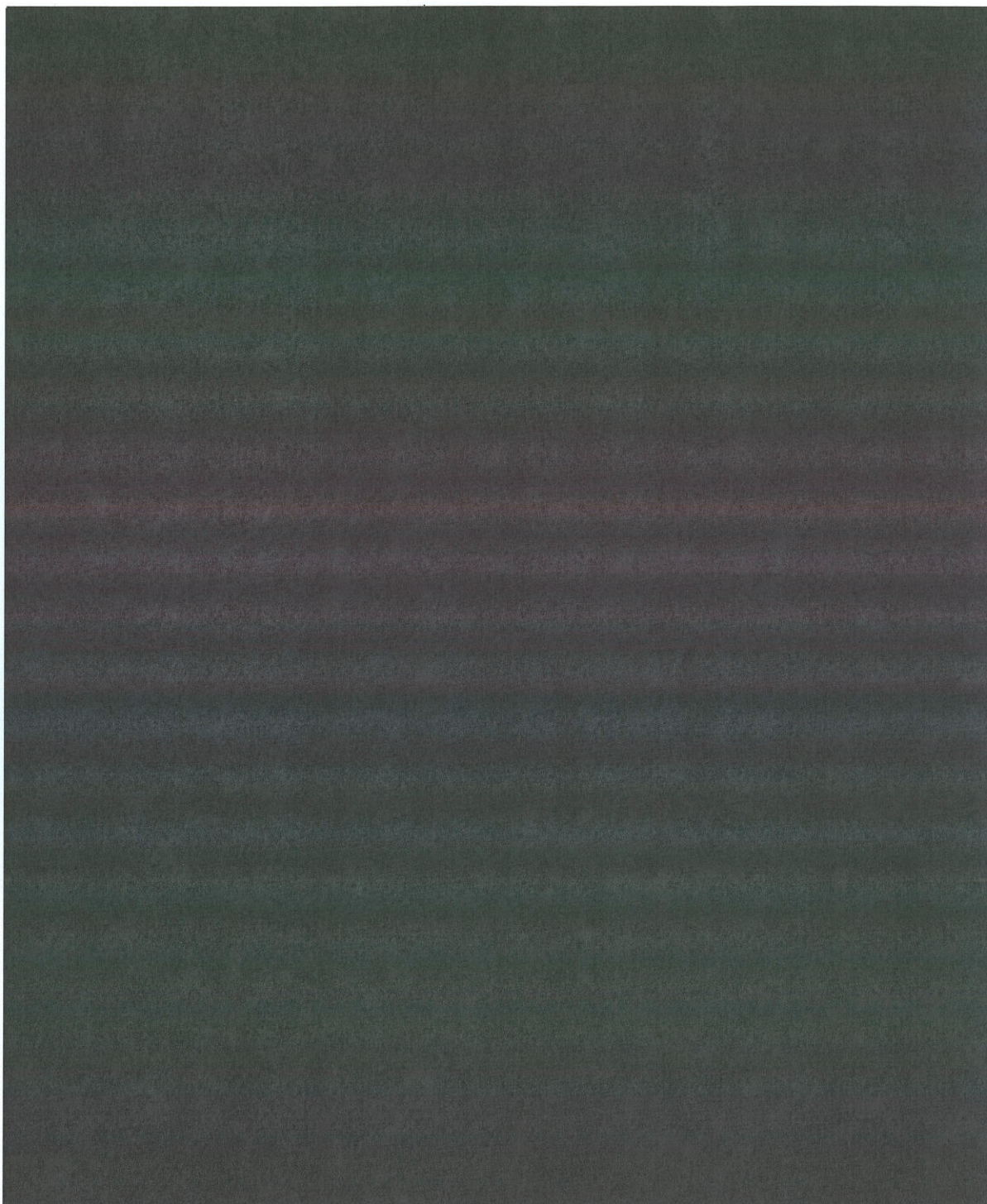
~~TOP SECRET//HCS//COMINT//NOFORN~~

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



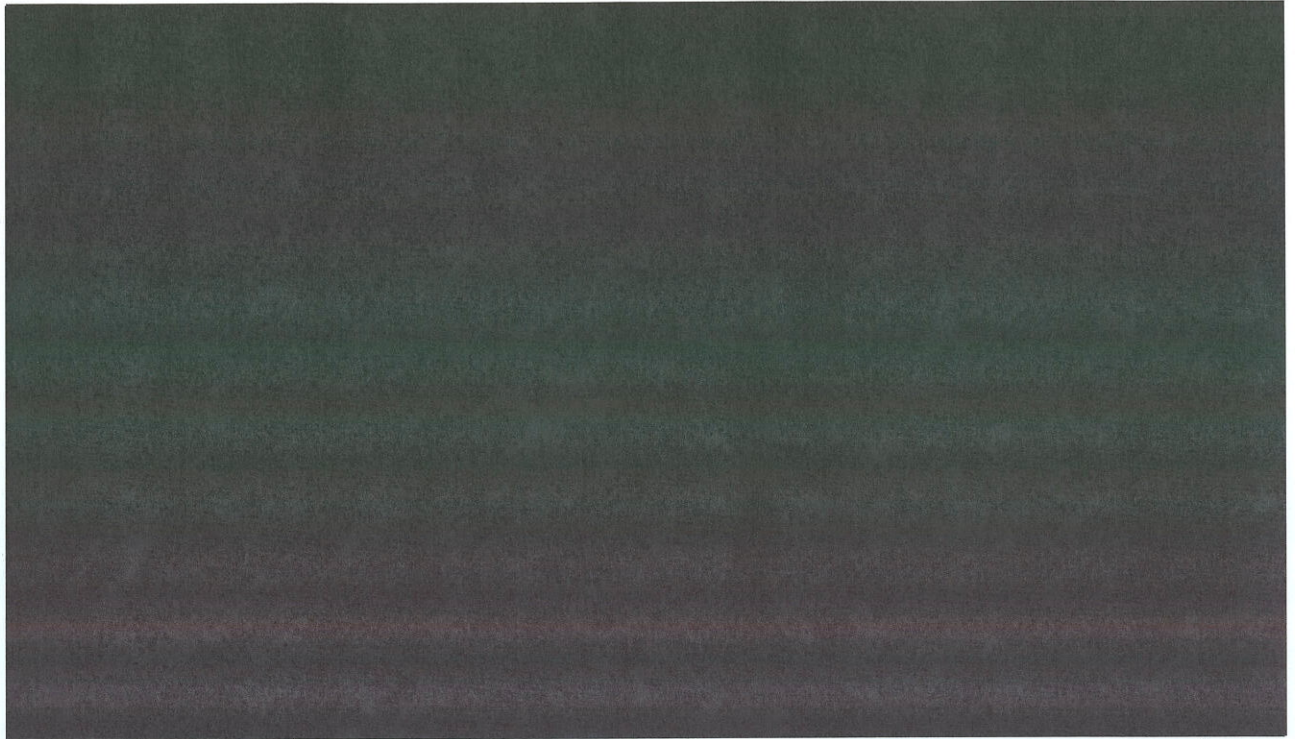
~~TOP SECRET//HCS//COMINT//NOFORN~~

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






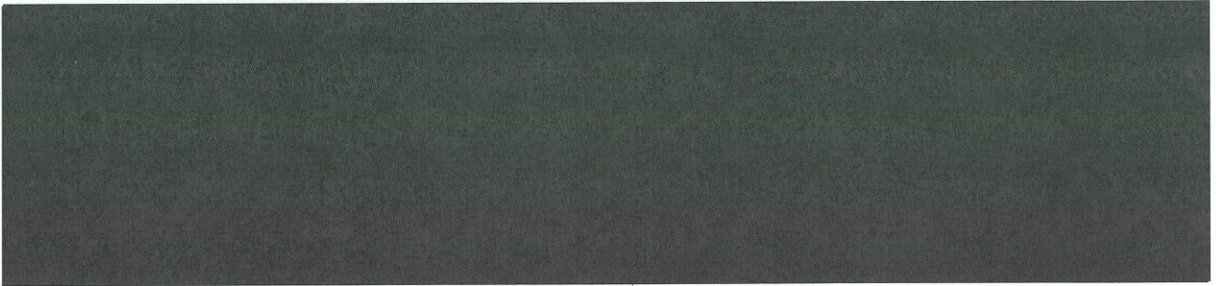
~~TOP SECRET//HCS//COMINT//NOFORN~~

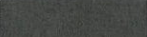
~~TOP SECRET//HCS//COMINT//NOFORN~~



B.  Exploitation of the Internet ~~(S)~~

To coordinate their plots, agents of  must have a secure means to communicate. One of the primary methods they have chosen is e-mail.⁵ As the Court is aware from many applications for electronic surveillance, FBI analysis has shown that  operatives have come to rely heavily on e-mail communications as a way to convey closely held operational plans. 

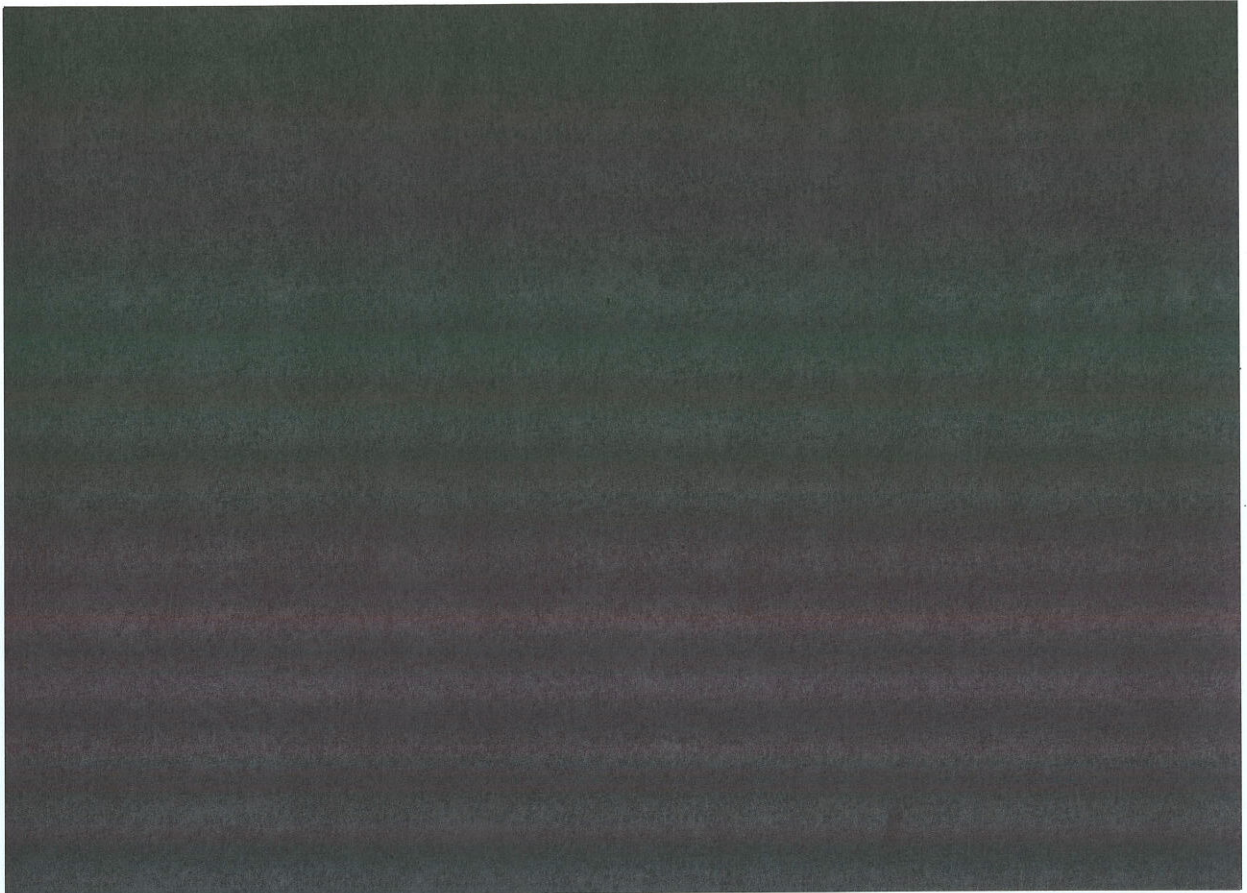


⁵ Throughout this memorandum we use the term "e-mail" to apply to web-based e-mail 



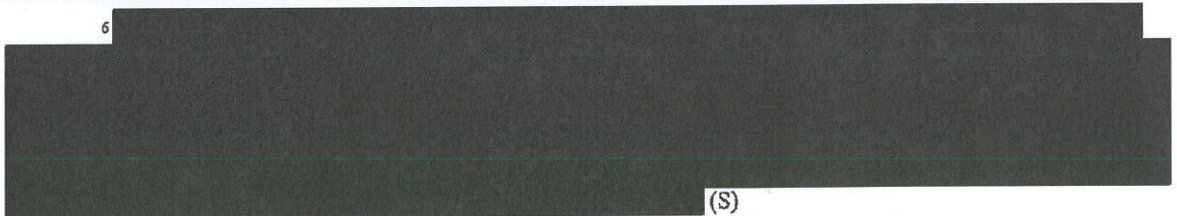
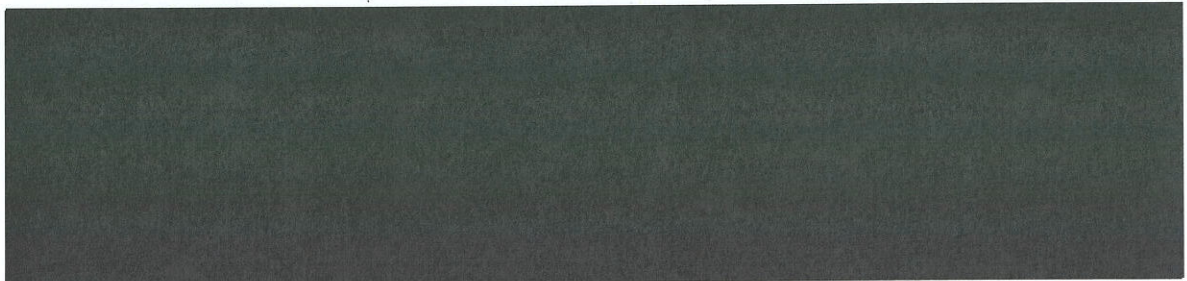
~~TOP SECRET//HCS//COMINT//NOFORN~~

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



C. Discovering the Enemy: Meta Data Analysis ~~(TS//SI//NF)~~

While [REDACTED] exploitation of the Internet poses a daunting challenge to the intelligence community, it also presents a great opportunity. The opportunity arises because [REDACTED]



(S)

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

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] DIRNSA Decl.

¶ 8(c).

DIRNSA Decl. ¶ 5. ~~(TS//SI//NF)~~

Analyzing meta data from this e-mail traffic—that is, the addressing information showing which e-mail addresses are in contact with other addresses⁷—can be a powerful tool for

⁷ “Meta data” is the information appearing on the “to,” “from,” “cc,” and “bcc” lines of a standard e-mail.

[REDACTED]

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

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

discovering enemy communications. Identifying enemy communications in the billions of bits of Internet traffic, however, is like finding a needle in a haystack. Worse, it is like trying to find a needle in a stream of billions of stalks of hay per second flowing by on a conveyor belt at the speed of light. Loosely speaking, for analysts to have a chance at finding the terrorists, they need a mechanism to convert that stream into a stationary haystack that can be searched in a targeted way. The mechanism for accomplishing that is to strip out from the stream of e-mail traffic solely the meta data—not the content of messages—so that it can be available for later analysis. Collecting and archiving meta data is thus 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 archive the data now, we will be able to use it in a targeted way to find the terrorists tomorrow. DIRNSA Decl. ¶¶ 12-13. ~~(TS//SI//NF)~~

Collecting meta data [REDACTED]

[REDACTED] offers at least two invaluable capabilities to analysts that are unavailable from any other approach. First, it allows for retrospective "contact chaining." For example, [REDACTED]

[REDACTED] By examining meta data that has been archived over a period of time, analysts can search to find the contacts that have been made by that "seed" e-mail address.⁸ The

[REDACTED]

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

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

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 who were previously thought to be unconnected. Indeed, computer algorithms would automatically identify not only the first tier of contacts made by the seed e-mail address, but also the further contacts made by the first tier e-mail addresses. DIRNSA Decl. ¶ 15. Going out to the "second hop" enhances the ability of analysts to find terrorist connections by greatly increasing the chances that they will find previously unknown terrorists. A seed e-mail, 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. ~~(TS//SI//NF)~~

The capabilities offered by such searching of a collected archive of meta data are vastly more powerful than chaining that might be performed through prospective pen registers targeted at individual e-mail accounts. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

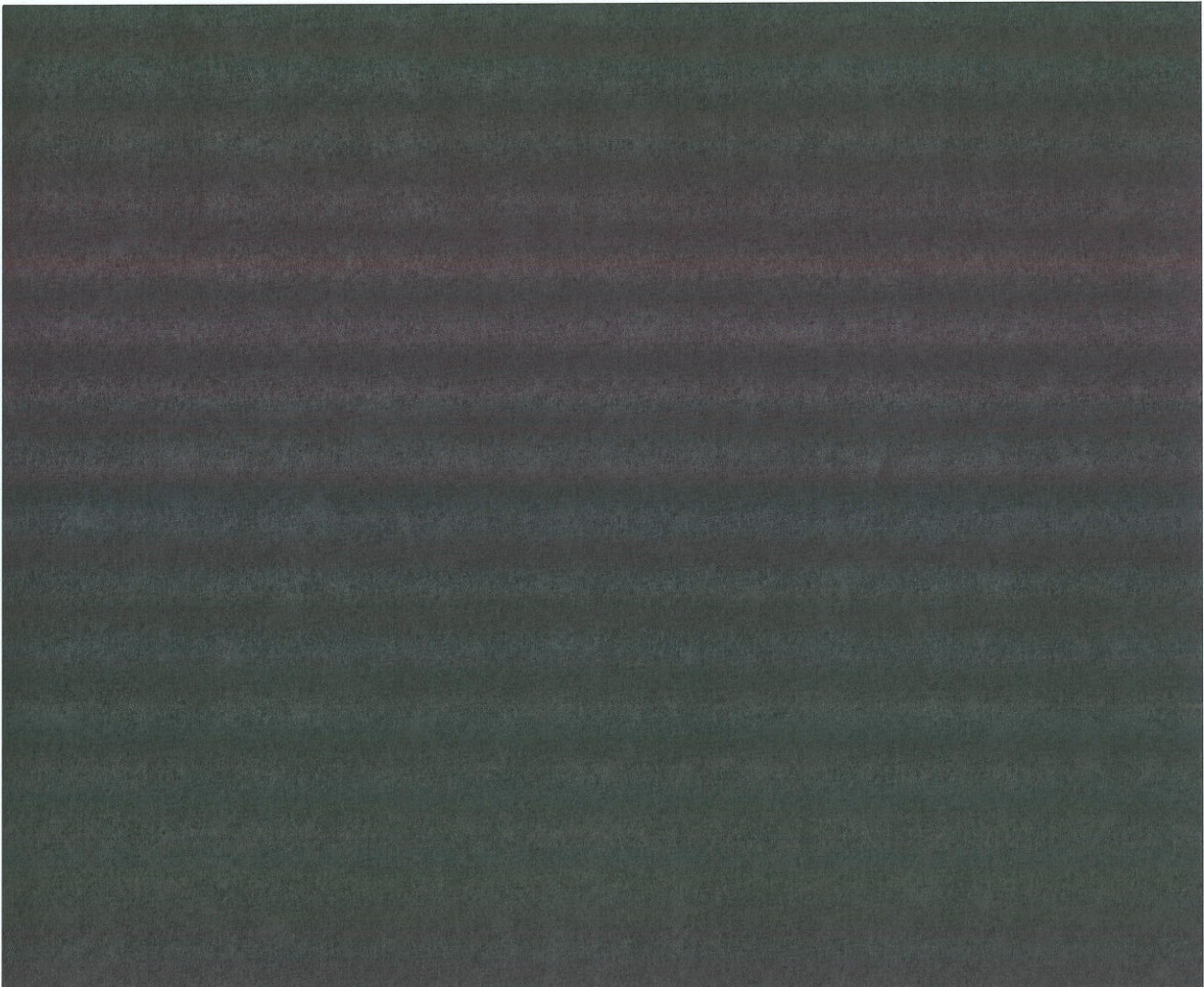
Moreover, individually targeted pen registers could never provide the instantaneous ability to trace terrorist connections by chaining two steps

[REDACTED]

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

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

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. DIRNSA Decl. ¶ 12. ~~(TS//SI//NF)~~



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

Performing the meta data analysis described above necessarily requires collecting data in *bulk*. In other words, it entails collecting data on a significant number of communications that

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

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

will not ever be found to have a connection with terrorists. The breadth of the collection, however, is inevitable. The very reason for collecting the data to preserve it for later analysis is that it is impossible to target solely the e-mail of terrorists, because the e-mail accounts used by terrorists are not yet known [REDACTED] ~~(S)~~

Although effective meta data analysis requires broad collection and archiving of meta data, it does not require indiscriminate, random collection of data. To the contrary, the NSA has no desire to collect more data than necessary. As we explain more fully below, the order sought in this Application targets collection of meta data [REDACTED]

[REDACTED] In addition, to minimize the amount of U.S. person information collected, this Application focuses almost exclusively on [REDACTED]

[REDACTED] DIRNSA Decl. ¶ 25.⁹ ~~(TS//SI//NF)~~

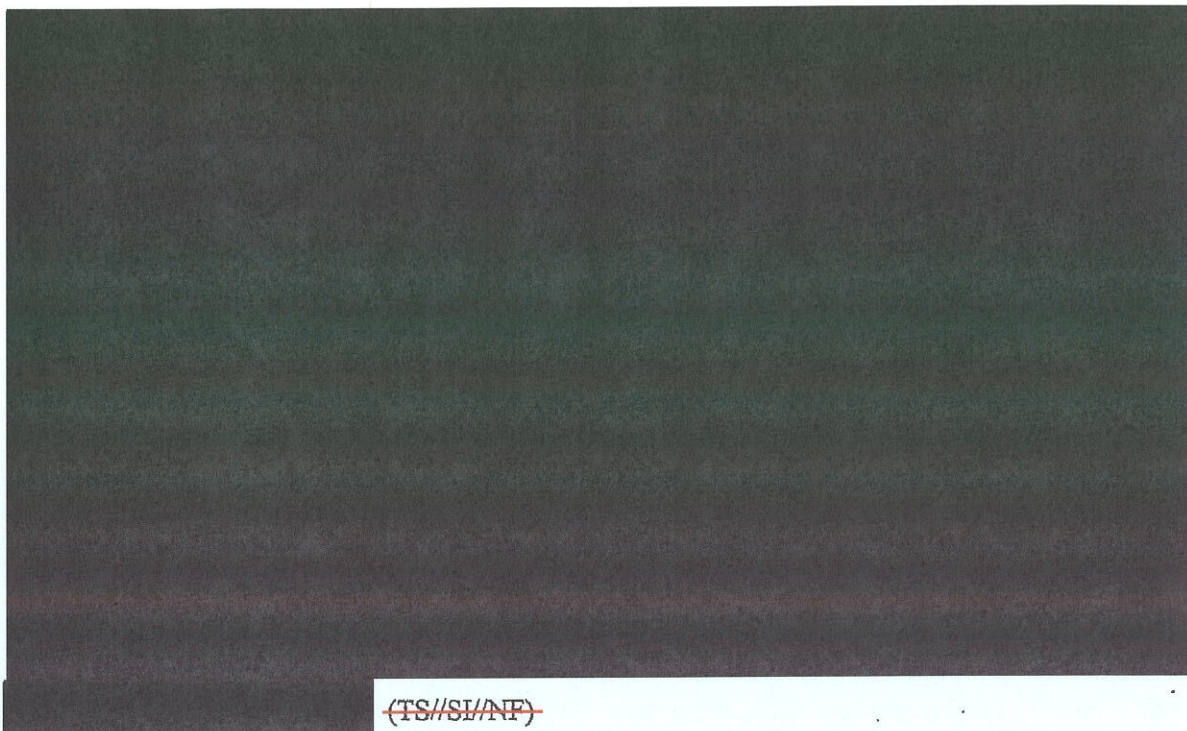
[REDACTED]

9

[REDACTED] DIRNSA Decl. ¶ 20 n.13.

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

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



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

E. Searching the Meta Data ~~(S)~~

After the NSA has collected and archived meta data, the use of that data will be subject to strict procedures and safeguards. First, as described in the attached Declaration from the Director, the NSA will query the archived data solely when it has identified an e-mail for which, "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 E-mail address is associated with [REDACTED]" DIRNSA Decl.

¶ 22. Similarly, [REDACTED] would be undertaken only with respect to such an identified

¹⁰ Were the NSA to use pen registers targeted individually at specific terrorist-associated e-mail accounts to collect the e-mail addresses in contact with those accounts and the e-mail addresses in contact with the first-tier of e-mail addresses, *i.e.*, going "two hops out"—a process that would entail approximately [REDACTED] pen register applications per year—the NSA would acquire approximately [REDACTED] percent of all the e-mail addresses that would be collected by the [REDACTED] if the current Application were granted. Of course, acquiring e-mail addresses using individually targeted pen registers, [REDACTED] would not permit the NSA to use the crucial analytic tools of historical contact chaining [REDACTED]. As a result, using such an individually targeted approach, the NSA would not be able, in fact, even to identify the [REDACTED] e-mail addresses on which to seek the individual pen registers. DIRNSA Decl. ¶ 21. ~~(TS//SI//NF)~~

"seed" e-mail address. Any query of the archived data would require approval from one of seven people: the Program Manager, Counterterrorism Advanced Analysis; the Chief or Deputy Chief, Counterterrorism Advanced Analysis Division; or one of four Counterterrorism Advanced Analysis Shift Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. *Id.* ¶ 28. The NSA estimates that less than one query would be conducted daily, and typically a very low proportion of the results of the query would include U.S. person information. *Id.* ¶ 26.¹¹ ~~(TS//SI//NF)~~

Second, NSA will apply several mechanisms to ensure appropriate oversight over the use of the meta data. The NSA will apply the existing (Attorney General approved) guidelines in United States Signals Intelligence Directive 18 (1993) ("USSID 18," Attachment D to the Application) to minimize the information reported concerning U.S. persons. DIRNSA Decl. ¶ 29. Prior to disseminating any U.S. person information, the Chief of Customer Response must determine that the information is related to counterterrorism information and is in fact necessary to understand the foreign intelligence information or to assess its importance. *Id.*; see USSID 18, § 7.2 (NSA reports may include the identity of a U.S. person only if the recipient of the report has a need to know that information as part of his official duties and, *inter alia*, the identity of the U.S. person is necessary to understand the foreign intelligence information or to assess its importance).

In addition, every time one of the limited number of NSA analysts permitted to search the archived data carries out such a search, the analyst's login and IP address, and the date, time and details of the search will be automatically logged to ensure an auditing capability. DIRNSA

¹¹ For example, the NSA estimates that [REDACTED] percent of all e-mail addresses given as investigative leads to the FBI and the CIA would include U.S. person information. Based on the number of expected leads, that would amount to information regarding approximately [REDACTED] U.S. persons each month. DIRNSA Decl. ¶ 26. ~~(TS//SI//NF)~~

Decl. ¶ 23. The NSA Inspector General, the NSA General Counsel, and the Signals Intelligence Directorate Oversight Compliance Office will each periodically review this program. *Id.* ¶ 30. The DIRNSA will direct the Inspector General and General Counsel to submit an initial report to him 45 days after the initiation of the collection to assess the efficacy of the management controls and to ensure that the dissemination of U.S. person information is accomplished in accordance with USSID 18 procedures. *Id.* The DIRNSA himself will, in coordination with the Attorney General, inform the leadership of the Congressional Intelligence Oversight Committees of the Court's approval of this collection activity. *Id.* ¶ 31. ~~(TS//SI//NF)~~

Third, the collected meta data will be kept online (that is, accessible for queries by cleared analysts) for only 18 months, at which time it will be transferred to a tape system that is inaccessible to software tools and queries from analysts. If data older than 18 months old is needed in a specific case, the tape library will be searchable only by a cleared administrator. *Id.* ¶ 27. ~~(TS//SI//NF)~~

Finally, when and if the Government seeks a reauthorization from the Court for the pen registers and trap and trace devices in the Application it will provide a report about the queries that have been made and the application of the reasonable articulable suspicion standard for determining that queried addresses were terrorist related. ~~(S//SI//NF)~~

F. The Foreign Intelligence Surveillance Act (U)

FISA provides a mechanism for the Government to obtain precisely the type of communications data that is vital for the meta data analysis described above—namely, the header/router/addressing information on e-mails and other electronic communications. Title IV of FISA 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 incorporates the definitions of the terms "pen register" and "trap and trace device" from 18 U.S.C. § 3127. *See* 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.

18 U.S.C. § 3127(3).¹² Similarly, a "trap and trace device" is defined as

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)

¹² "[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." *Id.* § 2510(12). The term "[c]ontents" includes "any information concerning the substance, purport, or meaning of [a particular] communication." *Id.* § 2510(8). (U)

LEGAL ANALYSIS (U)

Title IV of FISA directs that the Court "shall" authorize a pen register or trap and trace device if an application brought before it complies with the requirements of the statute. The most significant of those requirements are that the proposed collection come within the definition of "pen registers" and "trap and trace devices" and that the Government certify that the information "likely to be obtained" is "relevant to an ongoing investigation to protect against international terrorism." 50 U.S.C. § 1842(c). The attached Application fully complies with these requirements. (U)

First, the collection the Government proposes involves the use of "pen registers" and "trap and trace devices" because it will be accomplished by devices that acquire "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). Nothing in the definitions of pen registers or trap and trace devices requires that the "instrument" or "facility" on which the device is placed carry the communications solely of a single user. (U)

Second, as for relevance to an investigation, under the plain terms of FISA, the Government's certification of relevance is determinative. Unlike certain other certifications made in other contexts under the statute, *see, e.g.*, 50 U.S.C. § 1805(a)(5), FISA does not subject the certification of relevance to any review by the Court. Even if the Court could look behind that certification, the information sought in the Application meets the statutory standard. To the extent the Court construes the "relevance" standard under Title IV to require some tailoring of the collection to limit overbreadth, the collection proposed here is not overbroad. The intelligence tools that will enable the Government to be effective in finding [REDACTED] terrorists require access to this targeted pool of data. The Government proposes collection [REDACTED]

[REDACTED] and bulk collection [REDACTED]

[REDACTED] is the only method that will enable successful use of meta data analysis. More importantly, any tailoring standard must be informed by a balancing of the government interest at stake and any intrusion into privacy involved. Here, the Government's interest is overwhelming. It involves thwarting terrorist attacks that could take thousands of lives. The privacy interest, on the other hand, is minimal. The meta data collection has been targeted as narrowly as the NSA believes it can be while maintaining effectiveness; the type of data at issue is not constitutionally protected; and even though it would be collected, it would never even be *seen* by any human being unless a terrorist connection were first established. ~~(TS//SI//NF)~~

Finally, even if the result under the statute were not so clear, any doubt should be resolved in favor of construing the statute to permit the Application. Reading FISA to preclude the collection of the intelligence information described in the attached Application, which falls within the President's constitutional powers as Commander in Chief and Chief Executive, would raise grave constitutional questions that this Court should avoid by interpreting Title IV to authorize the proposed collection. ~~(S)~~

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

Title IV of FISA directs that the Court "shall" authorize a pen register or trap and trace device if an application complies with the requirements of the statute. 50 U.S.C. § 1842(d)(1).

In particular, section 402(d)(1) provides that,

[u]pon an application made pursuant to this section, the judge [of the Foreign Intelligence Surveillance 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 *if the judge finds that the application [for such an order] satisfies the requirements of this section.*

Id. (emphasis added). There are four statutory requirements. First, the device must qualify as a "pen register" and/or "trap and trace device." *Id.* §§ 1841(2), 1842(a)(1). Second, the application must have been approved by the Attorney General or a designated government attorney. *Id.* § 1842(c). Third, the application must include the identity of the U.S. government official seeking to use the pen register or trap and trace device covered by the application. *Id.* § 1842(c)(1). Finally, the applicant must certify that the information "likely to be obtained" is "relevant to an ongoing investigation to protect against international terrorism." *Id.* § 1842(c)(2).¹³ (U)

The second and third 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 registers and trap and trace devices covered by the Application. The only requirements that merit further discussion are that the devices sought must qualify as pen registers and trap and trace devices and that the Application must contain a certification of relevance. ~~(S)~~

¹³ Until 2001, section 402 of FISA imposed a higher standard on the Government—in particular by requiring it to present information demonstrating that "there is reason to believe that the . . . communication instrument" in question "has been or is about to be used in communication with" an agent of a foreign power or some other individual who "is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation" of federal criminal law. 50 U.S.C. § 1842(c)(3) (2000). Section 214 of the PATRIOT Act, however, eliminated that requirement. See Pub. L. No. 107-56, § 214(a)(3), 115 Stat. at 286. Congress thus recognized that requiring a showing of a specific link to an agent of a foreign power or to an individual otherwise engaged in international terrorism was too onerous (and made pen registers significantly more difficult to obtain in the foreign-intelligence and counterterrorism context than they were in the context of ordinary law enforcement). As Senator Leahy explained on the floor of the Senate, allowing the FBI to get pen registers "without having to meet the statutory 'agent of a foreign power' standard" was a "potentially sweeping change[] in the relationships between the law enforcement and intelligence agencies," but it was justified in this context "because the Fourth Amendment does not normally apply to such techniques and the FBI has comparable authority in its criminal investigations." 147 Cong. Rec. S10,993 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy); see also *id.* at S11,003 (statement of Sen. Leahy) (explaining that the "agent of a foreign power" standard was "more stringent than the standard under comparable criminal law enforcement procedures which require only a showing of relevance to a criminal investigation"; that, "in practice," the standard had been "almost as burdensome as the requirement to show probable cause required . . . for more intrusive techniques"; and that "[t]he FBI ha[d] made a clear case that a relevance standard is appropriate for counterintelligence and counterterrorism investigations, as well as for criminal investigations"). (U)

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

A. The Proposed Collection Will Employ "Pen Registers" and "Trap and Trace Devices." (U)

The devices described in the attached Application that will be used to accomplish the proposed collection readily qualify as "pen registers" and "trap and trace devices" under the statute. A "pen register" includes a "device" that "records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3); *see* 50 U.S.C. § 1841(2). The pen register definition thus focuses on the way that information is collected (by a device that records outgoing routing information from a communications facility) and on the type of information acquired (routing information, as opposed to contents of communications), not on the characteristics of the communications facility to which the pen register is attached. Similarly, a "trap and trace device" includes a "device" that "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." 18 U.S.C. § 3127(4). (U)

The collection proposed here will use devices that accomplish exactly those functions.



Recent statutory amendments eliminated any doubt that pen registers and trap

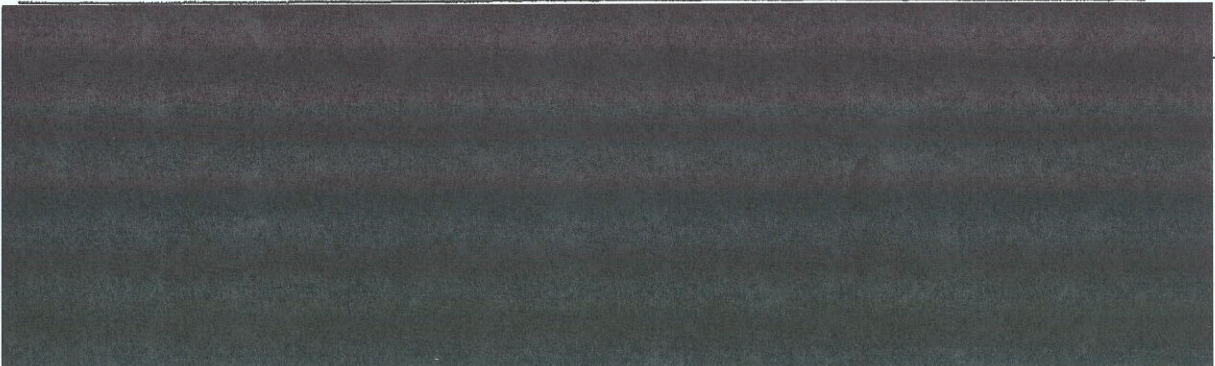


~~TOP SECRET//HCS//COMINT//NOFORN~~

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

and trace devices can be used to intercept e-mail [REDACTED] on the Internet. See *ACLU v. Dep't of Justice*, 265 F. Supp. 2d 20, 22 n.3 (D.D.C. 2003) ("[S]ection [216] of the Patriot Act expands the definition of pen registers and trap and trace devices so that they may be used not merely against telephones, but also against electronic communications (such as e-mail).").¹⁵ ~~(TS//SI//NF)~~

It is true that a pen register is most commonly used to record the routing information associated with a particular telephone number or e-mail account. But nothing in the statutory definition requires such a narrow focus. To the contrary, Congress used broad, generic terms to state that a pen register could be used to record information from any "instrument" or "facility"



¹⁵ Section 216 of the PATRIOT Act clarified title 18's definitions and other references to pen registers and trap and trace devices by making them expressly technology neutral. For example, references to "dialing and signaling information" and "the originating number" were amended to include references to "routing" and "addressing" information. Pub. L. No. 107-56, § 216(a)(2), (c)(3), 115 Stat. at 288-90. Section 216 even added an express reference to circumstances in which a law enforcement agency seeks to use "its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public"—a clear invocation of the Internet. *Id.* § 216(b)(1), 115 Stat. at 289. Section 216's changes apply to FISA because FISA incorporates title 18's definitions of pen registers and trap and trace devices. See 50 U.S.C. § 1841(2). In addition, section 214 of the PATRIOT Act made parallel amendments to section 402 of FISA. See Pub. L. No. 107-56, § 214(a)(4), 115 Stat. at 286. The PATRIOT Act's legislative history repeatedly refers to the need to ensure that pen registers and trap and trace devices apply to Internet communications. See, e.g., 147 Cong. Rec. S11,006 (daily ed. Oct. 25, 2001) (section-by-section analysis entered into the record by Sen. Leahy) (noting that section 216 "ensures that the pen register and trap and trace provisions apply to facilities other than telephone lines (e.g., the Internet)"); *id.* at S11,057 (section-by-section analysis entered into the record by Sen. Hatch) (describing section 216 as "[a]mend[ing] the pen register/trap and trace statute to apply to internet communications"); *id.* at S11,054 (DOJ analysis of bill entered into the record by Sen. Hatch) (noting that title II of the bill would make electronic surveillance statutes, including the pen/trap statute, "technology-neutral" by "ensuring that the same existing authorities that apply to telephones, for example, are made applicable to computers and use of e-mail on the Internet"); *id.* at S11,055 (same DOJ analysis stating that "[p]en/trap provisions would also now apply to Internet traffic, as well as telephone communications"). ~~(S)~~

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

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

used to transmit communications. The devices described in the Application will record information from such "facilities"—specifically, [REDACTED]

[REDACTED] Moreover, nothing in FISA further restricts these definitions to require that a pen or trap be targeted solely at the communications of a particular user. FISA requires that the Court's order approving the use of a pen register or trap and trace device specify "the identity, if known, of the person to whom is leased . . . 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) (emphasis added). Although the reference to "the telephone line" to which the device is attached might be read to suggest a focus on a single user, these provisions in no way suggest that pens and traps are *limited* to such a use. Rather, Congress again used broad terms to make clear that the pen or trap could equally be attached to any "other facility." The devices described in the attached Application would acquire information from such "other" facilities, *i.e.*, [REDACTED]

[REDACTED] (S)

Although there can be no doubt that the Application conforms with the plain language of the statute, it is also worth noting that courts have avoided construing the pen register and trap and trace provisions with cramped or overly technical readings that would frustrate their purposes. For example, until the PATRIOT Act's amendments, the definitions of pen registers and trap and trace devices hinged expressly on "attach[ing]" a "device" to a "telephone line," or using a "device" to identify "originating number[s]," 18 U.S.C. § 3127(3), (4) (2000), but the Department of Justice nevertheless routinely sought—and courts routinely granted—pen register

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

or trap and trace orders authorizing the collection of addressing and routing information from Internet communications.¹⁶ ~~(TS//SI//NF)~~

Given this background, there can be no doubt that the collection of Internet meta data that the Government seeks pursuant to the Application falls within the clarified scope of the pen register and trap and trace provisions. ~~(TS//SI//NF)~~

B. The Application Includes a Certification of Relevance That Satisfies Section 402(c). (U)

Section 402(c) of FISA requires that the Application include "a certification by the applicant that the information likely to be obtained is . . . relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." 50 U.S.C. § 1842(c). Section 402(a)(1) further requires that the investigation be "conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333." *Id.* § 1842(a)(1). The attached Application includes such a certification by the

¹⁶ See *Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the House Judiciary Comm.*, 106th Cong. 17 (2000) (statement of David Green, Deputy Chief of the Computer Crime and Intellectual Property Section, U.S. Department of Justice) ("We do view e-mail as subject to a pen register and trap and trace. In fact, we use it all the time in investigation of hacking cases, child porn cases, Internet fraud cases."); *id.* at 71 (prepared statement of Robert Com-Revere, Hogan & Hartson L.L.P.) (explaining that "[l]aw enforcement authorities have begun to get court orders for the installation of such devices at ISPs" even though, "[a]s a matter of legal interpretation, the current law does not clearly apply to ISPs and Internet communication"); *id.* at 75 (noting that there are "no reported cases" about the application of the pen/trap statute to ISPs); *id.* at 73-75 (describing a sealed case in which a magistrate judge had ordered an ISP to install a pen register or trap and trace device after concluding that the Government's proposal "to intercept email routing information is the functional equivalent of capturing telephone numbers with a pen register or trap and trace device" even though the drafters of the statute in 1986 had not contemplated "the issuance of court orders to capture email addresses of persons sending email to and receiving email from a targeted email address"); Computer Crime and Intellectual Property Section, U.S. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 113 (July 2002) ("Although the Pen/Trap statute previously included language which specifically referenced telephone communications, numerous courts [before 2001] had applied the statute to computer network communications."). ~~(S)~~

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

applicant—the Attorney General.¹⁷ See [REDACTED]

[REDACTED]
[REDACTED] 2, 26 (filed on [REDACTED]) (certifying that “the information likely to be obtained from the pen register and trap and trace devices requested in this application regarding [REDACTED]

[REDACTED] is relevant to an ongoing investigation to protect against international terrorism that is not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution” and averring that the investigation is “being conducted by the Federal Bureau of Investigation (FBI) under such guidelines as the Attorney General approves pursuant to Executive Order No. 12,333”). ~~(S)~~

The FBI is currently conducting more than [REDACTED] investigations into [REDACTED]

[REDACTED] Archiving and analyzing the meta data acquired by the devices attached to the [REDACTED] described in the Application will assist the FBI in obtaining foreign intelligence and, in particular, in identifying the e-mail addresses of [REDACTED] operating within the United States who are determined to attack our Nation. For example, contact chaining [REDACTED] of the archived information will allow the NSA to furnish the FBI with e-mail addresses that have been in contact with e-mail accounts the NSA reasonably suspects to be linked to [REDACTED]

[REDACTED] The FBI will then be able to begin its own investigations to identify the users of the e-mail addresses and to determine any links to international terrorist activities. In addition, the leads from the NSA would greatly enhance the FBI’s ability to “connect the dots” in existing FBI international terrorism investigations, thereby more fully uncovering links between an existing target and [REDACTED] The FBI would also benefit from being able to ask the

¹⁷ Under section 402(a)(1), the applicant may be either “the Attorney General or a designated attorney for the Government.” 50 U.S.C. § 1842(a)(1). (U)

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

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

NSA to perform contact chaining [REDACTED] on known terrorist-associated e-mail addresses uncovered by the FBI. ~~(TS//SI//NF)~~

The plain text of section 402 indicates that, while the Court has discretion to deny the attached Application if it does not meet any of the four requirements set forth in section 402(c)—*i.e.*, if the devices do not qualify as pen registers or trap and trace devices, if the Application was not approved by the Attorney General or a designated government attorney, or if the Application does not include the identity of the government official seeking to use the devices or a certification of relevance—Congress did not give the Court the power to look behind a certification of relevance to reevaluate its validity. Section 402 directs that the Court “shall enter an ex parte order” approving an application that meets the requirements of the section, and in setting out the requirement of a certification of relevance, requires solely that the Government make the certification, not that the Court review it in any way. 50 U.S.C. § 1842(d). (U)

The absence of any textual suggestion that the Court may reevaluate the certification of relevance or subject it to review is significant, because where Congress intended the Court to have a role in examining a certification made to the Court under FISA, it made that role express in the text of the Act. For example, under section 104 of FISA, which governs electronic surveillance, the Government must certify, among other things, that the information sought is “foreign intelligence information.” 50 U.S.C. § 1804(a)(7)(A). Under section 105(a)(5), that certification is expressly made subject to review by the Court for clear error, but only in cases involving U.S. persons. *See* 50 U.S.C. § 1805(a)(5) (court may approve application if it finds that, “if the target is a United States person, the certification or certifications [required by section 104] are not clearly erroneous”). Where the target is a non-U.S. person, the statute specifies no role for the Court in conducting review, and the result is that the Court cannot review the

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

certification at all. Indeed, the legislative history of section 105 makes it clear that the “court is not allowed to ‘look behind’ the certification in cases not involving U.S. persons.” S. Rep. No. 95-701, at 54, *reprinted in* 1978 U.S.C.C.A.N. 3973, 4023.¹⁸ (U)

The absence of any express indication in section 402(c) that the Court may reevaluate the certification of relevance is thus important, because “[w]here Congress includes particular language in one section of a statute but omits it in another section of the Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.” *Russello v. United States*, 464 U.S. 16, 23 (1983) (internal quotation marks omitted). (U)

The carefully circumscribed role Congress prescribed for the Court in looking behind any of the certifications required under various provisions of FISA—and its decision not to give the Court any power to look behind a certification of relevance under section 402—makes perfect sense given the subject matter of the certifications at issue. For electronic surveillance applications, for example, the certification that the information sought is “foreign intelligence information,” 50 U.S.C. § 1804(a)(7)(A), is a matter uniquely within the competence of the Executive. *See, e.g., Reno v. American-Arab Anti-Discrimination Comm.*, 525 U.S. 471, 490-91 (1999) (explaining that, when the Executive bases actions on “foreign-policy objectives and . . .

¹⁸ The legislative history explains:

If the application meets the requirements of [section 104(a)(7)], the court is not permitted to substitute its judgment for that of the executive branch officials, except where a U.S. person is the target of a surveillance. . . .

Despite the fact that the court is not allowed to “look behind” the certification in cases not involving U.S. persons there are several checks against the possibility of arbitrary executive action. First, the court, not the executive branch, makes the finding of whether probable cause exists that the target of surveillance is a foreign power or its agent. Second, the certification procedure assures written accountability within the executive branch for the decision made to engage in such surveillance. This constitutes an internal check on executive branch arbitrariness.

Moreover, it should be noted that if the description and certification do not fully comply with [section 104(a)(7)], they can and must be rejected by the court. Thus, the court could invalidate the certification if it . . . did not state that the information sought is deemed to be foreign intelligence information [that] cannot feasibly be obtained by normal investigative techniques.

S. Rep. No. 95-701, at 54, 1978 U.S.C.C.A.N. at 4023. (U)

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

foreign-intelligence products and techniques,” courts are “ill equipped to determine their authenticity and utterly unable to assess their adequacy”); *Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988) (“authority to classify and control access to information bearing on national security . . . flows primarily from [the] constitutional investment of [the foreign affairs] power in the President”). Congress thus precluded the Court from having any role in reviewing that certification in cases where the target is a non-U.S. person. To provide greater protection for the privacy rights of U.S. persons, Congress gave the Court some role in those cases, but even there restricted review to clear error. *See* 50 U.S.C. § 1805(a)(5). The certification at issue here under section 402(c) involves matters equally within the Executive’s expertise—namely, whether information likely to be obtained is “foreign intelligence information” or is “relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities.” 50 U.S.C. § 1842(c)(2). Particularly because there is no constitutionally protected interest at all in the type of information at issue under this provision (dialing, routing, addressing, or signaling information), *see infra* pp. __–__, it is perfectly in keeping with the statutory scheme for Congress here to restrict the Court’s role and provide the Court with no power to look behind the Government’s certification.¹⁹ (U)

The legislative history also confirms this interpretation. The Senate Report on the Act that added section 402 explains that Congress intended to “authorize[] FISA judges to issue a pen register or trap and trace order *upon a certification that* the information sought is relevant to” an investigation being conducted by the FBI. S. Rep. No. 105-185, at 27 (1998) (emphasis

¹⁹ The conclusion that the Government’s certification of relevance under section 402 is not subject to reexamination by the Court is also supported by the fact that the statute does not require the Government to provide any statement supporting the certification. In contrast, the electronic-surveillance provisions in Title I of FISA require the Government to include a statement providing the basis for its certification that the information sought is “foreign intelligence.” *Id.* § 1804(a)(7)(E). The absence of any similar requirement for the certificate of relevance further indicates that Congress did not intend for the Court to have a role in examining the Government’s justifications for its certification. (U)

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

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

added). It is the certification from the Executive that is important, not an independent evaluation by the Court. This makes sense, because Congress clearly recognized that providing independent judicial review was not always necessary under FISA to provide some check on executive action. As the legislative history explains in the context of unreviewable certifications under section 105, "the certification procedure assures written accountability within the executive branch for the decision made to engage in such surveillance. This constitutes an internal check on executive branch arbitrariness." S. Rep. No. 95-701, at 54, 1978 U.S.C.C.A.N. at 4023. (U)

In addition, the legislative history of section 402 explains that Congress wanted to equalize the playing field between criminal investigations on the one hand and foreign intelligence or international terrorism investigations on the other. See S. Rep. No. 105-185, at 27 (Title IV "establishes a predicate for the use of pen registers or trap and trace devices that is . . . analogous to the statutory standard for the use of these devices in criminal investigations").²⁰ Although the legislative history of Title IV does not elaborate further on the role, if any, that the Court should have in reviewing certifications of relevance, the legislative history of the comparable provisions in title 18, 18 U.S.C. §§ 3122(b)(2), 3123(a)(1), is more specific. It explains:

To issue an order, the court must first be satisfied that the information sought is relevant [*sic*] to an ongoing criminal investigation. *This provision does not envision an independent judicial review of whether the application meets the*

²⁰ According to the comparable criminal law enforcement provisions, "[a]n application [for a pen register or trap and trace device] shall include—(1) the identity of the attorney for the Government . . . making the application and the identity of the law enforcement agency conducting the investigation; and (2) a certification by the applicant that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b). In turn, the court "shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device . . . if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." *Id.* § 3123(a)(1). (U)

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

relevance standard, rather the court needs only to review the completeness of the certification submitted.

S. Rep. No. 99-541, at 47, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3601 (emphasis added). Thus, the legislative history of the provision on which sections 402(c) and (d) of FISA are modeled confirms that the Court's appropriate role is to determine solely that the certification is complete in that it makes the necessary statements, including, *inter alia*, that "the information likely to be obtained is . . . relevant to an ongoing investigation to protect against international terrorism." 50 U.S.C. § 1842(c)(2). (U)

Indeed, during the debate over the PATRIOT Act—which amended both section 402 of FISA and the comparable provisions in title 18—Senator Leahy discussed at length the restricted role the statutes permit the courts in approving applications for pen registers and trap and trace devices. He noted that judicial review in the context of pen registers is "unlike any other area in criminal procedure" because the statutes affirmatively "bar[] the exercise of judicial discretion in reviewing the justification for the order." 147 Cong. Rec. S10,999 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy). He was disappointed that the PATRIOT Act was not altering the existing law to provide for more searching judicial review.²¹ As he explained, "[t]he court is required to issue an order upon seeing the prosecutor's certification. The court is not authorized to look behind the certification to evaluate the judgement [*sic*] of the prosecutor." *Id.* at S11,000. Moreover, he specifically noted that his "concerns" about the lack of judicial "discretion to make the decision on relevance" were fully applicable to "pen registers and trap and trace under FISA," because the PATRIOT Act would not change existing law in that regard. *Id.* at S11,003. (U)

²¹ As Senator Leahy noted, the PATRIOT Act was not the first time Congress rejected an opportunity to make judicial review in the pen register context more robust. Senator Leahy had previously introduced bills that would have done so, and such proposals had received support from the Clinton Administration and the House Judiciary Committee at certain points, *see* 147 Cong. Rec. at S10,999-S11,000, but never became law. (U)

Given Congress's consistent refusal to change the judicial review standards in the pen register and trap and trace context, it is perhaps unsurprising that the federal courts of appeals that have interpreted the title 18 provisions have repeatedly concluded that, even in the criminal context, the role of the reviewing court is to examine the completeness of the application and not to engage in an independent inquiry into the basis for the certification. As the U.S. Court of Appeals for the Second Circuit has explained, 18 U.S.C. § 3122(b)(2) "was not intended to require independent judicial review of relevance; rather, the reviewing court need only verify the completeness of the certification." *In re United States*, 10 F.3d 931, 935 (2d Cir. 1993); *see also United States Telecom Ass'n v. FCC*, 227 F.3d 450, 454 (D.C. Cir. 2000) (pen register orders require only a certification of relevance rather than "the strict probable cause showing necessary for wiretaps"); *Brown v. Waddell*, 50 F.3d 285, 290 (4th Cir. 1995) (noting that a court may authorize a pen register or trap and trace device for law enforcement purposes based on a "mere finding" that the applicant has made the required certification and contrasting that "much less stringent" requirement with the probable cause determination needed to authorize intercepting the contents of communications); *United States v. Hallmark*, 911 F.2d 399, 402 (10th Cir. 1990) ("Given the lack of any 'legitimate expectation of privacy' at stake, the extremely limited judicial review required by 18 U.S.C. § 3122 is intended merely to safeguard against purely random use of this device by ensuring compliance with the statutory requirements established by Congress.") (quoting *Smith v. Maryland*, 442 U.S. 735, 739-46 (1979)); *cf. id.* (rejecting argument that "judicial review involved in pen register and trap and trace requests is so narrowly limited and essentially ministerial as to subject the courts to the discretion of the Executive in violation of the constitutional separation of powers"). Congress established this minimal role for the courts to expedite investigations in a context where countervailing privacy interests merit

~~TOP SECRET//ICS//COMINT//NOFORN~~

little weight because, as we discuss below, individuals possess no Fourth-Amendment-protected privacy interest in the information obtained by such devices. *See In re United States*, 846 F. Supp. 1555, 1559 (M.D. Fla. 1994); *see also Smith v. Maryland*, 442 U.S. 735 (1979) (no legitimate expectation of privacy in information obtained from telephone pen registers). (U)

C. Even if the Court Could Look Behind the Certification of Relevance, the Information Sought Is Relevant to an Ongoing International Terrorism Investigation. (U)

Even were the Court to conclude that it has discretion to review whether the bulk e-mail meta data likely to be obtained from the installation and use of the pen registers and trap and trace devices specified in the attached Application is information that is "relevant" to an ongoing investigation to protect against international terrorism, the collection satisfies that standard. ~~(S)~~

1. The Particular Information Sought Meets the Relevance Standard. (U)

Information is "relevant" to an ongoing international terrorism investigation if it bears upon, or is pertinent to, that investigation. *See* 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"); *see also 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"); *cf.* 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.") (emphasis added). As we have explained above, the bulk e-mail meta data that would be acquired from [REDACTED]

~~TOP SECRET//ICS//COMINT//NOFORN~~

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

described in the attached Application bears upon and is pertinent to the FBI's investigations into [REDACTED] because, when acquired, stored, and processed, the e-mail meta data would provide vital assistance to investigators in tracking down [REDACTED] operatives. Although admittedly a substantial portion of the e-mail meta data that is collected would not relate to operatives of [REDACTED] [REDACTED]²² the intelligence tool that the Government hopes to use to find [REDACTED] communications—meta data analysis—requires collecting and storing large volumes of the meta data [REDACTED] to enable later analysis. As we have explained, unless e-mail meta data is stored at the time of transmittal, it will be lost forever. All of the meta data collected is thus relevant, because it is necessary for the success of the investigative tool.

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

In addition, the collection the Government proposes has been carefully targeted at [REDACTED]

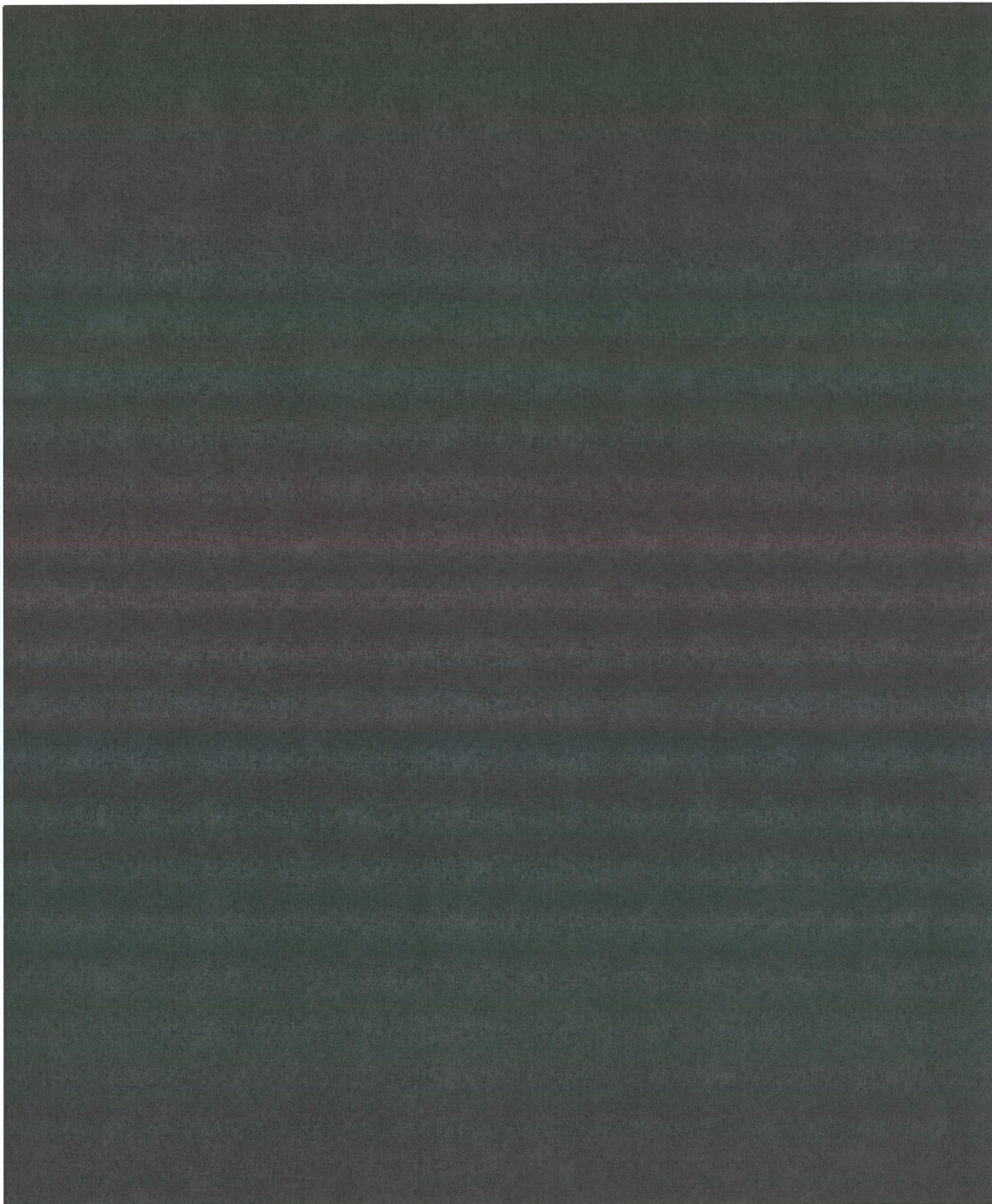
In particular:

[REDACTED]

²² The National Security Agency expects that this surveillance, over the course of a year, will result in the collection of meta data pertaining to [REDACTED] ~~(TS//SI//NF)~~

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

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

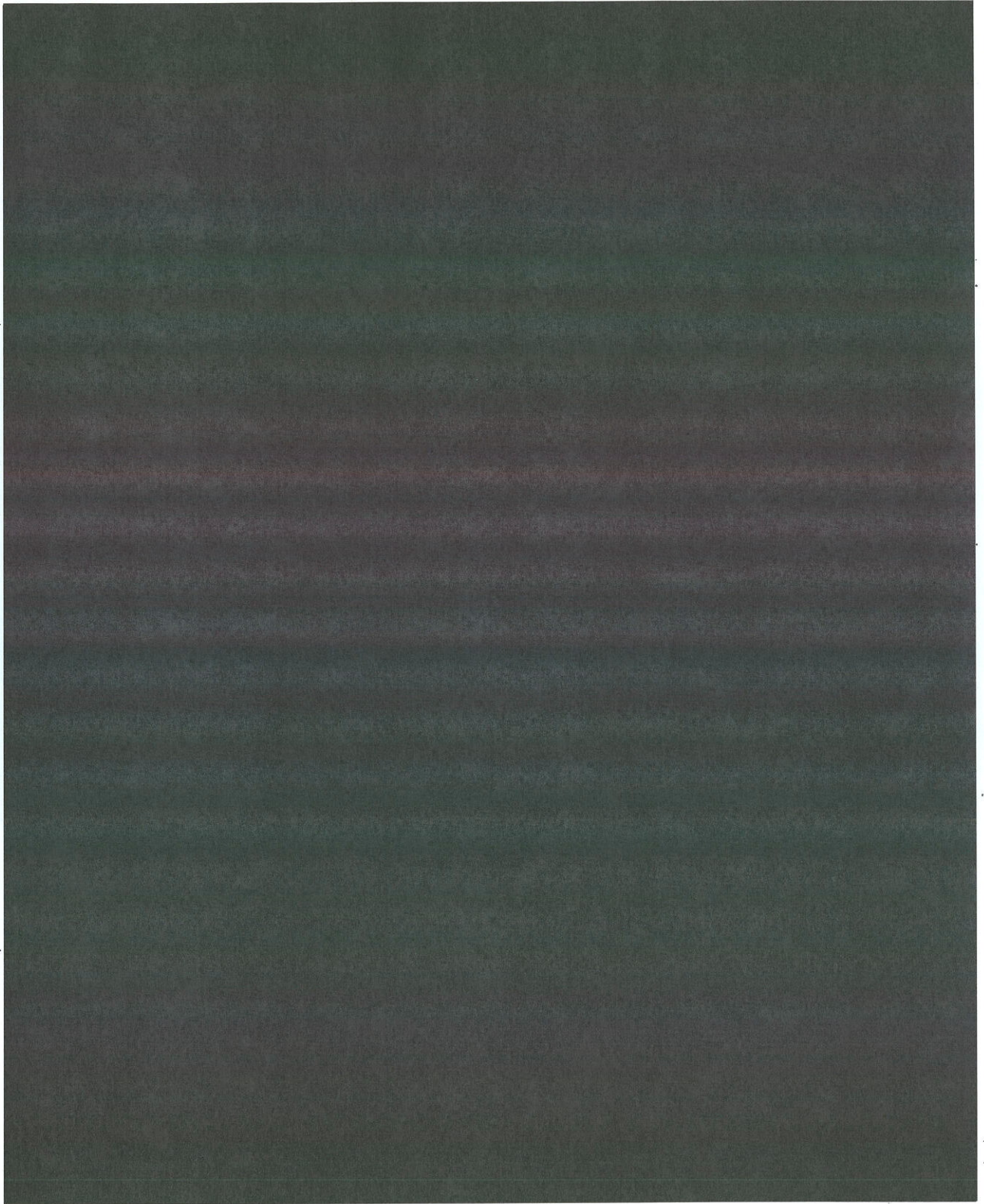


²³ See also DIRNSA Decl. ¶ 8(a)

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

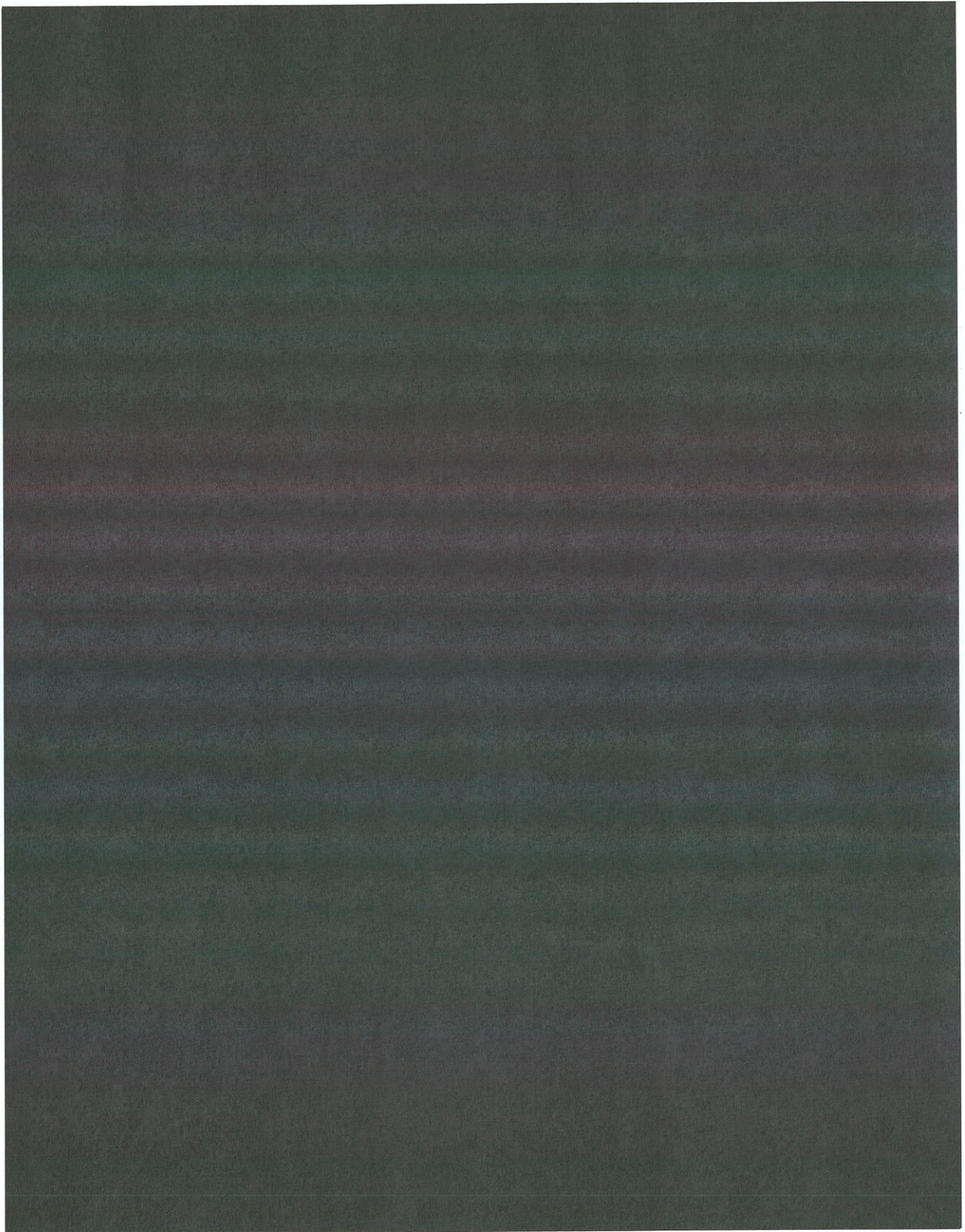
~~TOP SECRET//HCS//COMINT//NOFORN~~

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



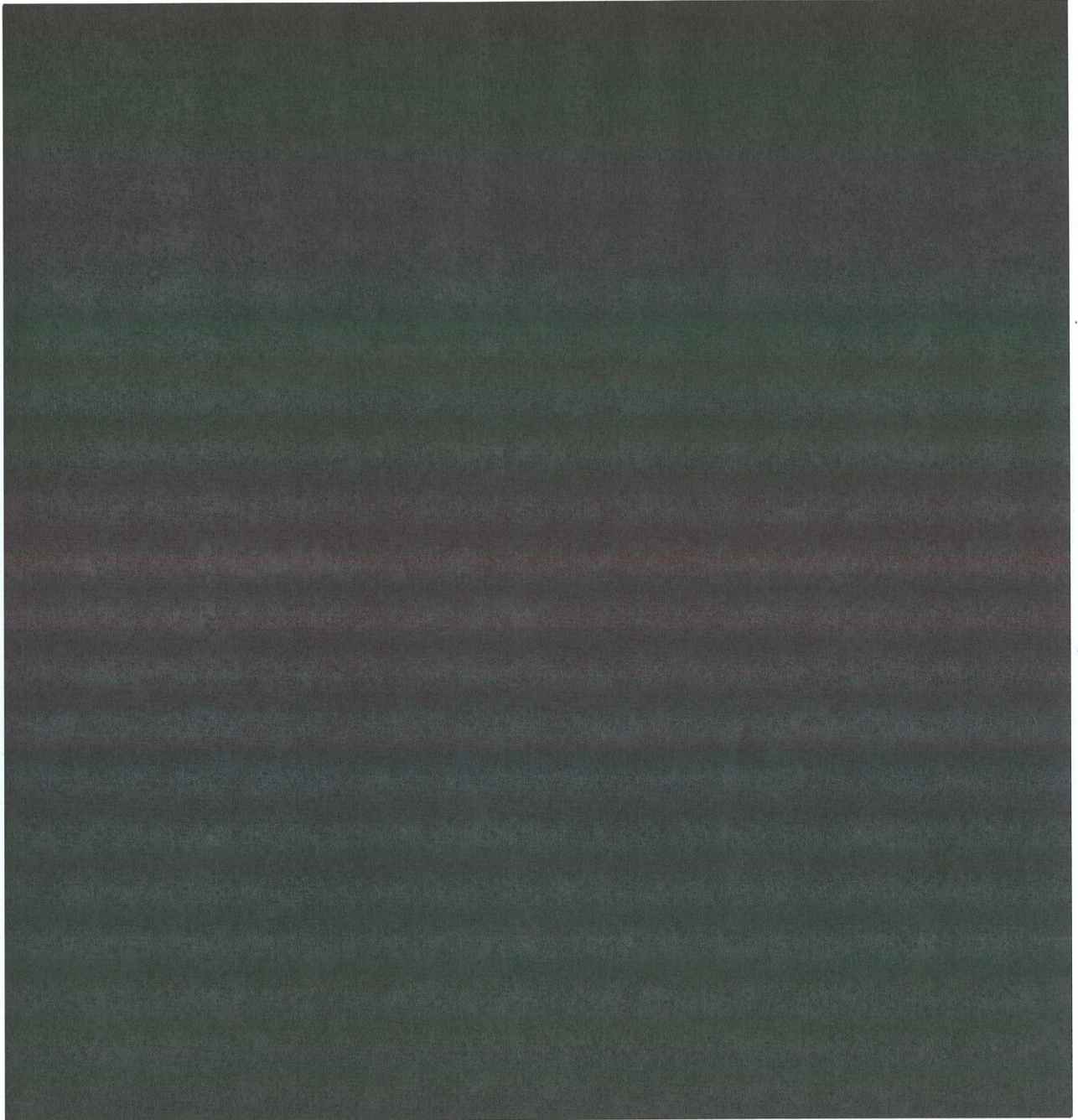
~~TOP SECRET//HCS//COMINT//NOFORN~~

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



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

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



24

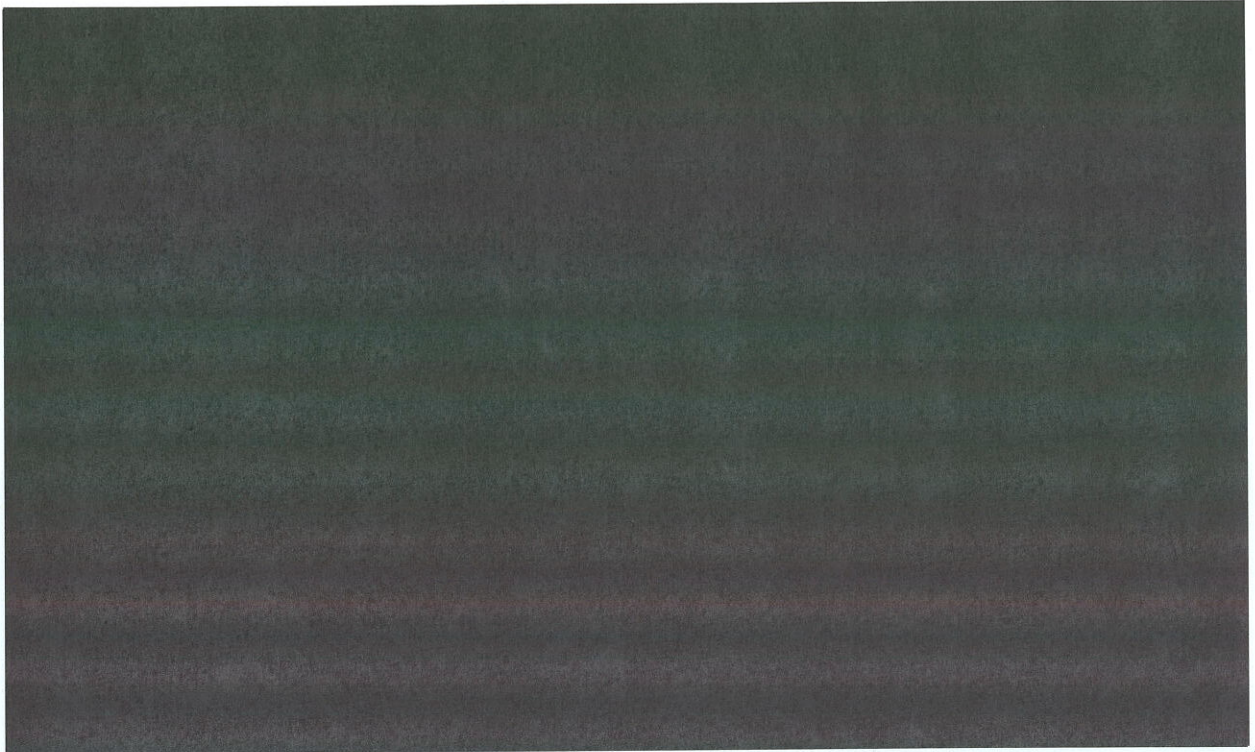
~~DIRNSA Decl. ¶ 8(e)(4) & n.8. (TS//SI//NF)~~

25

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

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

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



2. The Proposed Collection Is Appropriately Tailored. (U)

Although the Government has selected the [REDACTED]

[REDACTED] it remains true that the overwhelming majority of communications from which meta data will be collected will not be associated with [REDACTED]. That does not, however, present any infirmity under the statute. First, as noted above, all of the meta data collected is properly considered relevant to the FBI's investigations into [REDACTED] because full collection of all the data is vital for the use of the analytic tools the NSA will bring to bear to find [REDACTED] communications. In addition, it is important that Title IV of FISA does not expressly impose any requirement to tailor collection precisely to obtain solely communications that are strictly relevant to the investigation. Finally, and most importantly, even if the Court construes the [REDACTED]

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

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

relevance standard in section 402 to require some tailoring, the tailoring analysis must be informed by the balance between the overwhelming national security interest at stake here and the minimal intrusion into privacy interests that will be implicated by collecting meta data—especially meta data that will never even be seen by a human being unless a connection to a terrorist-associated e-mail is found. ~~(TS//SI//NF)~~

First, all of the meta data collected in bulk is relevant to the FBI's investigations into [REDACTED] for this reason: It is vital to have the pool of meta data available in order to use the analytical tools that will enable the NSA to discover enemy communications. *Cf. Oppenheimer Fund*, 437 U.S. at 351 ("relevant" in Fed. R. Civ. Proc. 26(b)(1) has been "construed broadly to encompass any matter that . . . could lead to other matter that could bear on, any issue that is or may be in the case"). The collection has been [REDACTED]

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

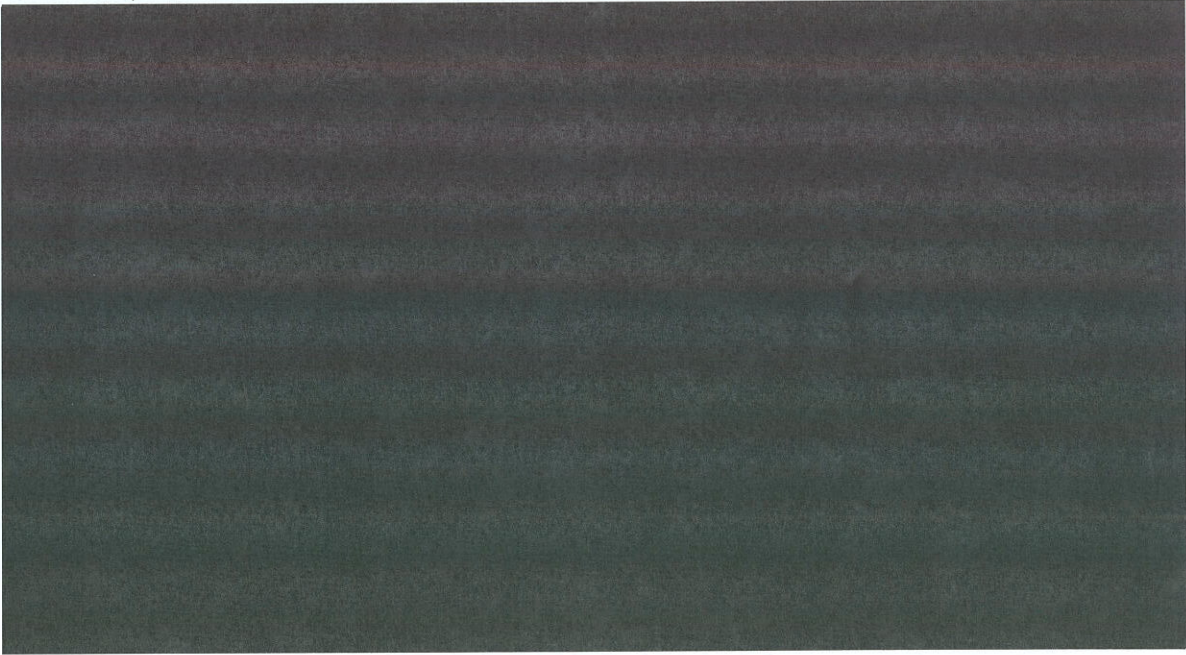
Second, there is no requirement in Title IV of FISA that pen registers or trap and trace devices acquire only narrowly tailored information. The only statutory requirement is that "the information likely to be obtained" be "relevant to an investigation to protect against international terrorism." 50 U.S.C. § 1842(c). That standard plainly 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 run-of-the-mill pen register cases, many communication events are recorded that do not directly bear upon the investigation at issue. (U)

In other contexts, moreover, even where greater privacy interests are at stake and where the terms of the statute do reflect a concern for tailoring collection, this Court has recognized that conditions may require substantially overbroad collection to obtain the relevant intelligence the

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

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

Government seeks. Thus, in the context of electronic surveillance, the text of FISA requires tailoring the collection to the objective of the surveillance by demanding that the Government set forth facts justifying its belief that “each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.” 50 U.S.C. § 1804(a)(4)(B). Nevertheless, even in that context—which implicates the substantially greater privacy protections that are accorded by the Constitution to the *contents* of communications²⁷—the Court has appropriately allowed a substantial amount of “overbroad” collection when necessary for technical reasons. For example, in Docket Nos. [REDACTED]



Here, the Government faces a somewhat analogous dilemma, but involving much lower stakes in terms of the privacy interests involved. The Government knows that the particular [REDACTED]

At present, however, it cannot identify precisely which communications from the stream of [REDACTED]

²⁷ Cf. S. Rep. No. 105-185, at 27 (explaining that Title IV of FISA was added because applying the Act’s requirements for interception of the contents of communications to the process for obtaining pen registers and trap and trace devices “impose[d] a standard that is more rigorous than the [C]onstitution requires”). (U)

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

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

millions are carrying terrorists' messages. It therefore seeks to collect solely the addressing information from the communications—not their contents—so that it can use the data later to trace the connections between terrorist e-mails. ~~(TS//SI//NF)~~

Finally, and most importantly, to the extent the Court concludes that the standard of relevance under the statute requires some element of tailoring to limit overbroad collection, any such tailoring analysis should be informed by balancing the Government's interests in conducting the collection against the potential intrusion into individual privacy interests that the collection will entail. One of the principal objectives of the entire statutory scheme under FISA is 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. Of course, as we explain below, there is no Fourth Amendment-protected interest in the e-mail meta data at issue here. As a result, the actual *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 402 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—can provide a useful guide for analysis here. ~~(S)~~

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

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

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. 822, 829 (2002). Under that analysis, moreover, the Supreme Court has made clear that, even where constitutionally protected interests are at stake, 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 quotation marks omitted); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995) ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."). Instead, the 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." *Vernonia*, 515 U.S. at 663. (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 noted that the roadblocks resulted in the arrest for drunken driving of only 1.6 percent of the drivers passing through them. The Court concluded that this success rate established sufficient "efficacy" to sustain the constitutionality of the practice. See *Michigan Dep't of State Police v. Sitz*, 496 U.S.

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

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

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). As the Fourth Circuit explained in rejecting a Fourth Amendment challenge to a state statute requiring incarcerated felons to supply a blood sample for a DNA data bank that could be used for solving crimes, "[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 v. Agee*, 453 U.S. 280, 307 (1981) (internal quotation marks omitted). Tracking down agents of [REDACTED] is essential to safeguarding the Nation from the grave threat of further terrorist attacks that could take hundreds, or thousands, of lives. The attached Application does not merely seek to collect meta data in connection with a routine investigation, but rather to help prevent another national tragedy. Acquiring bulk e-mail meta data is a crucial step in the process of locating terrorists. Archiving the meta data, moreover, is the only way to enable historical chaining [REDACTED] of electronic communications. Those methods of analysis are invaluable tools in efforts to connect the dots between terrorists. Relying solely on targeted meta data collection is a vastly inadequate response because the Government cannot know [REDACTED] exactly which e-mails 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 will be based on reasonable suspicion

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

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

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 meta data associated with their electronic communications. There is, of course, no constitutionally protected privacy interest in such e-mail meta data. Rather, it is precisely analogous to the dialed-number information for telephone calls considered by the Supreme Court in *Smith v. Maryland*, 442 U.S. 735 (1979), or the addressing information on the outside of a piece of mail. 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). The Court concluded that telephone subscribers know that they must convey the numbers they wish to call to the telephone company for the company to complete their calls. Thus, 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 743-44.²⁸ As a result, the installation of a pen register (or trap and trace device) does not even amount to a search under the Fourth Amendment. *See id.* at 745-46. ~~(S)~~

²⁸ See also *United States v. Miller*, 425 U.S. 435, 443 (1976) (“This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”). (U)

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

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

The principles outlined in *Smith* fully apply to the parallel context of e-mails. First, e-mail users have no subjective expectation of privacy in e-mail meta data information. Just like the numbers that a caller dials on a telephone, the addressing information on an e-mail is freely shared to enable the delivery of the message. Second, even if a user could somehow claim a subjective expectation of privacy in e-mail meta data, that is not an expectation "that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). 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 users assume the risk that the addressing information on their e-mails may be shared.²⁹ ~~(S)~~

In weighing the intrusion into privacy that the proposed collection would involve, it is also significant that, while the Government may collect and archive into a computer a large volume of meta data, only a tiny fraction of that information will ever be seen by any human being and then only on the basis of a targeted inquiry. As described below, the Government will search the archived data only in prescribed ways designed to uncover terrorist-associated e-mail accounts. Meta data concerning an individual's communications that is collected on one of the [REDACTED] will be subject to scanning by a computer algorithm, but the information pertaining to that individual's e-mail account 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 address [REDACTED]

The fact that no

²⁹ Commentators have also recognized that e-mail addressing information is analogous to telephone numbers, see Orin S. Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 611-15 (2003), and that, "[g]iven the logic of *Smith*, the [Supreme] Court is unlikely to recognize a constitutional difference between e-mail addressing information and the information that a telephone pen register reveals," Tracey Maclin, Katz, Kyllo, and Technology, 72 Miss. L.J. 51, 132 (2002). ~~(S)~~

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

person will ever view the overwhelming majority of the information collected here reduces even further the weight to be accorded any intrusion into privacy.³⁰ ~~(TS//SI//NF)~~

When the Government's need for the meta data collection at issue is balanced against the minimal intrusion on the privacy interests of those innocent users of the Internet whose e-mail meta data 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. ~~(S)~~

Two further analogies can help demonstrate that, even if the Court were permitted to review the Application for the tailoring of the "fit" between the collection sought and the critical terrorist-related information that the Government ultimately needs to use, the Application should be approved. (U)

First, the bulk collection of meta data is in many respects similar to an investigative response that might be used to deal with the ongoing threat posed by a serial sniper. To identify the sniper, the police may use road blocks to cordon off an area around a shooting and to photograph the license plates of every car leaving the area. Such an approach would

³⁰ As the Court is aware, in cases such as the matter in Docket Nos. [REDACTED] discussed above, where overbroad content collection is made inevitable by technological constraints, [REDACTED] Thus, even where constitutionally protected interests are actually at stake, overbreadth is considered permissible when necessary to obtain the critical foreign intelligence information that the Government seeks. ~~(S)~~

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

undoubtedly gather the license plates of hundreds, if not thousands, of innocent motorists. But the license plate information is not constitutionally protected, and it can provide a vital investigative tool if it is kept and then compared with the license plates of cars present at the next serial shooting. If the cars were permitted to leave without their license plates being recorded, it would be impossible to go back later and reconstruct which cars were present at the scene. Similarly, the pens and traps described in the attached Application would take "snap shots" of the meta data from certain electronic communications that could later provide crucial information for tracking down [REDACTED] agents. (S)

Second, to the extent that the information acquired [REDACTED] at least one end of each communication would be foreign—the acquisition would be analogous to obtaining a "mail cover" to monitor all articles of mail coming across the U.S. border from a particular country or region. It is well established, of course, 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) ("E-mail 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, e-mail 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)

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

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

(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").

There could be no doubt that it would be reasonable in a time of war for the Government to establish mail covers to track the articles of mail entering the United States from hostile territory or territory suspected of harboring enemy agents. ~~(TS//SI//NF)~~

In reality, there is long-established precedent for the Government, when the Nation is at risk of attack during time of war, to engage in far *more intrusive* actions to intercept or obstruct the enemy's electronic communications sent to or from the United States. Shortly after Congress declared war on Germany in World War I, President Wilson ordered the censorship of messages sent outside the United States via submarine cables, telegraph and telephone lines. See Exec. Order No. 2604 (Apr. 28, 1917).³¹ A few months later, the Trading with the Enemy Act expressly authorized government censorship of "communications by mail, cable, radio, or other means of transmission passing between the United States and any foreign country." Pub. L. No. 65-91, § 3(d), 40 Stat. 411, 413 (1917). On December 8, 1941, the day after Pearl Harbor was attacked, the Director of the FBI "was given temporary powers to direct all news censorship and to control all other telecommunications traffic in and out of the United States." Jack A. Gottschalk, "Consistent with Security" . . . *A History of American Military Press Censorship*, 5 Comm. & L. 35, 39 (1983) (emphasis added); see also Memorandum for the Secretary of War, Navy, State, Treasury, Postmaster General, Federal Communications Commission, from Franklin

³¹ The scope of the order was later extended to encompass messages sent to "points without the United States or to points on or near the Mexican border through which messages may be dispatched for purpose of evading the censorship herein provided." Exec. Order No. 2967 (Sept. 26, 1918). ~~(TS//SI//NF)~~

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

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

D. Roosevelt (Dec. 8, 1941), in *Official and Confidential File of FBI Director J. Edgar Hoover*, Microfilm Reel 3, Folder 60. President Roosevelt soon supplanted that temporary regime by establishing an Office of Censorship in accordance with the War Powers Act of 1941. See Pub. L. No. 77-354, § 303, 55 Stat. 838, 840-41 (Dec. 18, 1941); Gottschalk, 5 Comm. & L. at 40. The censorship regime gave the government access to "communications by mail, cable, radio, or other means of transmission passing between the United States and any foreign country." Pub. L. No. 77-354, § 303, 55 Stat. at 840; see also Exec. Order No. 8985, § 1, 6 Fed. Reg. 6625, 6625 (Dec. 19, 1941). ~~(TS//SI//NF)~~

Compared to the Government's practice in earlier armed conflicts, the acquisition of the meta data information described in the attached Application is extremely narrow. Not only does it involve solely information in which there is no constitutionally protected privacy interest (as opposed to the contents of communications), but it is also limited specifically to [REDACTED]

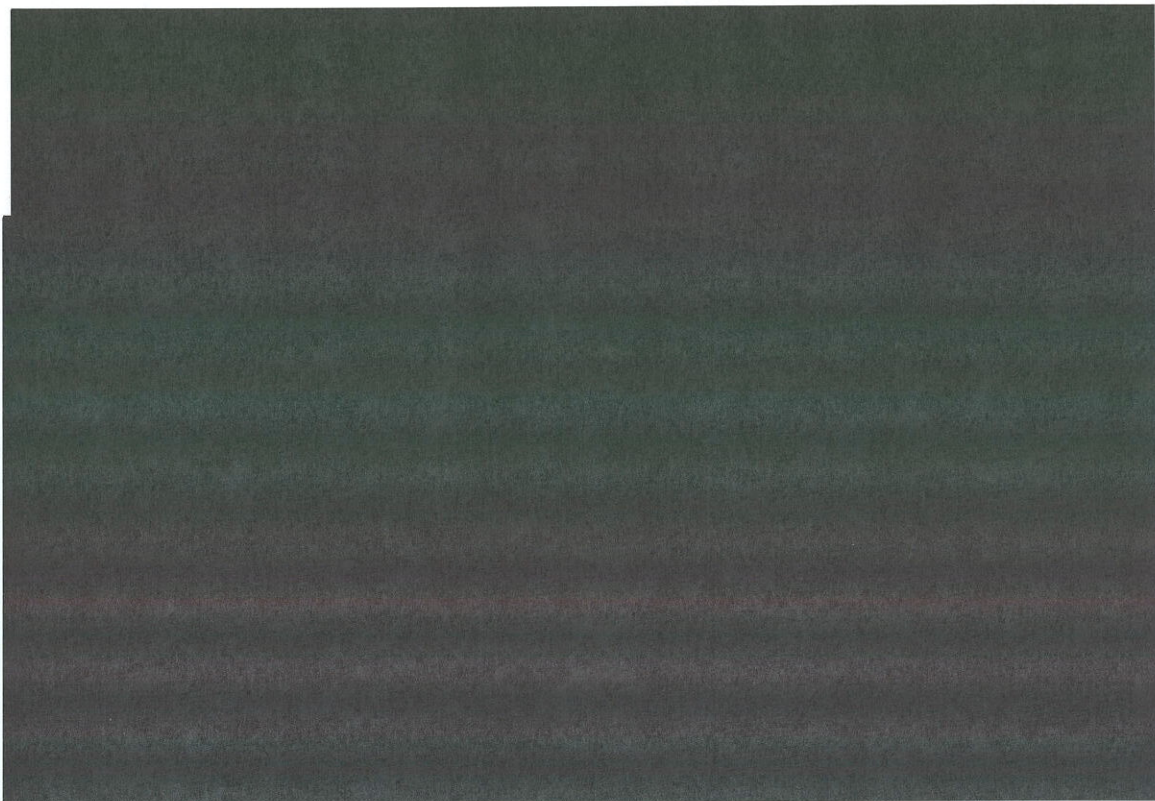
[REDACTED] Nor is there to be any attempt to censor the communications from which meta data will be acquired. ~~(TS//SI//NF)~~

Finally, to the extent the Court engages in a balancing of the Government's interest against the intrusion into privacy involved, [REDACTED]

[REDACTED]

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

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



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 one whole category of communications. If anything, the need for this specific information in a wartime context makes the Government's interest far more critical here than is the need for [REDACTED]

[REDACTED] ~~(TS//SI//NF)~~

32



(U)

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

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

The Government can assure the Court that, although the data collected under the attached Application will necessarily be broad in order to achieve the critical intelligence objectives of meta data 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)~~

First, any search or analysis of the collected data will occur only after the Government has identified a particular e-mail address that is associated with [REDACTED]

[REDACTED] In identifying such e-mail addresses, the Government will consider an e-mail 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 e-mail address is associated with agents of [REDACTED]

[REDACTED] DIRNSA Decl. ¶ 22. For example, [REDACTED]

[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").³³ The

³³ The "reasonable articulable suspicion" standard that the Government will impose on itself with respect to data collected through this Application is higher than that required by statute or the Constitution. Under FISA, the only standard to be satisfied prior to collecting information via a pen or trap is that the information be relevant to an ongoing international terrorism investigation. *See* 147 Cong. Rec. S11,003 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) (explaining that, before the PATRIOT Act, the pen register and trap and trace provisions under FISA "required a showing of reasonable suspicion, less than probable cause," that there was a specific link to an agent of a

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

determination that an e-mail address satisfies that standard must be approved by one of seven people: the Program Manager, Counterterrorism Advanced Analysis; the Chief or Deputy Chief, Counterterrorism Advanced Analysis Division; or one of four Counterterrorism Advanced Analysis Shift Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. DIRNSA Decl. ¶ 28. ~~(TS//SI//NF)~~

When such an e-mail address is identified, as outlined above, the NSA may perform [REDACTED] analysis with the meta data it has collected. It may perform contact-chaining—that is, it may search the archived data to determine what other e-mail addresses the target address has been in contact with. [REDACTED]

[REDACTED] It bears emphasis that, given the types of analysis the NSA will perform, no information about an e-mail address will ever be accessed by or presented in an intelligible form to any person unless either (i) that e-mail address has been in direct contact with a known terrorist e-mail address or is linked to such an address through one intermediary. [REDACTED]

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

Second, the Government will follow strict procedures ensuring the limited use of the archived data and protecting U.S. person information. These procedures will include ensuring that a record is made of every search of the archive created from the collected data, that a comprehensive auditing mechanism is in place to permit tracking of every keystroke used to access the archive, that the collected data will only be searchable by analysts and software

foreign power or to an individual otherwise engaged in international terrorism; also supporting the PATRIOT Act's further reduction of that standard, so as to "require only a showing of relevance to a criminal investigation"); cf. *In re United States*, 846 F. Supp. 1555, 1560 (M.D. Fla. 1994) (noting that, in the law-enforcement context, the pen register statute "contains no requirement for a finding of 'probable cause,' 'reasonable suspicion,' or the like"). The Fourth Amendment requires a "reasonable articulable suspicion" to justify a minimally intrusive *Terry* stop. Here, no Fourth Amendment interests are even implicated. (U)

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

algorithms for a period of 18 months, and that appropriate minimization procedures are in place to protect U.S. person information. DIRNSA Decl. ¶¶ 23, 25, 27. In particular, the NSA will use the USSID 18 (Attorney General approved) procedures to minimize the information reported concerning U.S. persons. *Id.* ¶ 29. In this regard, the procedures the Government proposes to use are more exacting than is even 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 e-mail meta data. ~~(S)~~

II. To Avoid Grave Constitutional Questions, the Court Should Construe FISA To Authorize the Pen Registers and Trap and Trace Devices the Government Seeks.
~~(S)~~

Even if the analysis above did not make it clear that FISA permits the collection the Government seeks, under the canon of constitutional avoidance, any doubt should be resolved in favor of construing the statute to authorize the collection described in the Application. It is a settled canon of construction that "where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Edward J. DeBartolo*

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

Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council, 485 U.S. 568, 575 (1988); *see also* *Crowell v. Benson*, 285 U.S. 22, 62 (1932) ("When the validity of an act of the Congress is drawn in question, and even if a serious doubt of constitutionality is raised, it is a cardinal principle that this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided."); *Public Citizen v. Dep't of Justice*, 491 U.S. 440, 466 (1989) ("[W]e are loath to conclude that Congress intended to press ahead into dangerous constitutional thickets in the absence of firm evidence that it courted those perils."); *Ashwander v. TVA*, 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). The canon of constitutional avoidance is particularly important in areas of national security and foreign affairs. *See Dep't of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988) (explaining that presidential authority to protect classified information flows directly from a "constitutional investment of power in the President" and that as a result "unless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs"); *see also Dames & Moore v. Regan*, 453 U.S. 654, 660-61 (1981) (emphasizing necessity of adjudicating a matter involving President's foreign affairs powers "on the narrowest possible ground capable of deciding the case") (citing *Ashwander*, 297 U.S. at 347 (Brandeis, J., concurring)). Here, construing FISA to preclude the signals intelligence activities that the Executive Branch has concluded are vital to wartime defense of the Nation would raise a grave constitutional question about whether the statute, as so construed, impermissibly impinges on the President's constitutionally assigned authorities as Commander in Chief and Chief Executive.

~~(S)~~

The Constitution vests power in the President as Commander in Chief of the armed forces, *see* U.S. Const. art. II, § 2, and, by making him Chief Executive, provides him with

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

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

authority over the conduct of the Nation's foreign affairs. See *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) ("[T]he President is the sole organ of the Nation in its external relations, and its sole representative with foreign nations.") (internal quotation marks and citations omitted). These sources of authority grant the President inherent power to protect the security of the Nation from foreign attack, see *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863) (noting that the President is "bound to resist force by force"), and to collect intelligence, see *Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948) ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports neither are nor ought to be published to the world."); *Curtiss-Wright*, 299 U.S. at 320 (The President "has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials."); *United States v. Marchetti*, 466 F.2d 1309, 1315 (4th Cir. 1972) ("Gathering intelligence information" is "within the President's constitutional responsibility for the security of the Nation as the Chief Executive and as Commander in Chief of our Armed forces."); *United States v. Truong Dinh Hung*, 629 F.2d 908, 914 (4th Cir. 1980) (noting the "principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance"). Indeed, as the Foreign Intelligence Surveillance Court of Review recently noted, every court to address the question has concluded that the President has inherent constitutional authority to conduct surveillance for foreign intelligence purposes without a warrant. *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. Rev. 2002). (U)

Given these inherent constitutional powers of the President, it has long been clear that, even in a non-wartime context, FISA's regulation of the Executive's authority to gather foreign intelligence presses against an uncertain constitutional boundary between the powers of the

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

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

Executive and Legislative Branches. Indeed, the legislative history of FISA makes it plain that Congress well recognized that, even in a non-war setting, FISA reached to the limits of congressional power. As Senator McClellan stated, "under any reasonable reading of the relevant court decisions, this bill approaches the outside limits of our Constitutional power to prescribe restrictions on and judicial participation in the President's responsibility to protect this country from threats from abroad, whether it be by electronic surveillance or other lawful means." *Foreign Intelligence Surveillance Act of 1976: Hearing Before the Subcomm. on Crim. Laws and Procs. of the Senate Comm. on the Judiciary*, 94th Cong. 2 (1976). The Conference Report even took the unusual step of expressly acknowledging the limits of Congress's ability to restrict the authority of the President: "the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court." H.R. Conf. Rep. No. 95-1720, at 35, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064. The Report thus effectively acknowledged that congressional power over the Executive's inherent authority to conduct foreign intelligence surveillance—even in a non-war context—was sufficiently open to doubt that the statute might be struck down. (U)


"Taking for granted" that the President does have "inherent authority to conduct warrantless searches to obtain foreign intelligence information," the Foreign Intelligence Surveillance Court of Review recently concluded that, "assuming that is so, FISA could not encroach on the President's constitutional power." *In re Sealed Case*, 310 F.3d at 742. Under that analysis, to conclude in this instance that FISA does not authorize the collection of meta data requested in the Application, and thus prohibits altogether the intelligence collection that the Executive has deemed vital, would clearly raise grave constitutional questions. ~~(TS//SI//NF)~~

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

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

The constitutional issue that would be raised by such a construction is particularly grave here, moreover, because of the wartime context in which the question arises. This case does not involve run-of-the-mill foreign intelligence collection, but rather intelligence collection determined by the Executive to be vital for defending the Nation from attack in the midst of a war—precisely the circumstances in which the President’s powers as Commander in Chief are at their height. As the Supreme Court has emphasized, when the Nation is attacked, the President is “bound to resist force by force,” and “[h]e must determine what degree of force the crisis demands.” *Prize Cases*, 67 U.S. (2 Black) at 668, 670.³⁴ Thus, in employing the armed forces to defend the Nation, the “President alone” is “constitutionally invested with the entire charge of hostile operations.” *Hamilton v. Dillin*, 88 U.S. (21 Wall.) 73, 87 (1874); *see also United States v. Sweeny*, 157 U.S. 281, 284 (1895) (“[T]he object of the [Commander-in-Chief Clause] is evidently to vest in the President . . . such supreme *and undivided* command as would be necessary to the prosecution of a successful war.”) (emphasis added). (U)

That authority as Commander in Chief includes, in particular, the authority to gather intelligence (and, in particular, enemy communications) for successful prosecution of the war. As early as the Civil War, for example, the “advantages of intercepting military telegraphic communications were not long overlooked. [Confederate] General Jeb Stuart actually had his own personal wiretapper travel along with him in the field.” Samuel Dash et al., *The Eavesdroppers* 23 (1971). And during World War I and World War II, Presidents Wilson and Roosevelt engaged in efforts to intercept or obstruct the enemy’s electronic communications sent to or from the United States. *See supra* p. _____. As courts have long recognized, “[i]t is



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

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

impossible for a government wisely to make critical decisions about . . . national defense without the benefit of dependable foreign intelligence." *Snepp v. United States*, 444 U.S. 507, 512 n.7 (1980) (per curiam); *see also Totten v. United States*, 92 U.S. 105, 106 (1876) (recognizing the President's power to use spies to "obtain information respecting the strength, resources, and movements of the enemy"); *cf. Johnson v. Eisentrager*, 339 U.S. 763, 788 (1950) ("The first of the enumerated powers of the President is that he shall be Commander-in-Chief of the Army and Navy of the United States. And, of course, grant of war power includes all that is necessary and proper for carrying these powers into execution.") (citation omitted). As the Supreme Court has explained:

When force is employed it should be intelligently directed, and this depends upon having reliable information—in time. As Chief Justice John Marshall said of Washington, "A general must be governed by his intelligence and must regulate his measures by his information. It is his duty to obtain correct information . . ." So we take it as undeniable that the military, *i.e.*, the Army, need a certain amount of information in order to perform their constitutional and statutory missions.

Laird v. Tatum, 408 U.S. 1, 5-6 (1972). (U)

Because reading the statute to preclude the acquisition of the bulk e-mail meta data described in the Application would raise a grave constitutional question about whether the statute impermissibly impinges on the President's authority as Commander in Chief, and in particular his responsibility to defend the Nation by thwarting further attacks, *see Haig v. Agee*, 453 U.S. 280, 307 (1981); *Prize Cases*, 67 U.S. (2 Black) at 668, this Court should interpret section 402 to authorize the collection the Government has requested. *Cf. Dames & Moore*, 453 U.S. at 678-82 (even where there is no express congressional authorization, legislation in related field may be construed to indicate congressional acquiescence in executive action in the field of foreign affairs). Such an interpretation is more than "fairly possible." *Crowell v. Benson*, 285 U.S. at 62. The critical term in the statute is "relevant," which is a term that is both elastic and context-

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

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

sensitive. In other contexts, courts have applied the canon of avoidance to avoid infringements on Executive power even without a clear textual hook for interpretation. *See, e.g., Public Citizen v. Dep't of Justice*, 491 U.S. at 452-53, 463-64 (rejecting a "straightforward reading" or "literalistic reading" to conclude that a committee that is "used" by the Justice Department is not "utilized" by it); *see also Ass'n of Am. Physicians & Surgeons v. Clinton*, 997 F.2d 898, 906 (D.C. Cir. 1993) (describing the decision in *Public Citizen* as adopting "an extremely strained construction . . . to avoid the constitutional question"). Here, by contrast, reading the term "relevant" to permit the collection of this critical information during wartime is a construction rooted in the text that requires no stretching of the ordinary meaning of the terms of the statute at all. In fact, for all the reasons outlined above, interpreting section 402 to authorize the collection the Government has requested is the best reading of the plain terms of the Act. The Government's proposed collection squarely fits the definitions of pen registers and trap and trace devices. In addition, the Government has certified that "the information likely to be obtained" is "relevant to an ongoing investigation to protect against international terrorism," and the Court has no discretion to look behind that certification. 50 U.S.C. § 1842(c). Even if the Court did have such discretion, the information sought is clearly relevant to the ongoing investigation to protect against further attacks [REDACTED] (TS//SI//NF)

Finally, application of the canon of constitutional avoidance is particularly warranted here given the unique circumstances of the case. In almost all cases of potential constitutional conflict, if a statute is construed to restrict the Executive, the Executive has the option of seeking additional clarifying legislation from Congress. In this case, by contrast, the Government cannot pursue that route because seeking legislation would inevitably compromise the secrecy of the collection program the Government wishes to undertake. That dilemma, potentially crippling for

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

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

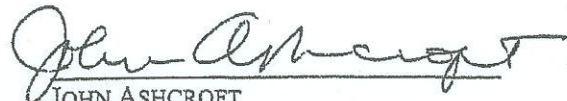
intelligence gathering in the midst of a war, can readily be avoided by applying standard canons to read the statute to permit the Court to grant the attached Application. ~~(S)~~

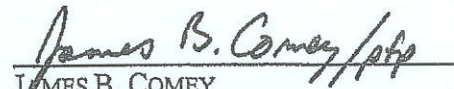
CONCLUSION (U)

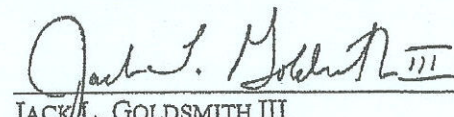
For the foregoing reasons, the Court should approve the Application. (U)

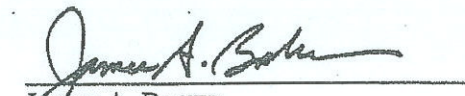
Respectfully submitted,

Dated: [REDACTED]


JOHN ASHCROFT
Attorney General


JAMES B. COMEY
Deputy Attorney General


JACK L. GOLDSMITH III
Assistant Attorney General,
Office of Legal Counsel


JAMES A. BAKER
Counsel for Intelligence Policy

PATRICK F. PHILBIN
Associate Deputy Attorney General

[REDACTED]
Attorney-Advisers,
Office of Legal Counsel

U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

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