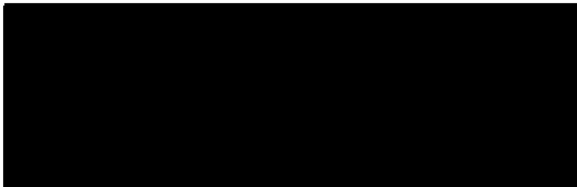


~~TOP SECRET//HCS//SI//NOFORN~~

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



(S)

Docket Number: BR:

06 - 05

EXHIBIT C

MEMORANDUM OF LAW IN SUPPORT OF APPLICATION FOR
CERTAIN TANGIBLE THINGS FOR INVESTIGATIONS TO PROTECT
AGAINST INTERNATIONAL TERRORISM

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

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

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

INTRODUCTION (U)

One of the greatest challenges the United States faces in the ongoing conflict with [REDACTED] is finding operatives of the enemy. As this Court is aware, one of the most significant tools that the U.S. Government can use to accomplish that task is metadata analysis. Under this Court's order in [REDACTED] Opinion and Order, No. PR/TT [REDACTED] ("[REDACTED]"), and subsequent related authorizations, the National Security Agency (NSA) is currently collecting metadata in bulk from electronic communications and applying sophisticated analytic tools to identify and find [REDACTED] operatives. The attached Application seeks this Court's authorization to collect in bulk from the [REDACTED] certain business records—call detail records, or “telephony metadata”—so that the NSA may use these same analytic tools to identify and find operatives of [REDACTED] (TS//SI//NF)

The attached Application for business records is made pursuant to title V of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1861 et seq., as amended, “Access to Certain Business Records for Foreign Intelligence Purposes,” to capitalize upon the unique opportunities the United States has for identifying communications of [REDACTED]. The collection sought here will make possible a potentially powerful tool that the Government has to discover enemy communications: metadata analysis. For telephone calls, metadata essentially consists of routing information that includes the telephone number of the calling party, the telephone number of the called party, and the date, time and duration of the call. It does not include the substantive content of the communication or the name, address, or financial information of a subscriber or customer. Relying solely on such metadata, the Government can analyze the contacts made by a telephone number reasonably suspected to be associated with a terrorist, and

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

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

thereby possibly identify other, previously unknown, terrorists. The primary advantage of metadata analysis as applied to telephony metadata is that it enables the Government to analyze past connections and patterns of communication. That analysis is possible, however, only if the Government has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related. In addition, individually targeted collection of metadata is inadequate for tracking the communications of terrorists [REDACTED]

[REDACTED]

[REDACTED]

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

In the attached Application, therefore, the Government requests that this Court order the production, in bulk and on an ongoing basis, of certain business records of the [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The Application fully satisfies all requirements of title V of FISA. In particular, the Application seeks the production of tangible things "for" an international terrorism investigation. 50 U.S.C. § 1861(a)(1). In addition, the Application includes a statement of facts demonstrating that there are reasonable grounds to believe that the business records sought are "relevant" to an authorized investigation. *Id.* § 1861(b)(2). Although the call detail records of the [REDACTED] [REDACTED] contain large volumes of metadata, the vast majority of which will not be terrorist-related, the scope of the business records request presents no infirmity under title V. All of the business records to be collected here are relevant to FBI investigations into [REDACTED] because the NSA can effectively conduct metadata analysis only if it has the data in bulk. (TS//SI//NF)

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

In addition, even if the metadata from non-terrorist communications were deemed not relevant, nothing in title V of FISA demands that a request for the production of "any tangible things" under that provision collect *only* information that is strictly relevant to the international terrorism investigation at hand. Were the Court to require some tailoring to fit the information that will actually be terrorist-related, the business records request detailed 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. As the Supreme Court has held, there is no constitutionally protected interest in metadata, such as numbers dialed on a telephone. Any intrusion is further reduced because only data connected to telephone numbers reasonably suspected to be terrorist-associated will ever be viewed by any human being. Indeed, only a tiny fraction (estimated by the NSA to be 0.000025% or one in four million) of the call detail records collected actually will be seen by a trained NSA analyst. Under the procedures the Government will apply, metadata reflecting the activity of a particular telephone number will only be seen by a human analyst if a computer search has established a connection to a terrorist-associated telephone number. ~~(TS//SI//NF)~~

The Application is completely consistent with this Court's ground breaking and innovative decision in [REDACTED] In that case, the Court authorized the installation and use of pen registers and trap and trace devices to collect bulk e-mail metadata from the [REDACTED]

[REDACTED] The Court found that all of "the information likely to be

obtained” from such collection “is relevant to an ongoing investigation to protect against international terrorism.” 50 U.S.C. § 1842(c)(2); [REDACTED] at 25-54. The Court explained that “the bulk collection of meta data—i.e., the collection of both a huge volume and high percentage of unrelated communications—is necessary to identify the much smaller number of [REDACTED] communications.” *Id.* at 49. Moreover, as was the case in [REDACTED] this Application 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)

BACKGROUND (U)

A. The Al Qaeda Threat (S)

On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation’s financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation’s Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a direct blow at the leadership of the Government of the United States. The attacks of September 11th resulted in approximately 3,000 deaths—the highest single-day death toll from hostile foreign attacks in the Nation’s history. These attacks shut down air travel in the United States,

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

disrupted the Nation's financial markets and government operations, and caused billions of dollars in damage to the economy. (U)

Before the September 11th attacks, al Qaeda had promised to attack the United States. In 1998, Osama bin Laden declared a "religious" war against the United States and urged that it was the moral obligation of all Muslims to kill U.S. civilians and military personnel. See Statement of Osama bin Laden, Ayman al-Zawahiri, et al., *Fatwah Urging Jihad Against Americans*, published in Al-Quds al-'Arabi (Feb. 23, 1998) ("To kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it, in order to liberate the al-Aqsa Mosque and the holy mosque from their grip, and in order for their armies to move out of all the lands of Islam, defeated and unable to threaten any Muslim."). Al Qaeda carried out those threats with a vengeance; they attacked the U.S.S. Cole in Yemen, the United States Embassy in Nairobi, and finally the United States itself in the September 11th attacks. (U)

It is clear that al Qaeda is not content with the damage it wrought on September 11th. Just a few months ago, Osama bin Laden pointed to "the explosions that . . . have take[n] place in the greatest European capitals" as evidence that "the mujahideen . . . have been able to break through all the security measures taken by" the United States and its allies. Osama bin Laden, audiotape released on Al-Jazeera television network (Federal Bureau of Investigation trans., Jan. 19, 2006). He warned that "the delay of [sic] inflicting similar operations in America has not been due to any impossibility of breaking through your security measures[,] for those operations are underway and you will see them in your midst as soon as they are done." *Id.* Several days later, bin Laden's deputy, Ayman al-Zawahiri, warned that the American people are destined for "a future colored by blood, the smoke of explosions and the shadows of terror." Ayman al-

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

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

Zawahiri, videotape released on the Al-Jazeera television network (Jan. 30, 2006). These recent threats were just the latest in a series of warnings since September 11th by al Qaeda leaders who have repeatedly promised to deliver another, even more devastating attack on America. *See, e.g.,* Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 24, 2004) (warning United States citizens of further attacks and asserting that "your security is in your own hands"); Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 18, 2003) ("We, God willing, will continue to fight you and will continue martyrdom operations inside and outside the United States . . ."); Ayman al-Zawahiri, videotape released on the Al-Jazeera television network (Oct. 9, 2002) ("I promise you [addressing the 'citizens of the United States'] that the Islamic youth are preparing for you what will fill your hearts with horror"). As recently as December 7, 2005, al-Zawahiri professed that al Qaeda "is spreading, growing, and becoming stronger," and that al Qaeda is "waging a great historic battle in Iraq, Afghanistan, Palestine, and even in the Crusaders' own homes." Ayman al-Zawahiri, videotape released on Al-Jazeera television network (Dec. 7, 2005). Indeed, since September 11th, al Qaeda has staged several large-scale attacks around the world, including in Tunisia, Kenya and Indonesia, killing hundreds of innocent people. In addition, Ayman al-Zawahiri claimed that al Qaeda played some role in the July 2005 attacks on London. *See* Declaration of John S. Redd, Director, National Counterterrorism Center ¶ 35 (May 22, 2006) (Exhibit B to the Application) ("NCTC Declaration"). Given that al Qaeda's leaders have repeatedly made good on their threats and that al Qaeda has demonstrated its ability to insert foreign agents into the United States to execute attacks, it is clear that the threat continues. ~~(TS//SI//NF)~~

Reliable intelligence indicates that [REDACTED] remains intent on striking the United States and U.S. interests. *See* NCTC Declaration ¶¶ 5-7, 8, 11-13. [REDACTED] is an international

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

organization with a global presence, with members located in at least 40 countries, and the capability to strike US interests anywhere in the world." *Id.* ¶ 5. Indeed, [REDACTED] continues its efforts to reconstitute communication links to a transnational network of [REDACTED] personnel and affiliated groups." *Id.* ¶ 39. Recent intelligence suggests that [REDACTED] has become "keenly" interested in soft targets, especially those that are densely populated. *Id.* ¶¶ 17, 75. [REDACTED] and its affiliates consistently have expressed an interest in attacking U.S. rail and mass transit systems, as well as continuing to target the civil aviation sector, including U.S. passengers and Western aircraft overseas. *Id.* ¶¶ 74-80. Moreover, the Intelligence Community is concerned that the next [REDACTED] attack in the United States might use chemical, biological, radiological or nuclear weapons, "especially given [REDACTED] clear intent to develop such capabilities and use them to strike the Homeland." *Id.* ¶ 81. In sum, [REDACTED] continues to present "a credible threat for a massive attack against the US Homeland." *Id.* ¶ 91. By helping to find and identify members and agents of [REDACTED], particularly those who are already within the United States, the proposed request for business records would greatly help the United States prevent another such catastrophic terrorist attack, one that [REDACTED] itself has claimed would be larger than the attacks of September 11th. (TS//SI//HCS//OC,NF)

B. [REDACTED] Use of Telephones to Communicate (S)

[REDACTED] use the international telephone system to communicate with one another between numerous countries all over the world, including to and from the United States. In addition, when they are located inside the United States, [REDACTED] operatives make domestic U.S. telephone calls. For purposes of preventing terrorist attacks against the United States, the most analytically significant [REDACTED] telephone communications are those that either have one end in the United States or that are purely domestic, because those

communications are particularly likely to identify individuals who are associated with [REDACTED] in the United States whose activities may include planning attacks on the homeland. See Declaration of Lieut. Gen. Keith B. Alexander, U.S. Army, Director, NSA, ¶ 5 (May 22, 2006) (Exhibit A to the Application) ("NSA Declaration"). The vast majority of the call detail records sought in the attached Application would include records of telephone calls that either have one end in the United States or are purely domestic, including local calls, although some records would relate to communications in which both ends were outside the United States. The United States needs to sort through this telephony metadata to find and identify [REDACTED] and thereby acquire vital intelligence that could prevent another deadly terrorist attack. (TS//SI//NF)

C. *Discovering the Enemy: Metadata Analysis* (TS//SI//NF)

Analyzing metadata from international and domestic telecommunications—such as information showing which telephone numbers have been in contact with which other telephone numbers, for how long, and when¹—can be a powerful tool for discovering communications of terrorist operatives. Collecting and archiving metadata is thus the best avenue for solving the following fundamental problem: although investigators do not know *exactly* where the terrorists' communications are hiding in the billions of telephone calls 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. NSA Declaration ¶¶ 7-11. As the NSA has explained, "[t]he ability to accumulate a metadata archive and set it aside for carefully controlled

¹ For telephone calls, "metadata" includes comprehensive communications routing information, including the telephone number of the calling party, the telephone number of the called party, and the date, time and duration of the call, as well as communications device and trunk identifiers. A "trunk" is a communication line between two switching systems. *Newton's Telecom Dictionary* 853 (20th ed. 2004). Telephony metadata does not include the content of the communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer. (S)

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

searches and analysis will substantially increase NSA's ability to detect and identify members of al Qaeda and its affiliates." *Id.* ¶ 8; see also [REDACTED] at 43-45. (TS//SI//NF)

Collecting and archiving metadata offers at least two invaluable capabilities to analysts that are unavailable from any other approach. First, it allows for retrospective "contact chaining." For example, analysts may learn that a particular telephone number is associated with [REDACTED] perhaps because it was found in the cell phone directory of a recently captured [REDACTED] agent. By examining metadata that has been archived over a period of time, analysts can search to find the contacts that have been made by that "seed" telephone number. The ability to see who communicates with whom may lead to the discovery of other terrorist operatives, may help to identify hubs or common contacts between targets of interest who were previously thought to be unconnected, and may help to discover individuals willing to become FBI assets. Indeed, computer algorithms can identify not only the first tier of contacts made by the telephone number reasonably suspected to be associated with [REDACTED] but also the further contacts made by the first and second tiers of telephone numbers. NSA Declaration ¶ 9. Going out beyond the first tier enhances the ability of analysts to find terrorist connections by increasing the chances that they will find previously unknown terrorists. A seed telephone number, for example, may be in touch with several telephone numbers previously unknown to analysts. Following the contact chain out two additional "hops" to examine the contacts made by the first two tiers of telephone numbers may reveal a contact that connects back to a different terrorist-associated telephone number already known to the analyst. Going out to the third tier is useful for telephony because, unlike e-mail traffic, which includes the heavy use of "spam," a telephonic device does not lend itself to simultaneous contact with large numbers of individuals.

(TS//SI//NF)

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

The capabilities offered by such searching of a collected archive of metadata are vastly more powerful than chaining that could be performed on data collected pursuant to national security letters issued by the Government under 18 U.S.C. § 2709 and targeted at individual telephone numbers. If investigators find a new telephone number when an [REDACTED] is captured, and the Government issues a national security letter for the local and long distance toll billing records for that particular account, it would only be able to obtain the first tier of telephone numbers that the [REDACTED] number has been in touch with. To find an additional tier of contacts, new national security letters would have to be issued for each telephone number identified in the first tier. The time it would take to issue the new national security letters would necessarily mean losing valuable data. And the data loss in the most critical cases would only be increased by terrorists' propensity [REDACTED]. Moreover, because telephone companies generally only keep call detail records in an easily accessible medium for up to two years, historical chaining analysis on the number may lead analysts to other individuals [REDACTED] by revealing the contacts that were made by a terrorist-associated telephone number more than two years ago. See NSA Declaration ¶ 12. (TS//SI//NF)

The second major tool analysts can use with an archive of collected metadata is [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Skilled analysts can then use a
[REDACTED] to determine whether there is another
telephone number within the archived metadata that shows a [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] Obviously, such [REDACTED] is a critical tool for

keeping up with terrorists [REDACTED] See NSA

Declaration ¶ 11. It provides an invaluable capability that could not be reproduced through any other mechanism [REDACTED]

[REDACTED] Such analysis can be performed only if the Government has collected and archived the data [REDACTED]

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

E. The Foreign Intelligence Surveillance Act (U)

FISA provides a mechanism for the Government to obtain business records—here, call detail records—[REDACTED] containing precisely the type of communications data that is vital for the metadata analysis described above—including the telephone number of the calling party, the telephone number of the called party, and the date, time and duration of the call. Section 501 of FISA, as recently amended by section 106 of the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192, 196-200 (Mar. 9, 2006) (“USA PATRIOT Reauthorization Act”), authorizes the Director of the FBI or his designee to apply to this Court

for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an 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 on the basis of activities protected by the First Amendment to the Constitution.

50 U.S.C. § 1861(a)(1).² ~~(S)~~

² The call detail records sought in the attached Application would not be collected by a “pen register” or “trap and trace device” as defined by 18 U.S.C. § 3127. Each of these terms refers to a “device or process” which either “records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted”—a pen register, *id.* § 3127(3), or “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”—a trap and trace device, *id.* § 3127(4). As the definitions make clear, pen registers and trap and

LEGAL ANALYSIS (U)

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

Section 501(c)(1) of FISA, as amended, directs the Court to enter an ex parte order requiring the production of tangible things if the judge finds that the Government's application meets the requirements of subsections 501(a) and (b). The most significant of those requirements are that the tangible things, which include business records, are "for" an investigation to protect against international terrorism. 50 U.S.C. § 1861(a)(1). Section 501(b)(2)(A) indicates that this requirement is one of relevance, providing that the Government's application must include

a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) [*i.e.*, following Attorney General-approved Executive Order 12333 guidelines and not conducted of a U.S. person solely on the basis of First Amendment-protected activities] to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of facts that they pertain to—(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.

Id. § 1861(b)(2)(A).³ (U)

trace devices are mechanical "device[s]," or perhaps software programs ("process[es]"), that "record" or "decode" data as communications signals are passing through the particular spot in the communications network where the "device" or "process" has been installed, or that "capture" data in a similar fashion. *See, e.g., United States Telecom Ass'n v. FBI*, 276 F.3d 620, 623 (D.C. Cir. 2002) ("Pen registers are devices that record the telephone numbers dialed by the surveillance's subject; trap and trace devices record the telephone numbers of the subject's incoming calls."). The mechanism by which the NSA would receive call detail records does not involve any such "device or process." Instead, [REDACTED] would copy and transmit the call detail records, [REDACTED] independently compile in their normal course of business, to the NSA in real or near-real time. (TS//SI//NF)

³ Until recently, section 501(b)(2) provided only that the Government's application "specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2) (Supp. I 2001). According to the legislative history of the USA PATRIOT Reauthorization Act, the provision was amended "to clarify that the

Thus, section 501(b)(2) of FISA requires that an application for an order requiring the production of business records must include a statement of facts showing that there are "reasonable grounds to believe" that certain criteria are met: (1) that the business records are relevant to an authorized investigation, other than a threat assessment, that is being conducted, for example, to protect against international terrorism; (2) that the investigation is being conducted under guidelines approved by the Attorney General under Executive Order 12333; and (3) that the investigation is not being conducted of a U.S. person solely upon the basis of activities protected by the First Amendment. *Id.* § 1861(b)(2)(A). All of these criteria are met here. (U)

Taking the last two requirements first, the attached Application establishes that the business records sought are for FBI investigations into [REDACTED] [REDACTED] at home and abroad," investigations which are being conducted under Attorney General-approved 12333 guidelines and that are not being conducted of any U.S. persons solely upon the basis of First Amendment-protected activities. In addition, the attached Application and accompanying declarations by the Directors of the NSA and National Counterterrorism Center certainly demonstrate that there are "reasonable grounds to believe" that the business records sought are "relevant" to authorized investigations to protect against international terrorism. (S)

A. The Business Records Sought Meet the Relevance Standard. (U)

Information is "relevant" to an authorized 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

tangible things sought by [an order under section 501] must be 'relevant' to an authorized preliminary or full investigation . . . to protect against international terrorism." H.R. Conf. Rep. No. 109-333, at 90 (2005). (U)

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

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). Indeed, section 501(b)(2) establishes a presumption that the Government has satisfied the relevancy requirement if it shows that the business records sought "pertain to—(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation." 50 U.S.C. § 1861(b)(2)(A). The USA PATRIOT Reauthorization Act added this presumption to section 501(b) to outline certain situations in which the Government automatically can establish relevance; the presumption was not intended to change the relevance standard for obtaining business records under section 501. *See* Pub. L. No. 109-177, § 106, 120 Stat. 196; H.R. Conf. Rep. No. 109-333, at 91 (Section 501(b)(2) "also requires a statement of facts to be included in the application that shows there are reasonable grounds to believe the tangible things sought are relevant, and, if such facts show reasonable grounds to believe that certain specified connections to a foreign power or an agent of a foreign power are present, the tangible things sought are presumptively relevant. *Congress does not intend to prevent the FBI from obtaining tangible things that it currently can obtain under section [501].*") (emphasis added). (U)

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

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

The FBI currently has over 1,000 open National Security Investigations targeting [REDACTED]

As we have explained above, the bulk telephony metadata sought in the attached Application is relevant to the FBI's investigations into [REDACTED] because, when acquired, stored, and processed, the telephony metadata would provide vital assistance to investigators in tracking down [REDACTED] operatives. Although admittedly a substantial portion of the telephony metadata that is collected would not relate to operatives of [REDACTED]⁴ the intelligence tool that the Government hopes to use to find [REDACTED] communications—metadata analysis—requires collecting and storing large volumes of the metadata to enable later analysis. All of the metadata collected is thus relevant, because the success of this investigative tool depends on bulk collection. (TS//SI//NF)

Archiving and analyzing the metadata sought in the attached Application will assist the FBI in obtaining foreign intelligence and, in particular, in identifying the telephone numbers of [REDACTED] operating within the United States. For example, contact chaining and [REDACTED] of the archived information will allow the NSA to identify telephone numbers that have been in contact with telephone numbers the NSA reasonably suspects to be linked to [REDACTED] and its affiliates. NSA may provide such information to the FBI, which can determine whether an investigation should be commenced to identify the users of the telephone numbers and to determine whether there are any links to international terrorist activities. The NSA estimates that roughly 800 telephone numbers will be tipped annually to the FBI, CIA, or other appropriate U.S. government or foreign government agencies. NSA Declaration ¶ 18. The FBI would also

⁴ The NSA expects that this business records request, over the course of a year, will result in the collection of metadata pertaining to [REDACTED] communications. See NSA Declaration ¶ 6. (TS//SI//NF)

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

be able to ask the NSA to perform contact chaining [REDACTED] on terrorist-associated telephone numbers known to the FBI. (TS//SI//NF)

The call detail records sought in the attached Application are certainly "relevant" to an authorized investigation in [REDACTED]

[REDACTED] As this Court recently noted in [REDACTED] the requirement of relevance is a relatively low standard. [REDACTED] at 29. In that case, the Court was interpreting a similar, and quite possibly more stringent standard than that presented here. There, the Court found that section 402(a) of FISA was satisfied, i.e., that "the information likely to be obtained is . . . relevant to an ongoing investigation to protect against international terrorism." 50 U.S.C. § 1842(c) (emphasis added).⁵ Here, by contrast, the Application need only establish that there are "reasonable grounds to believe" that the records sought are relevant to an authorized international terrorism investigation.⁶ *Id.* § 1861(b)(2)(A). (TS//SI//NF)

In evaluating whether metadata collected in bulk is "relevant" to investigations into [REDACTED] this Court has recognized that, "for reasons of both constitutional authority and practical competence, deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats and in

⁵ Although the Government argued that the statute did not permit the Court to look behind the Government's certification of relevance, the Court assumed for purposes of the case that it should consider the basis for the certification. [REDACTED] at 26-28. (TS//SI//NF)

⁶ The "reasonable grounds to believe" standard is simply a different way of articulating the probable cause standard. See *Maryland v. Pringle*, 540 U.S. at 371 (quoting *Brinegar v. United States*, 338 U.S. 160, 175 (1949) ("The substance of all the definitions of probable cause is a reasonable ground for belief of guilt")). As the Supreme Court has recently explained, "[t]he probable-cause standard is incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances." *Maryland v. Pringle*, 540 U.S. 366, 371 (2003). Rather than being "technical," these probabilities "are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Brinegar*, 338 U.S. at 176; see also *Pringle*, 540 U.S. at 370 (quoting *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (quoting *Brinegar*)). In addition, probable cause "does not require the fine resolution of conflicting evidence that a reasonable-doubt or even a preponderance standard demands." *Gerstein v. Pugh*, 420 U.S. 103, 121 (1975); see also *Illinois v. Gates*, 462 U.S. 213, 235 (1983) ("Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the [probable cause] decision."). (U)

determining the potential significance of intelligence-related information. Such deference is particularly appropriate in this context, where the Court is not charged with making independent probable cause findings.” [REDACTED] at 30-31. In [REDACTED] this Court noted that the proposed activity would result in the collection of metadata pertaining to [REDACTED] or electronic communications, all but a very small fraction of which could be expected to be unrelated to [REDACTED] and its affiliates. *Id.* at 39-40, 48. Nonetheless, this Court found that the bulk collection of metadata “is necessary to identify the much smaller number of [REDACTED] communications” and that therefore, “the scope of the proposed collection is consistent with the certification of relevance.” *Id.* at 48-49. In part that was because the NSA had explained, as it does here, that “more precisely targeted forms of collection against known accounts would tend to screen out the ‘unknowns’ that NSA wants discover, so that NSA needs bulk collection in order to identify unknown [REDACTED]” *Id.* at 42. Just as the bulk collection of e-mail metadata was relevant to FBI investigations into [REDACTED] so is the bulk collection of telephony metadata described herein. (~~TS//SI//NF~~)

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

Title V of FISA does not expressly impose any requirement to tailor a request for tangible things precisely to obtain solely records that are strictly relevant to the investigation. To the extent, however, the Court construes the “relevance” standard under Title V to require some tailoring of the requested materials to limit overbreadth, the request for tangible things proposed here is not overbroad. As this Court concluded in [REDACTED] “the applicable relevance standard does not require a statistical ‘tight fit’ between the volume of proposed collection and the much smaller proportion of information that will be directly relevant to [REDACTED]”

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

investigations.”⁷ *Id.* at 49-50. Instead, it is appropriate to use as a guideline the Supreme Court’s “special needs” jurisprudence, which balances any intrusion into privacy against the government interest at stake to determine whether a warrant or individualized suspicion is required. *See Board of Educ. v. Earls*, 536 U.S. 822, 829 (2002); *see generally* [REDACTED] at 50-52.⁸ Here, the Government’s interest is overwhelming. It involves thwarting terrorist attacks that could take thousands of lives. “This concern clearly involves national security interests beyond the normal need for law enforcement and is at least as compelling as other governmental interests that have been held to justify searches in the absence of individualized suspicion.” [REDACTED] at 51-52; *see also Haig v. Agee*, 453 U.S. 280, 307 (1981) (“It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.”) (internal quotation marks omitted). The privacy interest, on the other hand, is minimal. As we explain below, *see infra* § II, the type of data at issue is not constitutionally protected; and it would never even be *seen* by any human being unless a terrorist connection were first established. Indeed, only a tiny fraction (estimated to be 0.000025% or one in four million) of the call detail records included in the archive actually would be seen by a trained analyst.⁹

(TS//SI//NF)

⁷ As noted above, the relevance standard being interpreted in the pen register context in [REDACTED] that found in section 402 of FISA—is quite possibly more stringent than that required to be met by an application for business records under section 501 of FISA. (S)

⁸ Because, as we explain below, there is no Fourth Amendment-protected interest in the telephony metadata at issue here, the actual *standards* applied under Fourth Amendment balancing are far more rigorous than any that the Court should read into the statutory requirement that the business records sought under section 501 be “relevant” to an international terrorism investigation. 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)

⁹ The NSA would conduct contact chaining three “hops” out, i.e., to include the first three tiers of contacts made by the reasonably suspected [REDACTED] telephone number. Even though a substantial portion of the telephone numbers in those first three tiers of contacts may not be used by terrorist operatives, they are all “connected” to the seed telephone number. (TS//SI//NF)

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

And, as this Court recently found, "the Government need not make a showing that it is using the least intrusive means available. Rather, the question is whether the Government has chosen 'a reasonably effective means of addressing' the need." [REDACTED] at 52-53 (quoting *Earls*, 536 U.S. at 837) (internal citations omitted); see also *Earls*, 536 U.S. 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."). Here, as in [REDACTED] "senior responsible officials, whose judgment on these matters is entitled to deference . . . have articulated why they believe that bulk collection and archiving of meta data are necessary to identify and monitor [REDACTED] whose . . . communications would otherwise go undetected." [REDACTED] at 53-54. Such bulk collection is thus a "reasonably effective means to this end." *Id.* at 54. (TS//SI//NF)

In sum, as this Court previously concluded in the pen register context,

the bulk collection proposed in this case is analogous to suspicionless searches or seizures that have been upheld under the Fourth Amendment in that the Government's need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of detecting and monitoring [REDACTED] and thereby obtaining information likely to be relevant to ongoing FBI investigations. In these circumstances, the certification of relevance is consistent with the fact that only a very small proportion of the huge volume of information collected will be directly relevant to the FBI's [REDACTED] investigations.

Id. (TS//SI//NF)

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

C. The Government Will Apply Strict Minimization Procedures to the Use of the Collected Data. ~~(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 metadata analysis, the use of that information will be strictly tailored to identifying terrorist communications and will occur solely according to strict procedures and safeguards, including particular minimization procedures designed to protect U.S. person information. These procedures and safeguards are almost identical to the requirements imposed by this Court in [REDACTED] which authorized collection of a similar volume of metadata. ~~(TS//SI//NF)~~

First, as described in the attached Declaration from the Director of the NSA, the NSA will query the archived data solely when it has identified a known telephone number 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 telephone number is associated with [REDACTED] provided, however, that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution." NSA Declaration ¶ 13.¹⁰ Similarly, [REDACTED] would be undertaken only with respect to such an identified "seed" telephone number. For example, when an [REDACTED] operative is apprehended, his cellular telephone may contain a phone book listing telephone numbers. Telephone numbers listed in such a phone book would satisfy the "reasonable articulable suspicion" standard. This same

¹⁰ For example, a telephone number of a U.S. person could not be a seed number "if the *only* information thought to support the belief that the [number] is associated with [REDACTED] is that, in sermons or in postings on a web site, the U.S. person espoused jihadist rhetoric that fell short of 'advocacy . . . directed to inciting or producing imminent lawless action and . . . likely to incite or produce such action.' *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam)." [REDACTED] at 58. ~~(TS//SI//NF)~~

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

standard 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").¹¹ It bears emphasis that, given the types of analysis the NSA will perform, no information about a telephone number will ever be accessed by or presented in an intelligible form to any person unless either (i) that telephone number has been in direct contact with a reasonably suspected terrorist-associated telephone number or is linked to such a number through one or two intermediaries, or (ii) a computer search has indicated that the telephone number has the [REDACTED]

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

In addition, any query of the archived data would require approval from one of seven people: the Signals Intelligence Directorate Program Manager for Counterterrorism Special Projects; the Chief or Deputy Chief, Counterterrorism Advanced Analysis Division; or one of four specially authorized Counterterrorism Advanced Analysis Shift Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. NSA Declaration ¶ 19. NSA's Office of General Counsel (OGC) would review and approve proposed queries of archived metadata based on seed accounts reasonably believed to be used by U.S. persons. *Id.* ¶ 16. Finally, NSA's OGC will brief analysts concerning the authorization requested in the Application and the limited circumstances in which queries to the archive are permitted, as well

¹¹ 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 request for business records is that the information be relevant to an international terrorism investigation. The Fourth Amendment requires a "reasonable articulable suspicion" to justify a minimally intrusive *Terry* stop. Here, no Fourth Amendment interests are even implicated. (U)

as other procedures and restrictions regarding the retrieval, storage and dissemination of the archived data. *Id.* (~~TS//SI//NF~~)

Second, NSA will apply several mechanisms to ensure appropriate oversight over the use of the metadata. The NSA will apply the existing (Attorney General approved) guidelines in United States Signals Intelligence Directive 18 (1993) ("USSID 18") (Exhibit D to the Application) to minimize the information reported concerning U.S. persons. NSA Declaration ¶ 17. Prior to disseminating any U.S. person information, the Chief of Information Sharing Services in the Signals Intelligence Directorate 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). The Director of the NSA will direct the NSA Inspector General and General Counsel to submit an initial report to him 45 days after the receipt of records pursuant to the Order assessing the adequacy of the management controls for the processing and dissemination of U.S. person information. NSA Declaration ¶ 22. The Director of the NSA will provide the findings of that report to the Attorney General. *Id.* (~~TS//SI//NF~~)

In addition, every time one of the limited number of NSA analysts permitted to search the archived data carries out such a search, a record will be made, and 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. NSA Declaration ¶ 16. The NSA's OGC will monitor both the designation of individuals with access to the archived data and the functioning of this automatic logging

capability. *Id.* The NSA Inspector General, the NSA General Counsel, and the Signals Intelligence Directorate Oversight Compliance Office will periodically review this program. *Id.* ¶ 22. At least every ninety days, the Department of Justice will review a sample of NSA's justifications for querying the archived data. *Id.* ¶ 19. The Director of the NSA himself will, in coordination with the Attorney General, inform the Congressional Intelligence Oversight Committees of the Court's decision to issue the Order. *Id.* ¶ 23. (TS//SI//NF)

Third, the collected metadata will not be kept online (that is, accessible for queries by cleared analysts) indefinitely. The NSA has determined that for operational reasons it is important to retain the metadata online for five years, at which time it will be destroyed. *Id.* ¶ 20. The U.S. Government has a strong operational interest in retaining data online for five years to determine [REDACTED] and contacts associated with newly-discovered "seed" telephone numbers. *Id.* In addition, moving data off-line requires significant resources, raises the possibility of corruption and loss of data, and would incur probable delays in moving data back online for it to be accessed when needed. [REDACTED]

[REDACTED] [Order (Feb. 28, 2006). (TS//SI//NF)]

Finally, when and if the Government seeks an extension of any order from the Court requiring the production of business records containing telephony metadata, 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 telephone numbers were terrorist related. NSA Declaration ¶ 24. (TS//SI//NF)

II. The Application Fully Complies with the First and Fourth Amendments to the Constitution. (U)

There is, of course, no constitutionally protected privacy interest in the information contained in call detail records, or telephony metadata. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme 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; *see also id.* at 744 (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) (internal quotation marks omitted). 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 743-44.¹² Although the telephony metadata that would be obtained here would include not only telephone numbers dialed, but also the length and time of the calls and other routing information, there is no reasonable expectation that such information, which is routinely collected by the telephone companies for billing and fraud detection purposes, is private. The information contained in the

¹² *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)

call detail records of the telecommunications carriers in no way resembles the substantive contents of telephone communications that are protected by the Fourth Amendment. *See Katz v. United States*, 389 U.S. 347 (1967). (S)

Moreover, as this Court has previously found, because of the absence of a reasonable expectation of privacy in metadata, the large number of individuals whose telephony metadata will be obtained "is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur." [REDACTED] at 63. Nor would the derivative use of the archived metadata through contact chaining or [REDACTED] be prohibited by the Fourth Amendment. *See id.* at 63-66; *United States v. Calandra*, 414 U.S. 338, 354 (1974) (Grand jury "[q]uestions based on illegally obtained evidence are only a derivative use of the product of a past unlawful search and seizure. They work no new Fourth Amendment wrong."). (TS//SI//NF)

The proposed business records request is also consistent with the First Amendment. Good faith law enforcement investigation and data-gathering activities using legitimate investigative techniques do not violate the First Amendment, at least where they do not violate the Fourth Amendment. *See Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1064 (D.C. Cir. 1978); *see also* [REDACTED] at 66 ("The weight of authority supports the conclusion that Government information-gathering that does not constitute a Fourth Amendment search or seizure will also comply with the First Amendment when conducted as part of a good-faith criminal investigation."); *cf. Laird v. Tatum*, 408 U.S. 1, 10, 13 (1972) (the "subjective 'chill'" stemming from "the mere existence, without more, of a governmental investigative and data-gathering activity that is alleged to be broader in scope than is reasonably necessary for the accomplishment of a valid governmental purpose" does not constitute a

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

cognizable injury). As this Court recognized in the context of the Government's application to collect e-mail metadata in bulk,

the proposed collection of meta data is not for ordinary law enforcement purposes, but in furtherance of the compelling national interest of identifying and tracking [REDACTED] and ultimately of thwarting terrorist attacks. The overarching investigative effort [REDACTED] is not aimed at curtailing First Amendment activities and satisfies the "good faith" requirement . . .

Id. at 68. (TS//SI//NF)

Nonetheless, we are mindful of this Court's admonition that, because "the extremely broad nature of this collection carries with it a heightened risk that collected information could be subject to various forms of misuse, potentially involving abridgment of First Amendment rights of innocent persons . . . special restrictions on the accessing, retention, and dissemination of such information are necessary to guard against such misuse." *Id.* The strict restrictions proposed here on access to, and processing and dissemination of, the data are almost identical to those imposed by this Court in [REDACTED]. Compare NSA Declaration ¶¶ 13-24 with [REDACTED] at 82-87.¹³ In addition, the Department of Justice would review a sample of NSA's justifications for querying the archived data at least every ninety days. (TS//SI//NF)

¹³ One minor difference is that for operational reasons the NSA seeks to retain the telephony metadata collected online for five rather than four and a half years. Compare NSA Declaration ¶ 20 with [REDACTED] Order (Feb. 28, 2006) (approving retention online of the bulk e-mail metadata for four and a half years). (TS//SI//NF)

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

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

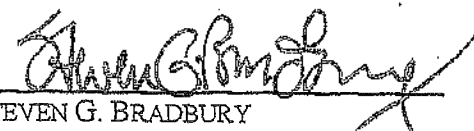
CONCLUSION (U)

For the foregoing reasons, the Court should grant the requested Order. (U)

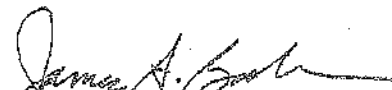
Respectfully submitted,

Dated: May 23, 2006


ALBERTO R. GONZALES
Attorney General


STEVEN G. BRADBURY
*Acting Assistant Attorney General,
Office of Legal Counsel*

JOHN A. EISENBERG
*Deputy Assistant Attorney General,
Office of Legal Counsel*


JAMES A. BAKER
Counsel for Intelligence Policy

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

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