

1 CINDY COHN (SBN 145997)
 cindy@eff.org
 2 LEE TIEN (SBN 148216)
 3 KURT OPSAHL (SBN 191303)
 MATTHEW ZIMMERMAN (SBN 212423)
 4 MARK RUMOLD (SBN 279060)
 DAVID GREENE (SBN 160107)
 5 JAMES S. TYRE (SBN 083117)
 ANDREW CROCKER (SBN 291596)
 6 ELECTRONIC FRONTIER FOUNDATION
 815 Eddy Street
 7 San Francisco, CA 94109
 8 Tel.: (415) 436-9333; Fax: (415) 436-9993

9 THOMAS E. MOORE III (SBN 115107)
 tmoore@rroyselaw.com
 10 ROYSE LAW FIRM, PC
 1717 Embarcadero Road
 11 Palo Alto, CA 94303
 12 Tel.: 650-813-9700; Fax: 650-813-9777

13 Counsel for Plaintiffs

RACHAEL E. MENY (SBN 178514)
 rmeny@kvn.com
 MICHAEL S. KWUN (SBN 198945)
 BENJAMIN W. BERKOWITZ (SBN 244441)
 KEKER & VAN NEST, LLP
 633 Battery Street
 San Francisco, California 94111
 Tel.: (415) 391-5400; Fax: (415) 397-7188

RICHARD R. WIEBE (SBN 121156)
 wiebe@pacbell.net
 LAW OFFICE OF RICHARD R. WIEBE
 One California Street, Suite 900
 San Francisco, CA 94111
 Tel.: (415) 433-3200; Fax: (415) 433-6382

ARAM ANTARAMIAN (SBN 239070)
 aram@eff.org
 LAW OFFICE OF ARAM ANTARAMIAN
 1714 Blake Street
 Berkeley, CA 94703
 Telephone: (510) 289-1626

14 **UNITED STATES DISTRICT COURT**
 15 **NORTHERN DISTRICT OF CALIFORNIA**
 16 **SAN FRANCISCO DIVISION**

17 FIRST UNITARIAN CHURCH OF LOS
 18 ANGELES, *et al.*

19 Plaintiffs,

20 v.

21 NATIONAL SECURITY AGENCY, *et al.*,

22 Defendants.

Case No: 3:13-cv-03287 JSW

**DECLARATION OF CINDY COHN
 IN SUPPORT OF PLAINTIFFS'
 OPPOSITION TO DEFENDANTS'
 MOTION TO DISMISS AND REPLY
 IN SUPPORT OF PLAINTIFFS'
 MOTION FOR PARTIAL
 SUMMARY JUDGMENT**

Date: April 25, 2014
 Time: 9:00 a.m.
 Courtroom 11, 19th Floor
 The Honorable Jeffrey S. White

1 I, CINDY COHN, hereby declare:

2 1. I am a lawyer duly licensed to practice law in the State of California and before this
3 district. I am the Legal Director of the Electronic Frontier Foundation, counsel of record for the
4 plaintiffs.

5 2. I have attached to this Declaration true and correct copies of the following
6 documents:

- 7 • **Exhibit A:** FISC Dkt. No. BR: 06-05, Ex. C, Mem. of Law in Supp. of Appl. for
8 Certain Tangible Things for Investigations to Protect Against International Terrorism
9 dated May 23, 2006;
- 10 • **Exhibit B:** President's Review Grp. on Intelligence and Commc'n Techs., Liberty
11 and Security in a Changing World, Report and Recommendations of the dated
12 December 12, 2013; and
- 13 • **Exhibit C:** Privacy and Civil Liberties Oversight Bd., Report on the Telephone
14 Records Program Conducted under Section 215 of the USA PATRIOT Act and on
15 the Operations of the Foreign Intelligence Surveillance Court dated January 23,
16 2014.

17 I declare under penalty of perjury under the laws of the United States that the foregoing is
18 true and correct. Executed on January 25, 2014, at San Francisco, California.

19
20
21
22
23
24
25
26
27
28

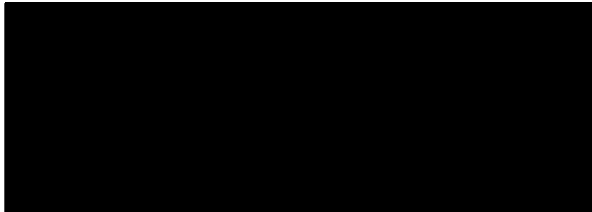
/s/ Cindy Cohn
CINDY COHN

Exhibit A

Exhibit A

~~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] [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] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [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]. The attached Application seeks this Court's authorization to collect in bulk [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 [REDACTED]. 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 who [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 [REDACTED]. [REDACTED] For billing and fraud detection purposes, [REDACTED] “call detail records” that contain routing information, including which telephone number called which other telephone number at what date and time, and for how long, i.e., “metadata.” 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 [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~~

~~TOP SECRET//ECS//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 [REDACTED] 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

[REDACTED]

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

~~TOP SECRET//ECS//SI//NOFORN~~

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

obtained” from such collection “is relevant to an ongoing investigation to protect against international terrorism.” 50 U.S.C. § 1842(c)(2); ██████████ 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 ██████████ communications.” *Id.* at 49. Moreover, as was the case in ██████████, 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~~

~~TOP SECRET//ECS//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, audiotope 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//ECS//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 ██████ remains intent on striking the United States and U.S. interests. *See* NCTC Declaration ¶¶ 5-7, 8, 11-13. “█████ is an international

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

~~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, ██████ “continues its efforts to reconstitute communication links to a transnational network of ██████ personnel and affiliated groups.” *Id.* ¶ 39. Recent intelligence suggests that ██████ has become “keenly” interested in soft targets, especially those that are densely populated. *Id.* ¶¶ 17, 75. ██████ 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 ██████ attack in the United States might use chemical, biological, radiological or nuclear weapons, “especially given [██████] clear intent to develop such capabilities and use them to strike the Homeland.” *Id.* ¶ 81. In sum, ██████ continues to present “a credible threat for a massive attack against the US Homeland.” *Id.* ¶ 91. By helping to find and identify ██████, 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 ██████ itself has claimed would be larger than the attacks of September 11th. (TS//SI//HCS//OC,NF)

B. ██████ Use of Telephones to Communicate (S)

██████ 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, ██████ ██████ make domestic U.S. telephone calls. For purposes of preventing terrorist attacks against the United States, the most analytically significant ██████ telephone communications are those that either have one end in the United States or that are purely domestic, because those

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

~~TOP SECRET//ECS//SI//NOFORN~~

communications are particularly likely to identify individuals who are associated with ██████████ 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 ██████████ 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//ECS//SI//NOFORN~~

~~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~~

~~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 [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' [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]

Obviously, such [REDACTED] is a critical tool for

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

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

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

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

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

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, ██████████ would copy and transmit the call detail records, ██████████ 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

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

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

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] 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~~

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

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

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

[REDACTED] Osama bin Laden [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~~

~~TOP SECRET//TICS//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 into [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] [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. See [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)

~~TOP SECRET//TICS//SI//NOFORN~~

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

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] of electronic communications, all but a very small fraction of which could be expected to be unrelated to [REDACTED] [REDACTED] *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]-related FBI

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

~~TOP SECRET//TICS//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//TICS//SI//NOFORN~~

~~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~~

~~TOP SECRET//ICS//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] [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//ICS//SI//NOFORN~~

~~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)

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

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

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

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

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

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] 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. *See generally* [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~~)

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

~~TOP SECRET//HCS//SI//NOFORN~~**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)

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

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

call detail records [REDACTED] 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 of [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//HCS//SI//NOFORN~~

~~TOP SECRET//HCS//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 ██████████ operatives and ultimately of thwarting terrorist attacks. The overarching investigative effort against ██████████ 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 ██████████. Compare NSA Declaration ¶¶ 13-24 with ██████████ 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 ██████████ Order ██████████ (approving retention online of the bulk e-mail metadata for four and a half years). (~~TS//SI//NF~~)

~~TOP SECRET//HCS//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


*Acting Assistant Attorney General,
Office of Legal Counsel*


*Deputy Assistant Attorney General,
Office of Legal Counsel*


Counsel for Intelligence Policy


*Senior Counsel,
Office of Legal Counsel*

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

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

All redactions taken in accordance with one or more of the following FOIA exemptions and statutes:

- (b) (1)
- (b) (3) - P.L. 86-36
- (b) (3) - 50 USC 3024(i)
- (b) (3) - 18 USC 798

~~SECRET~~

848

NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE

Fort George G. Meade, Maryland

UNITED STATES SIGNALS INTELLIGENCE

DIRECTIVE

18

27 July 1993

See Letter of Promulgation for instructions on reproduction or release of this document.

OPC: D2

CLASSIFIED BY NSA/CSSM 123-2

DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

27 July 1993

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE
(USSID)

18

LEGAL COMPLIANCE AND
MINIMIZATION PROCEDURES ~~(FOUO)~~

LETTER OF PROMULGATION

(U) This USSID prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. persons.

(U) This USSID has been completely rewritten to make it shorter and easier to understand. It constitutes a summary of the laws and regulations directly affecting USSS operations. All USSS personnel who collect, process, retain, or disseminate information to, from, or about U.S. persons or persons in the United States must be familiar with its contents.

~~(FOUO)~~ This USSID supersedes USSID 18 and USSID 18, Annex A (distributed separately to selected recipients), both of which are dated 20 October 1980, and must now be destroyed. Notify DIRNSA/CHCSS (USSID Manager) if this edition of USSID 18 is destroyed because of an emergency action; otherwise, request approval from DIRNSA/CHCSS before destroying this USSID.

~~(FOUO)~~ Release or exposure of this document to contractors and consultants without approval from the USSID Manager is prohibited. Instructions applicable to release or exposure of USSID to contractors and consultants may be found in USSID 12.

~~(FOUO)~~ Questions and comments concerning this USSID should be addressed to the Office of the General Counsel, NSA/CSS (Attention: [REDACTED] NSTS 963-3121 or [REDACTED])



J. M. McCONNELL
Vice Admiral, U.S. Navy
Director

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

28 October 1997

UNITED STATES SIGNALS INTELLIGENCE

DIRECTIVE

(USSID)

18

LEGAL COMPLIANCE AND MINIMIZATION
PROCEDURES ~~(FOUO)~~

CHANGE 1


LETTER OF PROMULGATION

~~(FOUO)~~ This hard copy change provides replacement pages for your copy of USSID 18, dated 27 July 1993.

Actions: 1. Change references to "P05" to read "P02" in paragraphs 5.4.d.(3), 7.1. (last line), 7.2.c.(6) (lines 3 and 5), 7.3.c.(1) (lines 2 and 3), 7.5., 8.3.b., and 8.4.b. in the basic USSID 18.

2. From your copy of USSID 18 remove and destroy pages A-1/1 through A-1/8.

3. Insert new pages A-1/1 through A-1/9 (replacement of pages in above action). These pages update the USSID to reflect current changes in standard minimization procedures for NSA electronic surveillances.

4. In the last paragraph of the Letter of Promulgation change to read: "Questions and comments concerning this USSID should be addressed to the Office of General Counsel, NSA/CSS, NSTS 963-3121 or 

5. On the Table of Contents (page iv), change the title of Appendix 1 to Annex A to read "Standardized Minimization Procedures For NSA Electronic Surveillances".

FOR THE EXECUTIVE AGENT:


USSID Manager

NOTE: DESTROY THIS PAGE AFTER POSTING THE ENCLOSED CHANGE MATERIAL.
RETAIN THE ORIGINAL LETTER OF PROMULGATION WITH USSID 18.

~~FOR OFFICIAL USE ONLY~~

~~SECRET~~USSID 18
27 July 1993

TABLE OF CONTENTS

SECTION 1 - PREFACE	1
SECTION 2 - REFERENCES	1
SECTION 3 - POLICY	2
SECTION 4 - COLLECTION	2
4.1. Communications to, from or About U.S. Persons and [REDACTED]	2
a. Foreign Intelligence Surveillance Court Approval	2
b. Attorney General Approval	2
c. DIRNSA/CHCSS Approval	2
d. Emergency Situations	3
e. Annual Reports	4
4.2. [REDACTED]	4
4.3. Incidental Acquisition of U.S. Person Information	4
4.4. Nonresident Alien Targets Entering the United States	5
4.5. U.S. Person Targets Entering the United States	5
4.6. Requests to Target U.S. Persons	5
4.7. Direction Finding	5
4.8. Distress Signals	5
4.9. COMSEC Monitoring and Security Testing of Automated Information Systems ..	6
SECTION 5 - PROCESSING	6
5.1. Use of Selection Terms During Processing	6
5.2. Annual Review by DDO	6
5.3. Forwarding of Intercepted Material	6
5.4. Nonforeign Communications	7
a. Communications between Persons in the United States	7
b. Communications between U.S. Persons	7
c. Communications Involving an Officer or Employee	7
of the U.S. Government	
d. Exceptions	7
5.5. Radio Communications with a Terminal in the United States	7
SECTION 6 - RETENTION	8
6.1. Retention of Communications to, from, or About U.S. Persons	8
a. Unenciphered Communications; and Communications Necessary	8
to Maintain Technical Data Bases for Cryptanalytic or	
Traffic Analytic Purposes	
b. Communications Which Could be Disseminated Under Section 7	8
6.2. Access	8
SECTION 7 - DISSEMINATION	8

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~CONFIDENTIAL~~USSID 18
27 July 1993

DISTRIBUTION

2	A041	12	B33
2	A055	5	B34
3	A1095	10	B35
8	A111	1	B351/
1	A112	1	B409
4	A113	14	B41
2	A114	10	B42
2	A12	4	B43
1	A13	7	B44
1	A131	3	B45
3	A132	1	B461
4	A133	1	B5094
4	A134	6	B521
1	A135	1	B522
4	A136	1	B54
2	A14	1	B5423
1	A153	1	B55
1	A209	1	B56
2	A21	4	B609
1	A22	1	B61
2	A23	1	B63
1	A405	1	B646
2	A42	2	B709
2	A609	2	B7095
1	A62	26	B71
1	A63	3	B72
1	A64	15	B73
1	A641	4	B75
1	A65	1	C SPO
6	A67	1	CMATT
1	A72	12	D1
1	B04	6	D2
3	B05	1	D3
1	B109	1	DCN
2	B209	1	E
5	B21	1	E09
1	B22	1	E1
2	B23	1	E11
1	B26	1	E31
1	B3094	3	E32
1	B3095	1	E32/B
3	B31	1	E32/G
4	B312	3	E42
6	B32	1	E54

TOTAL COPIES 1193

~~CONFIDENTIAL~~

Distribution Page 1 of 6

~~CONFIDENTIAL~~USSID 18
27 July 1993

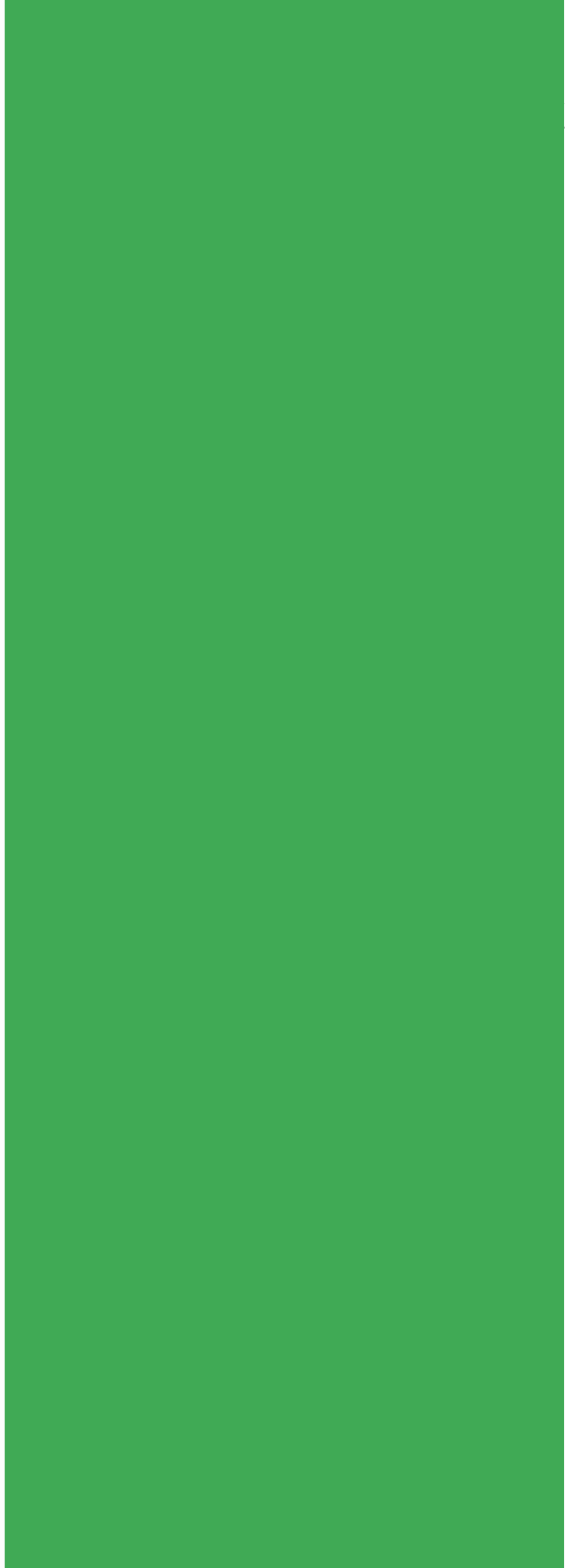
1	G01	1	L091
2	G111	1	LAO
3	G112	1	M091
1	G112	1	M31
1	G133	1	M5
1	G133C	1	M51
2	G223	1	M52
2	G23	1	N22
1	G24 (SLO)	1	N252
1	G27	1	N511
2	G31	1	N5209
1	G33	1	P042
1	G35	1	P043
1	G36	1	P0433
1	G364	150	P0442 (STOCK)
2	G36N	1	P05
2	G41	6	P052
1	G412	3	P0522
1	G42	1	P0533
1	G421	1	P0541
1	G44	1	P05A
1	G45	1	Q109
2	G5 NSOC (ASGC)	1	Q32
1	G5 NSOC (BSGC)	1	S9
1	G5 NSOC (NALA)	1	T09
1	G5 NSOC (NMJIC)	2	T093
1	G5 NSOC (SRO)	1	V09
1	G5 NSOC (WSGC)	1	W04
1	G509	1	W05
1	G561	1	W109
1	G562	1	W15
1	G564	1	W16
1	G58	1	W17
1	G71	1	W174
1	I11	1	W18
2	I2	1	W2091
1	J23	1	W21
1	J25	1	W232
1	J34	1	W27
1	K1	1	W309
1	K13	2	W31
2	K2	1	W32
1	K34	2	W33
1	K4	1	W335 (SOC)
1	K41	1	W341
2	K42	3	W4
1	K43	1	X41
3	K51	1	Z03
1	K52	1	Z09
1	K609	5	Z109
1	K609	1	Z11

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

USSID 18
27 July 1993

1 Z14
2 Z156
1 Z3
1 Z31
1 Z33
1 Z34
1 Z41
1 Z42



~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

USSID 18
27 July 1993



~~CONFIDENTIAL~~

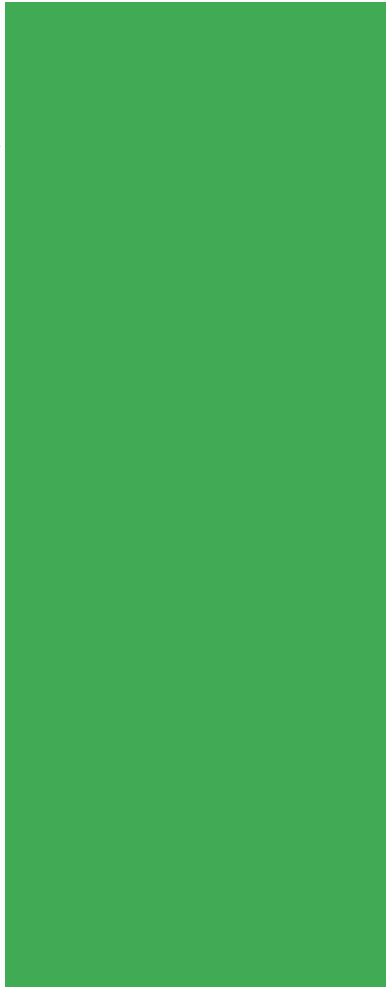
USSID 18
27 July 1993



~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

USSID 18
27 July 1993



~~CONFIDENTIAL~~

Distribution Page 6 of 6

~~SECRET~~

27 July 1993

USSID 18

LEGAL COMPLIANCE AND
MINIMIZATION PROCEDURES (U)

SECTION 1 - PREFACE

1.1. (U) The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government. The Supreme Court has ruled that the interception of electronic communications is a search and seizure within the meaning of the Fourth Amendment. It is therefore mandatory that signals intelligence (SIGINT) operations be conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment.

1.2. (U) In determining whether United States SIGINT System (USSS) operations are "reasonable," it is necessary to balance the U.S. Government's need for foreign intelligence information and the privacy interests of persons protected by the Fourth Amendment. Striking that balance has consumed much time and effort by all branches of the United States Government. The results of that effort are reflected in the references listed in Section 2 below. Together, these references require the minimization of U.S. person information collected, processed, retained or disseminated by the USSS. The purpose of this document is to implement these minimization requirements.

1.3. (U) Several themes run throughout this USSID. The most important is that intelligence operations and the protection of constitutional rights are not incompatible. It is not necessary to deny legitimate foreign intelligence collection or suppress legitimate foreign intelligence information to protect the Fourth Amendment rights of U.S. persons.

1.4. (U) Finally, these minimization procedures implement the constitutional principle of "reasonableness" by giving different categories of individuals and entities different levels of protection. These levels range from the stringent protection accorded U.S. citizens and permanent resident aliens in the United States to provisions relating to foreign diplomats in the U.S. These differences reflect yet another main theme of these procedures, that is, that the focus of all foreign intelligence operations is on foreign entities and persons.

SECTION 2 - REFERENCES

2.1. (U) References

- a. 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, Public Law No. 95-511.
- b. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

c. DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," dated 25 April 1988.

d. NSA/CSS Directive No. 10-30, "Procedures Governing Activities of NSA/CSS that Affect U.S. Persons," dated 20 September 1990.

SECTION 3 - POLICY

3.1. (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS.* The USSS will not intentionally COLLECT communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID.

SECTION 4 - COLLECTION

4.1. (S-CCO) Communications which are known to be to, from or about a U.S. PERSON [REDACTED] will not be intentionally intercepted, or selected through the use of a SELECTION TERM, except in the following instances:

a. With the approval of the United States Foreign Intelligence Surveillance Court under the conditions outlined in Annex A of this USSID.

b. With the approval of the Attorney General of the United States, if:

(1) The COLLECTION is directed against the following:

(a) Communications to or from U.S. PERSONS outside the UNITED STATES, or

(b) International communications to, from, [REDACTED] or [REDACTED]

(c) Communications which are not to or from but merely about U.S. PERSONS (wherever located).

(2) The person is an AGENT OF A FOREIGN POWER, and

(3) The purpose of the COLLECTION is to acquire significant FOREIGN INTELLIGENCE information.

c. With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and

(1) The person has CONSENTED to the COLLECTION by executing one of the CONSENT forms contained in Annex H, or

* Capitalized words in Sections 3 through 9 are defined terms in Section 9.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

(2) The person is reasonably believed to be held captive by a FOREIGN POWER or group engaged in INTERNATIONAL TERRORISM, or

(3) The TARGETED [REDACTED]

[REDACTED] and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex I, or

(4) The COLLECTION is directed against [REDACTED] between a U.S. PERSON in the UNITED STATES and a foreign entity outside the UNITED STATES, the TARGET is the foreign entity, and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex K, or

(5) Technical devices (e.g., [REDACTED]) are employed to limit acquisition by the USSS to communications to or from the TARGET or to specific forms of communications used by the TARGET (e.g., [REDACTED]) and the COLLECTION is directed against [REDACTED] voice and facsimile communications with one COMMUNICANT in the UNITED STATES, and the TARGET of the COLLECTION is [REDACTED]

(a) A non-U.S. PERSON located outside the UNITED STATES, [REDACTED]

(b) [REDACTED]

(6) Copies of approvals granted by the DIRNSA/CHCSS under these provisions will be retained in the Office of General Counsel for review by the Attorney General.

d. Emergency Situations.

(1) In emergency situations, DIRNSA/CHCSS may authorize the COLLECTION of information to, from, or about a U.S. PERSON who is outside the UNITED STATES when securing the prior approval of the Attorney General is not practical because:

(a) The time required to obtain such approval would result in the loss of significant FOREIGN INTELLIGENCE and would cause substantial harm to the national security.

(b) A person's life or physical safety is reasonably believed to be in immediate danger.

(c) The physical security of a defense installation or government property is reasonably believed to be in immediate danger.

(2) In those cases where the DIRNSA/CHCSS authorizes emergency COLLECTION, except for actions taken under paragraph d.(1)(b) above, DIRNSA/CHCSS shall find that there is probable cause that the TARGET meets one of the following criteria:

(a) A person who, for or on behalf of a FOREIGN POWER, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or INTERNATIONAL TERRORIST activities, or activities in preparation for INTERNATIONAL TERRORIST activities; or who conspires with, or knowingly aids and abets a person engaging in such activities.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

(b) A person who is an officer or employee of a FOREIGN POWER.

(c) A person unlawfully acting for, or pursuant to the direction of, a FOREIGN POWER. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the FOREIGN POWER.

(d) A CORPORATION or other entity that is owned or controlled directly or indirectly by a FOREIGN POWER.

(e) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

(3) In all cases where emergency collection is authorized, the following steps shall be taken:

(a) The General Counsel will be notified immediately that the COLLECTION has started.

(b) The General Counsel will initiate immediate efforts to obtain Attorney General approval to continue the collection. If Attorney General approval is not obtained within seventy two hours, the COLLECTION will be terminated. If the Attorney General approves the COLLECTION, it may continue for the period specified in the approval.

e. Annual reports to the Attorney General are required for COLLECTION conducted under paragraphs 4.1.c.(3) and (4). Responsible analytic offices will provide such reports through the Deputy Director for Operations (DDO) and the General Counsel to the DIRNSA/CHCSS for transmittal to the Attorney General by 31 January of each year.

4.2. (S-CCO) [REDACTED]

a. [REDACTED]

b. [REDACTED]

4.3. (U) Incidental Acquisition of U.S. PERSON Information. Information to, from or about U.S. PERSONS acquired incidentally as a result of COLLECTION directed against appropriate FOREIGN INTELLIGENCE TARGETS may be retained and processed in accordance with Section 5 and Section 6 of this USSID.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

4.4. ~~(S-CCO)~~ Nonresident Alien TARGETS Entering the UNITED STATES.

a. If the communications of a nonresident alien located abroad are being TARGETED and the USSS learns that the individual has entered the UNITED STATES, COLLECTION may continue for a period of 72 hours provided that the DIRNSA/CHCSS is advised immediately and:

(1) Immediate efforts are initiated to obtain Attorney General approval, or

(2) A determination is made within the 72 hour period that the [REDACTED]

b. If Attorney General approval is obtained, the COLLECTION may continue for the length of time specified in the approval.

c. If it is determined that [REDACTED] COLLECTION may continue at the discretion of the operational element.

d. If [REDACTED] or if Attorney General approval is not obtained within 72 hours, COLLECTION must be terminated [REDACTED] Attorney General approval is obtained, or the individual leaves the UNITED STATES.

4.5. ~~(C-CCO)~~ U.S. PERSON TARGETS Entering the UNITED STATES.

a. If communications to, from or about a U.S. PERSON located outside the UNITED STATES are being COLLECTED under Attorney General approval described in Section 4.1.b. above, the COLLECTION must stop when the USSS learns that the individual has entered the UNITED STATES.

b. While the individual is in the UNITED STATES, COLLECTION may be resumed only with the approval of the United States Foreign Intelligence Surveillance Court as described in Annex A.

4.6. ~~(S-CCO)~~ Requests to TARGET U.S. PERSONS. All proposals for COLLECTION against U.S. PERSONS, [REDACTED] must be submitted through the DDO and the General Counsel to the DIRNSA/CHCSS for review.

4.7. ~~(C-CCO)~~ Direction Finding. Use of direction finding solely to determine the location of a transmitter located outside of the UNITED STATES does not constitute ELECTRONIC SURVEILLANCE or COLLECTION even if directed at transmitters believed to be used by U.S. PERSONS. Unless COLLECTION of the communications is otherwise authorized under these procedures, the contents of communications to which a U.S. PERSON is a party monitored in the course of direction finding may only be used to identify the transmitter.

4.8. (U) Distress Signals. Distress signals may be intentionally collected, processed, retained, and disseminated without regard to the restrictions contained in this USSID.

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

~~SECRET~~USSID 18
27 July 1993

4.9. (U) COMSEC Monitoring and Security Testing of Automated Information Systems. Monitoring for communications security purposes must be conducted with the consent of the person being monitored and in accordance with the procedures established in National Telecommunications and Information Systems Security Directive 600, Communications Security (COMSEC) Monitoring, dated 10 April 1990. Monitoring for communications security purposes is not governed by this USSID. Intrusive security testing to assess security vulnerabilities in automated information systems likewise is not governed by this USSID.

SECTION 5 - PROCESSING

5.1. ~~(S-CCO)~~ Use of Selection Terms During Processing. When a SELECTION TERM is intended to INTERCEPT a communication on the basis of the content of the communication, or because a communication is enciphered, rather than on the basis of the identity of the COMMUNICANT or the fact that the communication mentions a particular individual, the following rules apply:

a. No SELECTION TERM that is reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON (wherever located), [REDACTED] may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained by use of such SELECTION TERM.

b. No SELECTION TERM that has resulted in the INTERCEPTION of a significant number of communications to or from such persons or entities may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained.

c. SELECTION TERMS that have resulted or are reasonably likely to result in the INTERCEPTION of communications to or from such persons or entities shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE.

5.2. ~~(S-CCO)~~ Annual Review by DDO.

a. All SELECTION TERMS that are reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON or terms that have resulted in the INTERCEPTION of a significant number of such communications shall be reviewed annually by the DDO or a designee.

b. The purpose of the review shall be to determine whether there is reason to believe that FOREIGN INTELLIGENCE will be obtained, or will continue to be obtained, by the use of these SELECTION TERMS.

c. A copy of the results of the review will be provided to the Inspector General and the General Counsel.

5.3. ~~(C-CCO)~~ Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA, intermediate processing facilities, and collaborating centers.

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

~~SECRET~~USSID 18
27 July 19935.4. ~~(S-CCO)~~ Nonforeign Communications.

a. Communications between persons in the UNITED STATES. Private radio communications solely between persons in the UNITED STATES inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be promptly destroyed unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

b. Communications between U.S. PERSONS. Communications solely between U.S. PERSONS will be treated as follows:

(1) Communications solely between U.S. PERSONS inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be destroyed upon recognition, if technically possible, except as provided in paragraph 5.4.d. below.

(2) Notwithstanding the preceding provision, cryptologic data (e.g., signal and encipherment information) and technical communications data (e.g., circuit usage) may be extracted and retained from those communications if necessary to:

- (a) Establish or maintain intercept, or
- (b) Minimize unwanted intercept, or
- (c) Support cryptologic operations related to FOREIGN COMMUNICATIONS.

c. Communications involving an Officer or Employee of the U.S. Government. Communications to or from any officer or employee of the U.S. Government, or any state or local government, will not be intentionally intercepted. Inadvertent INTERCEPTIONS of such communications (including those between foreign TARGETS and U.S. officials) will be treated as indicated in paragraphs 5.4.a. and b., above.

d. Exceptions: Notwithstanding the provisions of paragraphs 5.4.b. and c., the DIRNSA/CHCSS may waive the destruction requirement for international communications containing, inter alia, the following types of information:

- (1) Significant FOREIGN INTELLIGENCE, or
 - (2) Evidence of a crime or threat of death or serious bodily harm to any person, or
 - (3) Anomalies that reveal a potential vulnerability to U.S. communications security.
- Communications for which the Attorney General or DIRNSA/CHCSS's waiver is sought should be forwarded to NSA/CSS, Attn: P05- PO2.

5.5. ~~(S-CCO)~~ Radio Communications with a Terminal in the UNITED STATES.

a. All radio communications that pass over channels with a terminal in the UNITED STATES must be processed through a computer scan dictionary or similar device unless those communications occur over channels used exclusively by a FOREIGN POWER.

b. International common-access radio communications that pass over channels with a terminal in the UNITED STATES, other than [REDACTED] communications, may be processed without the use of a computer scan dictionary or similar device if necessary to determine whether a channel contains communications of FOREIGN INTELLIGENCE interest which NSA may wish

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18
27 July 1993

to collect. Such processing may not exceed two hours without the specific prior written approval of the DDO and, in any event, shall be limited to the minimum amount of time necessary to determine the nature of communications on the channel and the amount of such communications that include FOREIGN INTELLIGENCE. Once it is determined that the channel contains sufficient communications of FOREIGN INTELLIGENCE interest to warrant COLLECTION and exploitation to produce FOREIGN INTELLIGENCE, a computer scan dictionary or similar device must be used for additional processing.

c. Copies of all DDO written approvals made pursuant to 5.5.b. must be provided to the General Counsel and the Inspector General.

SECTION 6 - RETENTION

6.1. ~~(S-CCO)~~ Retention of Communications to, from or About U.S. PERSONS.

a. Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:

(1) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the DDO determines in writing that retention for a longer period is required to respond to authorized FOREIGN INTELLIGENCE requirements.

(2) Communications necessary to maintain technical data bases for cryptanalytic or traffic analytic purposes may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. Sufficient duration may vary with the nature of the exploitation and may consist of any period of time during which the technical data base is subject to, or of use in, cryptanalysis. If a U.S. PERSON'S identity is not necessary to maintaining technical data bases, it should be deleted or replaced by a generic term when practicable.

b. Communications which could be disseminated under Section 7, below (i.e., without elimination of references to U.S. PERSONS) may be retained in their original or transcribed form.

6.2. ~~(S-CCO)~~ Access. Access to raw traffic storage systems which contain identities of U.S. PERSONS must be limited to SIGINT production personnel.

SECTION 7 - DISSEMINATION

7.1. ~~(C-CCO)~~ Focus of SIGINT Reports. All SIGINT reports will be written so as to focus solely on the activities of foreign entities and persons and their agents. Except as provided in Section 7.2., FOREIGN INTELLIGENCE information concerning U.S. PERSONS must be disseminated in a manner which does not identify the U.S. PERSON. Generic or general terms or phrases must be substituted for the identity (e.g., "U.S. firm" for the specific name of a U.S. CORPORATION or "U.S. PERSON" for the specific name of a U.S. PERSON). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year and any requests from SIGINT customers for such identities should be referred to P05, P02.

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18
27 July 1993

7.2. ~~(C-CCO)~~ Dissemination of U.S. PERSON Identities. SIGINT reports may include the identification of a U.S. PERSON only if one of the following conditions is met and a determination is made by the appropriate approval authority that the recipient has a need for the identity for the performance of his official duties:

a. The U.S. PERSON has CONSENTED to the dissemination of communications of, or about, him or her and has executed the CONSENT form found in Annex H of this USSID, or

b. The information is PUBLICLY AVAILABLE (i.e., the information is derived from unclassified information available to the general public), or

c. The identity of the U.S. PERSON is necessary to understand the FOREIGN INTELLIGENCE information or assess its importance. The following nonexclusive list contains examples of the type of information that meet this standard:

(1) FOREIGN POWER or AGENT OF A FOREIGN POWER. The information indicates that the U.S. PERSON is a FOREIGN POWER or an AGENT OF A FOREIGN POWER.

(2) Unauthorized Disclosure of Classified Information. The information indicates that the U.S. PERSON may be engaged in the unauthorized disclosure of classified information.

(3) International Narcotics Activity. The information indicates that the individual may be engaged in international narcotics trafficking activities. (See Annex J of this USSID for further information concerning individuals involved in international narcotics trafficking).

(4) Criminal Activity. The information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.

(5) Intelligence TARGET. The information indicates that the U.S. PERSON may be the TARGET of hostile intelligence activities of a FOREIGN POWER.

(6) Threat to Safety. The information indicates that the identity of the U.S. PERSON is pertinent to a possible threat to the safety of any person or organization, including those who are TARGETS, victims or hostages of INTERNATIONAL TERRORIST organizations. Reporting units shall identify to P05 any report containing the identity of a U.S. PERSON reported under this subsection (6). Field reporting to P05 should be in the form of a CRITCOMM message (DDI XAO) and include the report date-time-group (DTG), product serial number and the reason for inclusion of the U.S. PERSON'S identity.

(7) Senior Executive Branch Officials. The identity is that of a senior official of the Executive Branch of the U.S. Government. In this case only the official's title will be disseminated. Domestic political or personal information on such individuals will be neither disseminated nor retained.

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

7.3. ~~(C-CCO)~~ Approval Authorities. Approval authorities for the release of identities of U.S. persons under Section 7 are as follows:

a. DIRNSA/CHCSS. DIRNSA/CHCSS must approve dissemination of:

(1) The identities of any senator, congressman, officer, or employee of the Legislative Branch of the U.S. Government.

(2) The identity of any person for law enforcement purposes.

b. Field Units and NSA Headquarters Elements. All SIGINT production organizations are authorized to disseminate the identities of U.S. PERSONS when:

(1) The identity is pertinent to the safety of any person or organization.

(2) The identity is that of a senior official of the Executive Branch.

(3) The U.S. PERSON has CONSENTED under paragraph 7.2.a. above.

c. DDO and Designees.

(1) In all other cases, U.S. PERSON identities may be released only with the prior approval of the Deputy Director for Operations, the Assistant Deputy Director for Operations, the Chief, P05, the Deputy Chief, P05, or, in their absence, the Senior Operations Officer of the National SIGINT Operations Center. The DDO or ADDO shall review all U.S. identities released by these designees as soon as practicable after the release is made.

(2) For law enforcement purposes involving narcotics related information, DIRNSA has granted to the DDO authority to disseminate U.S. identities. This authority may not be further delegated.

7.4. (U) Privileged Communications and Criminal Activity. All proposed disseminations of information constituting U.S. PERSON privileged communications (e.g., attorney/client, doctor/patient) and all information concerning criminal activities or criminal or judicial proceedings in the UNITED STATES must be reviewed by the Office of General Counsel prior to dissemination.

7.5. (U) Improper Dissemination. If the name of a U.S. PERSON is improperly disseminated, the incident should be reported to P05 within 24 hours of discovery of the error.

P02

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

SECTION 8 - RESPONSIBILITIES

8.1. (U) Inspector General. The Inspector General shall:

- a. Conduct regular inspections and perform general oversight of NSA/CSS activities to ensure compliance with this USSID.
- b. Establish procedures for reporting by Key Component and Field Chiefs of their activities and practices for oversight purposes.
- c. Report to the DIRNSA/CHCSS, annually by 31 October, concerning NSA/CSS compliance with this USSID.
- d. Report quarterly with the DIRNSA/CHCSS and General Counsel to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense (Intelligence Oversight).

8.2. (U) General Counsel. The General Counsel shall:

- a. Provide legal advice and assistance to all elements of the USSS regarding SIGINT activities. Requests for legal advice on any aspect of these procedures should be sent by CRITICOMM to DDI XDI, or by NSA/CSS secure telephone 963-3121, or [REDACTED]
- b. Prepare and process all applications for Foreign Intelligence Surveillance Court orders and requests for Attorney General approvals required by these procedures.
- c. Advise the Inspector General in inspections and oversight of USSS activities.
- d. Review and assess for legal implications as requested by the DIRNSA/CHCSS, Deputy Director, Inspector General or Key Components Chief, all new major requirements and internally generated USSS activities.
- e. Advise USSS personnel of new legislation and case law that may affect USSS missions, functions, operations, activities, or practices.
- f. Report as required to the Attorney General and the President's Intelligence Oversight Board and provide copies of such reports to the DIRNSA/CHCSS and affected agency elements.
- g. Process requests from any DoD Intelligence component for authority to use signals as described in Procedure 5, Part 5, of DoD 5240.1-R, for periods in excess of 90 days in the development, test, or calibration of ELECTRONIC SURVEILLANCE equipment and other equipment that can intercept communications.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~USSID 18
27 July 1993

8.3. (U) Deputy Director for Operations (DDO). The DDO shall:

a. Ensure that all SIGINT production personnel understand and maintain a high degree of awareness and sensitivity to the requirements of this USSID.

b. Apply the provisions of this USSID to all SIGINT production activities. The DDO staff focal point for USSID 18 matters is P05 (use CRITICOMM DDI XAO).
P02

c. Conduct necessary reviews of SIGINT production activities and practices to ensure consistency with this USSID.

d. Ensure that all new major requirements levied on the USSS or internally generated activities are considered for review by the General Counsel. All activities that raise questions of law or the proper interpretation of this USSID must be reviewed by the General Counsel prior to acceptance or execution.

8.4. (U) All Elements of the USSS. All elements of the USSS shall:

a. Implement this directive upon receipt.

b. Prepare new procedures or amend or supplement existing procedures as required to ensure adherence to this USSID. A copy of such procedures shall be forwarded to NSA/CSS, Attn: P05. P02.

c. Immediately inform the DDO of any tasking or instructions that appear to require actions at variance with this USSID.

d. Promptly report to the NSA Inspector General and consult with the NSA General Counsel on all activities that may raise a question of compliance with this USSID.

SECTION 9 - DEFINITIONS

9.1. ~~(S-CCO)~~ AGENT OF A FOREIGN POWER means:

a. Any person, other than a U.S. PERSON, who:

(1) Acts in the UNITED STATES as an officer or employee of a FOREIGN POWER, or as a member of a group engaged in INTERNATIONAL TERRORISM or activities in preparation therefor; or

(2) Acts for, or on behalf of, a FOREIGN POWER that engages in clandestine intelligence activities in the UNITED STATES contrary to the interests of the UNITED STATES, when the circumstances of such person's presence in the UNITED STATES indicate that such person may engage in such activities in the UNITED STATES, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

b. Any person, including a U.S. PERSON, who:

(1) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a FOREIGN POWER, which activities involve, or may involve, a violation of the criminal statutes of the UNITED STATES; or

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18
27 July 1993

(2) Pursuant to the direction of an intelligence service or network of a FOREIGN POWER, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such FOREIGN POWER, which activities involve or are about to involve, a violation of the criminal statutes of the UNITED STATES; or

(3) Knowingly engages in sabotage or INTERNATIONAL TERRORISM, or activities that are in preparation therefor, for or on behalf of a FOREIGN POWER; or

(4) Knowingly aids or abets any person in the conduct of activities described in paragraphs 9.1.b.(1) through (3) or knowingly conspires with any person to engage in those activities.

c. For all purposes other than the conduct of ELECTRONIC SURVEILLANCE as defined by the Foreign Intelligence Surveillance Act (see Annex A), the phrase "AGENT OF A FOREIGN POWER" also means any person, including U.S. PERSONS outside the UNITED STATES, who are officers or employees of a FOREIGN POWER, or who act unlawfully for or pursuant to the direction of a FOREIGN POWER, or who are in contact with or acting in collaboration with an intelligence or security service of a FOREIGN POWER for the purpose of providing access to information or material classified by the UNITED STATES Government and to which the person has or has had access. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this provision; absent evidence that the person is taking direction from or acting in knowing concert with a FOREIGN POWER.

9.2. ~~(C)~~ COLLECTION means intentional tasking or SELECTION of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.

9.3. (U) COMMICANT means a sender or intended recipient of a communication.

9.4. (U) COMMUNICATIONS ABOUT A U.S. PERSON are those in which the U.S. PERSON is identified in the communication. A U.S. PERSON is identified when the person's name, unique title, address, or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A mere reference to a product by brand name or manufacturer's name, e.g., "Boeing 707" is not an identification of a U.S. person.

9.5. (U) CONSENT, for SIGINT purposes, means an agreement by a person or organization to permit the USSS to take particular actions that affect the person or organization. An agreement by an organization with the National Security Agency to permit COLLECTION of information shall be deemed valid CONSENT if given on behalf of such organization by an official or governing body determined by the General Counsel, National Security Agency, to have actual or apparent authority to make such an agreement.

9.6. (U) CORPORATIONS, for purposes of this USSID, are entities legally recognized as separate from the persons who formed, own, or run them. CORPORATIONS have the nationality of the nation state under whose laws they were formed. Thus, CORPORATIONS incorporated under UNITED STATES federal or state law are U.S. PERSONS.

9.7. (U) ELECTRONIC SURVEILLANCE means:

a. In the case of an electronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is a party to the communication.

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

b. In the case of a nonelectronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is visibly present at the place of communication.

c. The term ELECTRONIC SURVEILLANCE does not include the use of radio direction finding equipment solely to determine the location of a transmitter.

9.8. ~~(C)~~ FOREIGN COMMUNICATION means a communication that has at least one COMMUNICANT outside of the UNITED STATES, or that is entirely among FOREIGN POWERS or between a FOREIGN POWER and officials of a FOREIGN POWER, but does not include communications intercepted by ELECTRONIC SURVEILLANCE directed at premises in the UNITED STATES used predominantly for residential purposes.

9.9. (U) FOREIGN INTELLIGENCE means information relating to the capabilities, intentions, and activities of FOREIGN POWERS, organizations, or persons, and for purposes of this USSID includes both positive FOREIGN INTELLIGENCE and counterintelligence.

9.10. (U) FOREIGN POWER means:

a. A foreign government or any component thereof, whether or not recognized by the UNITED STATES,

b. A faction of a foreign nation or nations, not substantially composed of UNITED STATES PERSONS,

c. An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments,

d. A group engaged in INTERNATIONAL TERRORISM or activities in preparation therefor,

e. A foreign-based political organization, not substantially composed of UNITED STATES PERSONS, or

f. An entity that is directed and controlled by a foreign government or governments.

9.11. (U) INTERCEPTION means the acquisition by the USSS through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but does not include the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signal.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

9.12. (U) INTERNATIONAL TERRORISM means activities that:

a. Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the UNITED STATES or of any State, or that would be a criminal violation if committed within the jurisdiction of the UNITED STATES or any State, and

b. Appear to be intended:

(1) to intimidate or coerce a civilian population,

(2) to influence the policy of a government by intimidation or coercion, or

(3) to affect the conduct of a government by assassination or kidnapping, and

c. Occur totally outside the UNITED STATES, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

9.13. (U) PUBLICLY AVAILABLE INFORMATION means information that has been published or broadcast for general public consumption, is available on request to a member of the general public, has been seen or heard by a casual observer, or is made available at a meeting open to the general public.

9.14. ~~(C)~~ SELECTION, as applied to manual and electronic processing activities, means the intentional insertion of a [REDACTED] telephone number, [REDACTED] into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing.

9.15. ~~(C)~~ SELECTION TERM means the composite of individual terms used to effect or defeat SELECTION of particular communications for the purpose of INTERCEPTION. It comprises the entire term or series of terms so used, but not any segregable term contained therein. It applies to both electronic and manual processing.

9.16. (U) TARGET, OR TARGETING: See COLLECTION.

9.17. (U) UNITED STATES, when used geographically, includes the 50 states and the District of Columbia, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Northern Mariana Islands, and any other territory or possession over which the UNITED STATES exercises sovereignty.

9.18. ~~(C)~~ UNITED STATES PERSON:

a. A citizen of the UNITED STATES,

b. An alien lawfully admitted for permanent residence in the UNITED STATES,

c. Unincorporated groups and associations a substantial number of the members of which constitute a. or b. above, or

d. CORPORATIONS incorporated in the UNITED STATES, including U.S. flag nongovernmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

e. The following guidelines apply in determining whether a person is a U.S. PERSON:

(1) A person known to be currently in the United States will be treated as a U.S. PERSON unless that person is reasonably identified as an alien who has not been admitted for permanent residence or if the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a U.S. PERSON.

(2) A person known to be currently outside the UNITED STATES, or whose location is not known, will not be treated as a U.S. PERSON unless such person is reasonably identified as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a U.S. PERSON.

(3) A person known to be an alien admitted for permanent residence may be assumed to have lost status as a U.S. PERSON if the person leaves the UNITED STATES and it is known that the person is not in compliance with the administrative formalities provided by law (8 U.S.C. Section 1203) that enable such persons to reenter the UNITED STATES without regard to the provisions of law that would otherwise restrict an alien's entry into the UNITED STATES. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

(4) An unincorporated association whose headquarters are located outside the UNITED STATES may be presumed not to be a U.S. PERSON unless the USSS has information indicating that a substantial number of members are citizens of the UNITED STATES or aliens lawfully admitted for permanent residence.

(5) CORPORATIONS have the nationality of the nation-state in which they are incorporated. CORPORATIONS formed under U.S. federal or state law are thus U.S. persons, even if the corporate stock is foreign-owned. The only exception set forth above is CORPORATIONS which are openly acknowledged to be directed and controlled by foreign governments. Conversely, CORPORATIONS incorporated in foreign countries are not U.S. PERSONS even if that CORPORATION is a subsidiary of a U.S. CORPORATION.

(6) Nongovernmental ships and aircraft are legal entities and have the nationality of the country in which they are registered. Ships and aircraft fly the flag and are subject to the law of their place of registration.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~USSID 18
27 July 1993

ANNEX A

PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE
SURVEILLANCE ACT (U)

SECTION 1 - PURPOSE AND APPLICABILITY

1.1. (U) The Foreign Intelligence Surveillance Act (the Act) governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information. A complete copy of the Act is found at Annex B to NSA/CSS Directive 10-30. The Act covers the intentional collection of the communications of a particular, known U.S. person who is in the United States, all wiretaps in the United States, the acquisition of certain radio communications where all parties to that communication are located in the United States, and the monitoring of information in which there is a reasonable expectation of privacy. The Act requires that all such surveillances be directed only at foreign powers and their agents as defined by the Act and that all such surveillances be authorized by the United States Foreign Intelligence Surveillance Court, or in certain limited circumstances, by the Attorney General.

SECTION 2 - GENERAL

2.1. (U) Procedures and standards for securing Court orders or Attorney General certifications to conduct electronic surveillances are set forth in the Act. Requests for such orders or certifications should be forwarded by the appropriate Key Component through the NSA General Counsel to the Director, NSA/Chief, CSS and should be accompanied by a statement of the facts and circumstances justifying a belief that the target is a foreign power or an agent of a foreign power and that each of the facilities or places at which the surveillance will be directed are being used, or are about to be used, by that foreign power or agent. If the proposed surveillance meets the requirements of the Act and the Director approves the proposal, attorneys in the Office of the General Counsel will draw the necessary court application or request for Attorney General certification.

SECTION 3 - MINIMIZATION PROCEDURES

3.1. ~~(S-CCO)~~ Surveillances authorized by the Act are required to be carried out in accordance with the Act and pursuant to the court order or Attorney General certification authorizing that particular surveillance. In some cases, the court orders are tailored to address particular problems, and in those instances the NSA attorney will advise the appropriate NSA offices of the terms of the court's orders. In most cases, however, the court order will incorporate without any changes the standardized minimization procedures set forth in Appendix 1.

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

~~SECRET~~

USSID 18 ANNEX A
27 July 1993

SECTION 4 - RESPONSIBILITIES

4.1. (U) The General Counsel will review all requests to conduct electronic surveillances as defined by the Act, prepare all applications and materials required by the Act, and provide pertinent legal advice and assistance to all elements of the United States SIGINT System.

4.2. (U) The Inspector General will conduct regular inspections and oversight of all SIGINT activities to assure compliance with this Directive.

4.3. (U) All SIGINT managers and supervisors with responsibilities relating to the Act will ensure that they and their personnel are thoroughly familiar with the Act, its implementing procedures, and any court orders or Attorney General certifications pertinent to their mission. Personnel with duties related to the Act will consult the General Counsel's office for any required legal advice and assistance or training of newly assigned personnel. Appropriate records will be maintained demonstrating compliance with the terms of all court orders and Attorney General certifications, and any discrepancies in that regard will be promptly reported to the offices of the General Counsel and Inspector General.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~USSID 18 ANNEX A
27 July 1993

APPENDIX 1

Standard Minimization Procedures for
NSA Electronic Surveillances

Table of Contents

Section 1 — Applicability and Scope Section	A-1/2
Section 2 — Definitions	A-1/2
a. Acquisition	A-1/2
b. Communications concerning a U.S. Person	A-1/2
c. Communications of a U.S. Person	A-1/2
d. Consent	A-1/2
e. Foreign communication [Domestic Communication]	A-1/2
f. Identification of a U.S. Person	A-1/3
g. Processed or Processing	A-1/3
h. Publicly available information	A-1/3
i. Technical data base	A-1/3
j. U.S. person	A-1/3
Section 3 — Acquisition and Processing — General	A-1/3
a. Acquisition	A-1/3
b. Verification	A-1/3
c. Monitoring, Recording, and Processing	A-1/4
d. U.S. Persons Employed by the Foreign Power	A-1/4
e. Destruction of Raw Data	A-1/4
f. Non-Pertinent Communications	A-1/5
g. Change in Target's Location or Status	A-1/5
Section 4 — Acquisition and Processing — Special Procedures	A-1/5
a. Collection Against Residential Premises	A-1/5
b. Attorney-Client Communications	A-1/6
Section 5 — Domestic Communications	A-1/6
a. Dissemination	A-1/6
b. Retention	A-1/6
Section 6 — Foreign Communications of or Concerning U.S. Persons	A-1/7
a. Retention	A-1/7
b. Dissemination	A-1/7
Section 7 — Other Foreign Communications	A-1/8
Section 8 — Collaboration with Foreign Communications	A-1/8

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~

USSID 18 ANNEX A
APPENDIX 1
27 July 1993

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, DC

STANDARDIZED MINIMIZATION

PROCEDURES FOR NSA ELECTRONIC SURVEILLANCES

Pursuant to Section 101(h) of the Foreign Intelligence Surveillance Act of 1978 (hereinafter "the Act"), the following procedures have been adopted by the Attorney General and shall be followed by the NSA in implementing this electronic surveillance: (U)

SECTION 1 - APPLICABILITY AND SCOPE (U)

These procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is collected in the course of electronic surveillance as ordered by the United States Foreign Intelligence Surveillance Court under Section 102(b) or authorized by Attorney General Certification under Section 102(a) of the Act. These procedures also apply to non-United States persons where specifically indicated. (U)

SECTION 2 - DEFINITIONS (U)

In addition to the definitions in Section 101 of the Act, the following definitions shall apply to these procedures:

(a) Acquisition means the collection by NSA through electronic means of a nonpublic communication to which it is not an intended party. (U)

(b) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person. (U)

(c) Communications of a United States person include all communications to which a United States person is a party. (U)

(d) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization shall be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement. (U)

(e) Foreign communication means a communication that has at least one communicant outside of the United States, or that is entirely among:

- (1) foreign powers;
- (2) officers and employees of foreign powers; or
- (3) a foreign power and officers or employees of a foreign power.

All other communications are domestic communications. (S-CCO)

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~USSID 18 ANNEX A
APPENDIX 1
27 July 1993

(f) Identification of a United States person means the name, unique title, address, or other personal identifier of a United States person in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person. ~~(S-CCO)~~

(g) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. (U)

(h) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation. (U)

(i) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S-CCO)~~

(j) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person: (U)

(1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person. (U)

(2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person. (U)

(3) A person known to be an alien admitted for permanent residence loses status as a United States person if the person leaves the United States and is not in compliance with Title 8, United States Code, Section 1203 enabling re-entry into the United States. Failure to follow the statutory procedures provides a reasonable basis to conclude that the alien has abandoned any intention of maintaining his status as a permanent resident alien. (U)

(4) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence. (U)

SECTION 3 - ACQUISITION AND PROCESSING - GENERAL (U)

(a) Acquisition (U)

The acquisition of information by electronic surveillance shall be made in accordance with the certification of the Attorney General or the court order authorizing such surveillance and conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the surveillance. ~~(S-CCO)~~

(b) Verification (U)

At the initiation of the electronic surveillance, the NSA or the Federal Bureau of Investigation, if providing operational support, shall verify that the communication lines or telephone numbers being targeted are the lines or numbers of the target authorized by court order or Attorney General certification. Thereafter, collection personnel will monitor the acquisition of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications outside the authorized scope of the surveillance or information concerning United States persons not related to the purpose of the surveillance. ~~(S-CCO)~~

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18 ANNEX A
APPENDIX 1
27 July 1993

(c) Monitoring, Recording, and Processing (U)

(1) Electronic surveillance of the target may be monitored contemporaneously, recorded automatically, or both. (U)

(2) Personnel who monitor the electronic surveillance shall exercise reasonable judgement in determining whether particular information acquired must be minimized and shall destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either as clearly not relevant to the authorized purpose of the surveillance (e.g., the communication does not contain foreign intelligence information) or as containing evidence of a crime which may be disseminated under these procedures. ~~(S-CCO)~~

(3) Communications of or concerning United States persons that may be related to the authorized purpose of the surveillance may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, and 6 of these procedures. ~~(C)~~

(4) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S-CCO)~~

(5) Each communication shall be reviewed to determine whether it is a domestic or foreign communication to or from the targeted premises and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5 and 6 of these procedures. ~~(S-CCO)~~

(6) Magnetic tapes or other storage media containing foreign communications may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, shall not include United States person names or identifiers and shall be limited to those selection terms reasonably likely to identify [redacted] that are authorized for intentional collection under Executive Order 12333 implementing procedures. ~~(S-CCO)~~

(7) Further processing, retention and dissemination of foreign communications shall be made in accordance with Sections 4, 6, and 7, as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications shall be made in accordance with Sections 4 and 5 below. ~~(S-CCO)~~

(d) U.S. Persons Employed by the Foreign Power ~~(C)~~

Communications of or concerning United States persons employed by a foreign power may be used and retained as otherwise provided in these procedures except that:

(1) Such United States persons shall not be identified in connection with any communication that the person places or receives on behalf of another unless the identification is permitted under Section 6 of these procedures; and

(2) personal communications of United States persons that could not be foreign intelligence may only be retained, used, or disseminated in accordance with Section 5 of these procedures. ~~(S-CCO)~~

(e) Destruction of Raw Data ~~(C)~~

Communications and other information, including that reduced to graphic or "hard copy" form such as [redacted] shall be reviewed for retention in accordance with the standards set forth in these procedures. Communications and other information, in any form, that do not meet such retention standards and that are known to contain communications of or concerning United States persons shall be promptly destroyed. ~~(S-CCO)~~

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18 ANNEX A
APPENDIX I
27 July 1993

(f) Non-pertinent Communications (U)

(1) Communications determined to fall within established categories of non-pertinent communications, such as those set forth in subparagraph (6) of this section, should not be retained unless they contain information that may be disseminated under Sections 5, 6, or 7 below. (U)

(2) Monitors may listen to all communications, including those that initially appear to fall within established categories until they can reasonably determine that the communication cannot be disseminated under Sections 5, 6, or 7 below. ~~(S-CCO)~~

(3) Communications of United States persons will be analyzed to establish categories of communications that are not pertinent to the authorized purpose of the surveillance. (U)

(4) These categories should be established after a reasonable period of monitoring the communications of the targets. (U)

(5) Information that appears to be foreign intelligence may be retained even if it is acquired as a part of a communication falling within a category that is generally non-pertinent. ~~(S-CCO)~~

(6) Categories of non-pertinent communications which may be applied in these surveillance include:

- (i) Calls to and from United States Government officials;
- (ii) Calls to and from children;
- (iii) Calls to and from students for information to aid them in academic endeavors;
- (iv) Calls between family members; and
- (v) Calls relating solely to personal services, such as food orders, transportation,

etc. ~~(S-CCO)~~

(g) Change in Target's Location or Status ~~(S-CCO)~~

(1) During periods of known extended absence by a targeted agent of a foreign power from premises under surveillance, only communications to which the target is a party may be retained and disseminated. ~~(S-CCO)~~

(2) When there is reason to believe that the target of an electronic surveillance is no longer a foreign power or an agent of a foreign power, or no longer occupies the premises authorized for surveillance, that electronic surveillance shall be immediately terminated, and shall not resume unless subsequently approved under the Act. When any person involved in collection or processing of an electronic surveillance being conducted pursuant to the Act becomes aware of information tending to indicate a material change in the status or location of a target, the person shall immediately ensure that the NSA's Office of General Counsel is also made aware of such information. ~~(S-CCO)~~

SECTION 4 - ACQUISITION AND PROCESSING - SPECIAL PROCEDURES (U)

(a) Collection Against Residential Premises ~~(S-CCO)~~

(1) An electronic surveillance directed against premises located in the United States and used for residential purposes shall be conducted by technical means designed to limit the information acquired to communications that have one communicant outside the United States; [REDACTED]

The technical means employed shall consist of [REDACTED]

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

SECRETUSSID 18 ANNEX A
APPENDIX 1
27 July 1993

_____ equipment or equipment capable of identifying international _____
or other particular international communications known to be used by the targeted foreign power
and its agents. Communications to or from the target residential premises that are processed through a _____
_____ of a foreign power or agent of a
foreign power located in a foreign country, or on the foreign country or foreign city telephone direct dialing
codes (area codes) for the areas in which such foreign powers or agents are located. ~~(S-CCO)~~

(2) _____
_____~~(S-CCO)~~

(3) Domestic communications that are incidentally acquired during collection against residential
premises shall be handled under Section 5 of these procedures. ~~(S-CCO)~~

(b) Attorney-Client Communications ~~(S)~~

As soon as it becomes apparent that a communication is between a person who is known to be
under criminal indictment and an attorney who represents that individual in the matter under indictment (or
someone acting on behalf of the attorney), monitoring of that communication will cease and the communica-
tion shall be identified as an attorney-client communication in a log maintained for that purpose. The relevant
portion of the tape containing that conversation will be placed under seal and the Department of Justice, Office
of Intelligence Policy and Review, shall be notified so that appropriate procedures may be established to pro-
tect such communications from review or use in any criminal prosecution, while preserving foreign intelli-
gence information contained therein. ~~(S-CCO)~~

SECTION 5 - DOMESTIC COMMUNICATIONS (U)

(a) Dissemination (U)

Communications identified as domestic communications shall be promptly destroyed, except
that:

(1) domestic communications that are reasonably believed to contain foreign intelligence infor-
mation shall be disseminated to the Federal Bureau of Investigation (including United States person identi-
ties) for possible further dissemination by the Federal Bureau of Investigation in accordance with its minimiza-
tion procedures;

(2) domestic communications that do not contain foreign intelligence information, but that are
reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed, shall
be disseminated (including United States person identities) to appropriate Federal law enforcement authori-
ties, in accordance with Section 106(b) of the Act and crimes reporting procedures approved by the Secretary
of Defense and the Attorney General; and

(3) domestic communications that are reasonably believed to contain technical data base infor-
mation, as defined in Section 2(i), may be disseminated to the Federal Bureau of Investigation and to other
elements of the U.S. SIGINT system. ~~(S-CCO)~~

(b) Retention (U)

(1) Domestic communications disseminated to Federal law enforcement agencies may be re-
tained by the NSA for a reasonable period of time, not to exceed six months (or any shorter period set by court
order), to permit law enforcement agencies to determine whether access to original recordings of such com-
munications is required for law enforcement purposes. ~~(S-CCO)~~

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18 ANNEX A
APPENDIX 1
27 July 1993

(2) Domestic communications reasonably believed to contain technical data base information may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation. ~~(S-CCO)~~

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis. ~~(S-CCO)~~

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements. ~~(S-CCO)~~

SECTION 6 – FOREIGN COMMUNICATIONS OF OR CONCERNING UNITED STATES PERSONS (U)

(a) Retention (U)

Foreign communications of or concerning United States persons acquired by the NSA in the course of an electronic surveillance subject to these procedures may be retained only:

(1) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities. ~~(S-CCO)~~

(b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise dissemination of intelligence reports based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance; e.g., the identity of a senior official in the Executive Branch;

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18 ANNEX A
APPENDIX 1
27 July 1993

(3) the communication or information indicates that the United States person may be:

(A) an agent of a foreign power;

(B) a foreign power as defined in Section 101(a)(4) or (6) of the Act;

(C) residing outside the United States and holding an official position in the government or military forces of a foreign power;

(D) a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

(E) acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material.

(4) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information; but only after the agency that originated the information certifies that it is properly classified;

(6) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) the acquisition of the United States person's communication was authorized by a court order issued pursuant to Section 105 of the Act and the communication may relate to the foreign intelligence purpose of the surveillance;

(8) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed; provided that dissemination is for law enforcement purposes and is made in accordance with Section 106(b) of the Act and crimes reporting procedures approved by the Secretary of Defense and the Attorney General. (U)

SECTION 7 - OTHER FOREIGN COMMUNICATIONS (U)

Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy. (U)

SECTION 8 - COLLABORATION WITH FOREIGN GOVERNMENTS ~~(S-CCO)~~(a) The sharing or exchange of foreign communications governed by these procedures with signals intelligence authorities of collaborating foreign governments (Second Parties) may be undertaken by the NSA only with the written assurance of the Second Party that the use of those foreign communications will be subject to the retention and dissemination provisions of these procedures. ~~(S-CCO)~~(b) Domestic communications and communications to or from United States persons shall not be shared with Second Parties. ~~(S-CCO)~~(c) Foreign plain text communications may be shared with Second Parties if they are first reviewed by NSA analysts, who shall remove references to United States persons that are not necessary to understand or assess the foreign intelligence information contained therein. ~~(S-CCO)~~

(d) Foreign enciphered or encoded communications may be shared with Second Parties without such prior review, provided that at least annually a representative sampling of those shared communications that can be deciphered or decoded is reviewed by the NSA to ensure that any references therein to United States persons are necessary to understand or assess the foreign intelligence information being disseminated.

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~

USSID 18 ANNEX A
APPENDIX 1
27 July 1993

nated. Corrective measures with respect to each target or line shall be undertaken as necessary to maintain compliance with the above dissemination standard. The results of each review shall be made available to the Attorney General or a designee. ~~(S-CCO)~~

Approved by Attorney General Janet Reno on 1 July 1997

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

USSID 18
27 July 1993

ANNEX B

OPERATIONAL ASSISTANCE TO THE FEDERAL BUREAU OF INVESTIGATION (U)

SECTION 1 - GENERAL

1.1. (U) In accordance with the provisions of Section 2.6 of E.O. 12333, and the NSA/FBI Memorandum of Understanding of 25 November 1980, the National Security Agency may provide specialized equipment and technical knowledge to the FBI to assist the FBI in the conduct of its lawful functions. When requesting such assistance, the FBI will certify to the General Counsel of NSA that such equipment or technical knowledge is necessary to the accomplishment of one or more of the FBI's lawful functions.

1.2. (U) NSA may also provide expert personnel to assist FBI personnel in the operation or installation of specialized equipment when that equipment is to be employed to collect foreign intelligence. When requesting the assistance of expert personnel, the FBI will certify to the General Counsel that such assistance is necessary to collect foreign intelligence and that the approval of the Attorney General (and, when necessary, a warrant from a court of competent jurisdiction) has been obtained.

SECTION 2 - CONTROL

2.1. (U) No operational assistance as discussed in Section 1 shall be provided without the express permission of the Director, NSA/Chief, CSS, Deputy Director, NSA, the Deputy Director for Operations, or the Deputy Director for Technology and Systems. The Deputy Director for Operations and the Deputy Director for Technology and Systems may approve requests for such assistance only with the concurrence of the General Counsel.

~~FOR OFFICIAL USE ONLY~~

~~CONFIDENTIAL~~

USSID 18
27 July 1993

ANNEX C

SIGNALS INTELLIGENCE SUPPORT TO U.S. AND ALLIED MILITARY EXERCISE COMMAND AUTHORITIES (U)

SECTION 1 - POLICY

1.1. ~~(C)~~ Signals Intelligence support to U.S. and Allied military exercise command authorities is provided for in USSID 56 and DoD Directive 5200.17 (M-2). Joint Chiefs of Staff Memorandum MJCS111-88, 18 August 1988, and USSID 4, 16 December, 1988, establish doctrine and procedures for providing signals intelligence support to military commanders. The procedures in this Annex provide policy guidelines for safeguarding the rights of U.S. persons in the conduct of exercise SIGINT support activities.

SECTION 2 - DEFINITIONS

2.1. (U) The term "Military Tactical Communications" means United States and Allied military exercise communications, within the United States and abroad, that are necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.

SECTION 3 - PROCEDURES

3.1. ~~(C-ECO)~~ The USSS may collect, process, store, and disseminate military tactical communications that are also communications of, or concerning, U.S. persons.

a. Collection efforts will be conducted in such a manner as to avoid, to the extent feasible, the intercept of non-exercise-related communications.

b. Military tactical communications may be stored and processed without deletion of references to U.S. persons if the names and communications of the U.S. persons who are exercise participants, whether military, government, or contractor, are contained in, or such communications constitute, exercise-related communications or fictitious communications or information prepared for the exercise.

c. Communications of U.S. persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible, provided that a record describing the signal or frequency user in technical and generic terms may be retained for signal identification and Collection-avoidance purposes. Inadvertently intercepted communications that contain anomalies in enciphered communications that reveal a potential vulnerability to United States communications security should be forwarded to the NSA Deputy Director for Information Systems Security.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

USSID 18 ANNEX C
27 July 1993

d. Dissemination of military exercise communications, exercise reports, or information files derived from such communications shall be limited to those authorities and persons participating in the exercise or conducting reviews and critiques thereof.

~~CONFIDENTIAL~~

USSID 18
27 July 1993

ANNEX D

TESTING OF ELECTRONIC EQUIPMENT (U)

SECTION 1 - PURPOSE AND APPLICABILITY

1.1. (U) This Annex applies to the testing of electronic equipment that has the capability to intercept communications and other non-public information. Testing includes development, calibration, and evaluation of such equipment, and will be conducted, to the maximum extent practical, without interception or monitoring of U.S. persons.

SECTION 2 - PROCEDURES

2.1. (U) The USSS may test electronic equipment that has the capability to intercept communications and other information subject to the following limitations:

a. To the maximum extent practical, the following should be used:

- (1) Laboratory-generated signals,
- (2) Communications transmitted between terminals located outside the United States not used by any known U.S. person,
- (3) Official government agency communications with the consent of an appropriate official of that agency, or an individual's communications with the consent of that individual,
- (4) Public broadcast signals, or
- (5) Other communications in which there is no reasonable expectation of privacy (as approved in each instance by the NSA General Counsel).

b. Where it is not practical to test electronic equipment solely against signals described in paragraph 2.1.a., above, testing may be conducted, provided:

- (1) the proposed test is coordinated with the NSA General Counsel;
- (2) the test is limited in scope and duration to that necessary to determine the capability of the equipment;
- (3) no particular person is targeted without consent and it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance; and
- (4) the test does not exceed 90 calendar days.

~~FOR OFFICIAL USE ONLY~~

USSID 18 ANNEX D
27 July 1993

c. Where the test involves communications other than those identified in 2.1 .a. and a test period longer than 90 days is required, the Foreign Intelligence Surveillance Act requires that the test be approved by the Attorney General. Such proposals and plans shall be submitted by USSS elements through the General Counsel, NSA, to the Director, NSA/Chief, CSS for transmission to the Attorney General. The test proposal shall state the requirement for an extended test involving such communications, the nature of the test, the organization that will conduct the test, and the proposed disposition of any signals or communications acquired during the test.

2.2. (U) The content of any communication other than communications between non-U.S. persons outside the United States which are acquired during a test and evaluation shall be:

a. retained and used only for the purpose of determining the capability of the electronic equipment;

b. disclosed only to persons conducting or evaluating the test; and

c. destroyed before or immediately upon completion of the testing.

2.3. (U) The technical parameters of a communication, such as frequency, modulation, and time of activity of acquired electronic signals, may be retained and used for test reporting or collection-avoidance purposes. Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance, provided such dissemination and use are limited to testing, evaluation, or collection-avoidance purposes.

~~FOR OFFICIAL USE ONLY~~

~~SECRET~~

USSID 18
27 July 1993

ANNEX E

SEARCH AND DEVELOPMENT OPERATIONS (U)

SECTION 1 - PROCEDURES

1.1. (U) This Annex provides the procedures for safeguarding the rights of U.S. persons when conducting SIGINT search and development activities.

1.2. ~~(S-CCO)~~ The USSS may conduct search and development activities with respect to signals throughout the radio spectrum under the following limitations:

a. Signals may be collected only for the purpose of identifying those signals that:

(1) may contain information related to the production of foreign intelligence or counterintelligence;

(2) are enciphered or appear to contain secret meaning;

(3) are necessary to assure efficient signals intelligence collection or to avoid the collection of unwanted signals; or,

(4) reveal vulnerabilities of United States communications security.

b. Communications originated or intended for receipt in the United States or originated or intended for receipt by U.S. persons shall be processed in accordance with Section 5 of USSID 18, provided that information necessary for cataloging the constituent elements of the signal environment may be processed and retained if such information does not identify a U.S. person. Information revealing a United States communications security vulnerability may be retained.

c. Information necessary for cataloging the constituent elements of the signal environment may be disseminated to the extent such information does not identify U.S. persons. Communications equipment nomenclature may be disseminated. Information that reveals a vulnerability to United States communications security may be disseminated to the appropriate communications security authorities.

d. All information obtained in the process of search and development that appears to be of foreign intelligence value may be forwarded to the proper analytic office within NSA for processing and dissemination in accordance with relevant portions of USSID 18.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~CONFIDENTIAL~~

USSID 18
27 July 1993

ANNEX F

ILLICIT COMMUNICATIONS (C)

SECTION 1 - PROCEDURES

1.1. ~~(C)~~ The USSS may collect, retain, process, and disseminate illicit communications without reference to the requirements concerning U.S. persons.

1.2. ~~(C)~~ The term "illicit communications" means a communication transmitted in violation of either the Communications Act of 1934 and regulations issued thereunder or international agreements, which because of its explicit content, message characteristics, or method of transmission, is reasonably believed to be a communication to or from an agent or agents of foreign powers, whether or not U.S. persons.

~~CONFIDENTIAL~~

USSID 18
27 July 1993

ANNEX G

TRAINING OF PERSONNEL IN THE OPERATION AND USE OF SIGINT COLLECTION AND OTHER SURVEILLANCE EQUIPMENT (U)

SECTION 1 - APPLICABILITY

1.1. (U) This Annex applies to all USSS use of SIGINT collection and other surveillance equipment for training purposes.

SECTION 2 - POLICY

2.1. (U) Training of USSS personnel in the operation and use of SIGINT collection equipment shall be conducted, to the maximum extent that is practical, without interception of the communications of U.S. persons or persons in the United States who have not given consent to such interception. Communications and information protected by the Foreign Intelligence Surveillance Act (FISA) (see Annex A) will not be collected for training purposes.

SECTION 3 - PROCEDURES

3.1. (U) The training of USSS personnel in the operation and use of SIGINT collection and other surveillance equipment shall include guidance concerning the requirements and restrictions of the FISA, Executive Order 12333, and USSID 18.

3.2. (U) The use of SIGINT collection and other surveillance equipment for training purposes is subject to the following limitations:

a. To the maximum extent practical, use of such equipment for training purposes shall be directed against otherwise authorized intelligence targets;

b. The contents of private communications of nonconsenting U.S. persons may not be acquired unless the person is an authorized target of electronic surveillance; and

c. The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.

3.3. (U) The limitations in paragraph 3.2. do not apply in the following instances:

a. Public broadcasts, distress signals, or official United States Government communications may be monitored, provided that, where government agency communications are monitored, the consent of an appropriate official is obtained; and

USSID 18 ANNEX G
27 July 1993

b. Minimal acquisition of information is permitted as required for calibration purposes.

3.4. (U) Information collected during training that involves authorized intelligence targets may be retained in accordance with Section 6 of USSID 18 and disseminated in accordance with Section 7 of USSID 18. Information other than distress signals collected during training that does not involve authorized intelligence targets or that is acquired inadvertently shall be destroyed as soon as practical or upon completion of the training and may not be disseminated outside the USSS for any purpose. Distress signals should be referred to the DDO.

~~FOR OFFICIAL USE ONLY~~

USSID 18
27 July 1993

ANNEX H
CONSENT FORMS (U)

SECTION 1 - PURPOSE

1.1. (U) The forms set forth in this Annex are for use in recording consent by U.S. persons for USSS elements to collect and disseminate foreign communications concerning that person. The first form is consent to collect and disseminate a U.S. person's communications as well as references to that person in foreign communications. The second form is consent to collect and disseminate only references to the U.S. person and does not include communications to or from that person.

1.2. (U) Section 4.1.c. of USSID 18 states that the Director, NSA/Chief, CSS has authority to approve the consensual collection of communications to, from or about U.S. persons. Elements of the USSS proposing to conduct consensual collection should forward a copy of the executed consent form and any pertinent information to the Director, NSA/Chief, CSS for approval.

1.3. (U) The forms provided on the following pages may be reproduced, provided the security classifications (top and bottom) are removed. It is the responsibility of the user to properly reclassify the document in accordance with requisite security guidelines.

~~SECRET~~

USSID 18 ANNEX H
27 July 1993

CONSENT AGREEMENT

SIGNALS INTELLIGENCE COVERAGE

I, _____, hereby consent to the National Security Agency undertaking to seek and disseminate communications to or from or referencing me in foreign communications for the purpose of _____

This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent, as well as to any signals intelligence reports that may relate to the purpose stated above.

Except as otherwise provided by Executive Order 12333 procedures, this consent covers only information that relates to the purpose stated above and is effective for the period _____ to _____.

Signals intelligence reports containing information derived from communications to or from me may only be disseminated to me and to _____. Signals intelligence reports containing information derived from communications referencing me may only be disseminated to me and to _____ except as otherwise permitted by procedures under Executive Order 12333.

(SIGNATURE)

(TITLE)

(DATE)

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~

USSID 18 ANNEX H
27 July 1993

CONSENT AGREEMENT

SIGNALS INTELLIGENCE COVERAGE

I, _____, hereby consent to the National Security Agency undertaking to seek and disseminate references to me in foreign communications for the purpose of _____

This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent, as well as to any signals intelligence reports that may relate to the purpose stated above.

Except as otherwise provided by Executive Order 12333 procedures, this consent covers only references to me in foreign communications and information therefrom that relates to the purpose stated above and is effective for the period _____ to _____

Signals intelligence reports containing information derived from communications referencing me and related to the purpose stated above may only be disseminated to me and to _____ except as otherwise permitted by procedures under Executive Order 12333.

(SIGNATURE)

(TITLE)

(DATE)

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

ANNEX I

FORM FOR CERTIFICATION OF
OPENLY ACKNOWLEDGED ENTITIES ~~(S-CCO)~~

The form below should be used for Director approvals for the collection of communications of entities that are openly acknowledged to be directed and controlled by a foreign power as specified in Section 4.1.c.(3) of USSID 18.

DIRECTOR, NSA/CHIEF, CSS

Certification for Openly Acknowledged Entities Under
Section 4.A.1.(b) of the Classified Annex
to DOD 5240.1R

Certification to the Attorney General:

~~(S-CCO)~~ The Director, NSA, hereby certifies that [REDACTED] located in the United States and openly acknowledged to be directed and controlled by (Government X), is a new target of collection. The purpose of the surveillance is (to collect intelligence regarding Government X) in accordance with valid intelligence requirements. The surveillance will entail intentional interception or deliberate selection of the target's international communications. Standard minimization procedures will be applied to any information collected that relates to U.S. persons.

Director, NSA/Chief, CSS

Copy to: Deputy Secretary of Defense

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

~~SECRET~~

USSID 18
27 July 1993

ANNEX K

[REDACTED]
[REDACTED] (S-CCO)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(S-CCO)

[REDACTED]

[REDACTED]

[REDACTED]

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

Exhibit B

Exhibit B

LIBERTY AND SECURITY IN A CHANGING WORLD

12 December 2013

**Report and Recommendations of
The President's Review Group on Intelligence
and Communications Technologies**

This page has been intentionally left blank.

Transmittal Letter

Dear Mr. President:

We are honored to present you with the Final Report of the Review Group on Intelligence and Communications Technologies. Consistent with your memorandum of August 27, 2013, our recommendations are designed to protect our national security and advance our foreign policy while also respecting our longstanding commitment to privacy and civil liberties, recognizing our need to maintain the public trust (including the trust of our friends and allies abroad), and reducing the risk of unauthorized disclosures.

We have emphasized the need to develop principles designed to create strong foundations for the future. Although we have explored past and current practices, and while that exploration has informed our recommendations, this Report should not be taken as a general review of, or as an attempt to provide a detailed assessment of, those practices. Nor have we generally engaged budgetary questions (although some of our recommendations would have budgetary implications).

We recognize that our forty-six recommendations, developed over a relatively short period of time, will require careful assessment by a wide range of relevant officials, with close reference to the likely consequences. Our goal has been to establish broad understandings and principles that

can provide helpful orientation during the coming months, years, and decades.

We are hopeful that this Final Report might prove helpful to you, to Congress, to the American people, and to leaders and citizens of diverse nations during continuing explorations of these important questions.

Richard A. Clarke

Michael J. Morell

Geoffrey R. Stone

Cass R. Sunstein

Peter Swire

Acknowledgements

The Review Group would like to thank the many people who supported our efforts in preparing this Report. A number of people were formally assigned to assist the Group, and all performed with professionalism, hard work, and good cheer. These included Brett Freedman, Kenneth Gould, and other personnel from throughout the government. We thank as well the many other people both inside and outside of the government who have contributed their time and energy to assisting in our work.

This page has been intentionally left blank.

Table of Contents

Preface

Executive Summary

Recommendations

Chapter I: Principles

Chapter II: Lessons of History

- A. The Continuing Challenge
- B. The Legal Framework as of September 11, 2001
- C. September 11 and its Aftermath
- D. The Intelligence Community

Chapter III: Reforming Foreign Intelligence Surveillance Directed at United States Persons

- A. Introduction
- B. Section 215: Background
- C. Section 215 and "Ordinary" Business Records

- D. National Security Letters
- E. Section 215 and the Bulk Collection of Telephony Meta-data
 - 1. The Program
 - 2. The Mass Collection of Personal Information
 - 3. Is Meta-data Different?
- F. Secrecy and Transparency

Chapter IV: Reforming Foreign Intelligence Surveillance Directed at Non-United States Persons

- A. Introduction
- B. Foreign Intelligence Surveillance and Section 702
- C. Privacy Protections for United States Persons Whose Communications are Intercepted Under Section 702
- D. Privacy Protections for Non-United States Persons

Chapter V: Determining What Intelligence Should Be Collected and How

- A. Priorities and Appropriateness
- B. Monitoring Sensitive Collection
- C. Leadership Intentions

- D. Cooperation with Our Allies

Chapter VI: Organizational Reform in Light of Changing Communications Technology

- A. Introduction
- B. The National Security Agency
 - 1. “Dual-Use” Technologies: The Convergence of Civilian Communications and Intelligence Collection
 - 2. Specific Organizational Reforms
- C. Reforming Organizations Dedicated to the Protection of Privacy and Civil Liberties
- D. Reforming the FISA Court

Chapter VII: Global Communications Technology: Promoting Prosperity, Security, and Openness in a Networked World

- A. Introduction
- B. Background: Trade, Internet Freedom, and Other Goals
 - 1. International Trade and Economic Growth
 - 2. Internet Freedom

3. Internet Governance and Localization Requirements
- C. Technical Measures to Increase Security and User Confidence
- D. Institutional Measures for Cyberspace
- E. Addressing Future Technological Challenges

Chapter VIII. Protecting What We Do Collect

- A. Personnel Vetting and Security Clearances
 1. How the System Works Now
 2. How the System Might be Improved
 3. Information Sharing
- B. Network Security
 1. Executive Order 13578
 2. Physical and Logical Separation
- C. Cost-Benefit Analysis and Risk Management

Conclusion

Appendix A: The Legal Standards for Government Access to Communications

Appendix B: Overview of NSA Privacy Protections Under FAA 702

Overview of NSA Privacy Protections Under EO 12333

Appendix C: US Intelligence: Multiple Layers of Rules and Oversight

Appendix D: Avenues for Whistle-blowers in the Intelligence
Community

Appendix E: US Government Role in Current Encryption Standards

Appendix F: Review Group Briefings and Meetings

Appendix G: Glossary

Preface

On August 27, 2013, the President announced the creation of the Review Group on Intelligence and Communications Technologies. The immediate backdrop for our work was a series of disclosures of classified information involving foreign intelligence collection by the National Security Agency. The disclosures revealed intercepted collections that occurred inside and outside of the United States and that included the communications of United States persons and legal permanent residents, as well as non-United States persons located outside the United States. Although these disclosures and the responses and concerns of many people in the United States and abroad have informed this Report, we have focused more broadly on the creation of sturdy foundations for the future, safeguarding (as our title suggests) liberty and security in a rapidly changing world.

Those rapid changes include unprecedented advances in information and communications technologies; increased globalization of trade, investment, and information flows; and fluid national security threats against which the American public rightly expects its government to provide protection. With this larger context in mind, we have been mindful of significant recent changes in the environment in which intelligence collection takes place.

For example, traditional distinctions between “foreign” and “domestic” are far less clear today than in the past, now that the same communications devices, software, and networks are used globally by

friends and foes alike. These changes, as well as changes in the nature of the threats we face, have implications for the right of privacy, our strategic relationships with other nations, and the levels of innovation and information-sharing that underpin key elements of the global economy.

In addressing these issues, the United States must pursue multiple and often competing goals at home and abroad. In facing these challenges, the United States must take into account the full range of interests and values that it is pursuing, and it must communicate these goals to the American public and to key international audiences. These goals include:

Protecting The Nation Against Threats to Our National Security.

The ability of the United States to combat threats from state rivals, terrorists, and weapons proliferators depends on the acquisition of foreign intelligence information from a broad range of sources and through a variety of methods. In an era increasingly dominated by technological advances in communications technologies, the United States must continue to collect signals intelligence globally in order to assure the safety of our citizens at home and abroad and to help protect the safety of our friends, our allies, and the many nations with whom we have cooperative relationships.

Promoting Other National Security and Foreign Policy Interests.

Intelligence is designed not only to protect against threats but also to safeguard a wide range of national security and foreign policy interests, including counterintelligence, counteracting the international elements of

organized crime, and preventing drug trafficking, human trafficking, and mass atrocities.

Protecting the Right to Privacy. The right to privacy is essential to a free and self-governing society. The rise of modern technologies makes it all the more important that democratic nations respect people's fundamental right to privacy, which is a defining part of individual security and personal liberty.

Protecting Democracy, Civil Liberties, and the Rule of Law. Free debate within the United States is essential to the long-term vitality of American democracy and helps bolster democracy globally. Excessive surveillance and unjustified secrecy can threaten civil liberties, public trust, and the core processes of democratic self-government. All parts of the government, including those that protect our national security, must be subject to the rule of law.

Promoting Prosperity, Security, and Openness in a Networked World. The United States must adopt and sustain policies that support technological innovation and collaboration both at home and abroad. Such policies are central to economic growth, which is promoted in turn by economic freedom and spurring entrepreneurship. For this reason, the United States must continue to establish and strengthen international norms of Internet freedom and security.

Protecting Strategic Alliances. The collection of intelligence must be undertaken in a way that preserves and strengthens our strategic relationships. We must be respectful of those relationships and of the

leaders and citizens of other nations, especially those with whom we share interests, values, or both. The collection of intelligence should be undertaken in a way that recognizes the importance of cooperative relationships with other nations and that respects the legitimate privacy interests and the dignity of those outside our borders.

The challenge of managing these often competing goals is daunting. But it is a challenge that the nation must meet if it is to live up to its promises to its citizens and to posterity.

Executive Summary

Overview

The national security threats facing the United States and our allies are numerous and significant, and they will remain so well into the future. These threats include international terrorism, the proliferation of weapons of mass destruction, and cyber espionage and warfare. A robust foreign intelligence collection capability is essential if we are to protect ourselves against such threats. Because our adversaries operate through the use of complex communications technologies, the National Security Agency, with its impressive capabilities and talented officers, is indispensable to keeping our country and our allies safe and secure.

At the same time, the United States is deeply committed to the protection of privacy and civil liberties—fundamental values that can be and at times have been eroded by excessive intelligence collection. After careful consideration, we recommend a number of changes to our intelligence collection activities that will protect these values without undermining what we need to do to keep our nation safe.

Principles

We suggest careful consideration of the following principles:

- 1. The United States Government must protect, at once, two different forms of security: national security and personal privacy.*

In the American tradition, the word “security” has had multiple meanings. In contemporary parlance, it often refers to *national security* or *homeland security*. One of the government’s most fundamental responsibilities is to protect this form of security, broadly understood. At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: “The right of the people to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ” (emphasis added). Both forms of security must be protected.

2. The central task is one of risk management; multiple risks are involved, and all of them must be considered.

When public officials acquire foreign intelligence information, they seek to reduce risks, above all risks to national security. The challenge, of course, is that multiple risks are involved. Government must consider all of those risks, not a subset, when it is creating sensible safeguards. In addition to reducing risks to national security, public officials must consider four other risks:

- Risks to privacy;
- Risks to freedom and civil liberties, on the Internet and elsewhere;
- Risks to our relationships with other nations; and
- Risks to trade and commerce, including international commerce.

3. The idea of "balancing" has an important element of truth, but it is also inadequate and misleading.

It is tempting to suggest that the underlying goal is to achieve the right "balance" between the two forms of security. The suggestion has an important element of truth. But some safeguards are not subject to balancing at all. In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, and gender.

4. The government should base its decisions on a careful analysis of consequences, including both benefits and costs (to the extent feasible).

In many areas of public policy, officials are increasingly insistent on the need for careful analysis of the consequences of their decisions, and on the importance of relying not on intuitions and anecdotes, but on evidence and data. Before they are undertaken, surveillance decisions should depend (to the extent feasible) on a careful assessment of the anticipated consequences, including the full range of relevant risks. Such decisions should also be subject to continuing scrutiny, including retrospective analysis, to ensure that any errors are corrected.

Surveillance of US Persons

With respect to surveillance of US Persons, we recommend a series of significant reforms. Under section 215 of the Foreign Intelligence Surveillance Act (FISA), the government now stores bulk telephony meta-data, understood as information that includes the telephone numbers that both originate and receive calls, time of call, and date of call. (Meta-data does not include the content of calls.). We recommend that Congress should end such storage and transition to a system in which such meta-data is held privately for the government to query when necessary for national security purposes.

In our view, the current storage by the government of bulk meta-data creates potential risks to public trust, personal privacy, and civil liberty. We recognize that the government might need access to such meta-data, which should be held instead either by private providers or by a private third party. This approach would allow the government access to the relevant information when such access is justified, and thus protect national security without unnecessarily threatening privacy and liberty. Consistent with this recommendation, we endorse a broad principle for the future: as a general rule and without senior policy review, the government should not be permitted to collect and store mass, undigested, non-public personal information about US persons for the purpose of enabling future queries and data-mining for foreign intelligence purposes.

We also recommend specific reforms that will provide Americans with greater safeguards against intrusions into their personal domain. We

endorse new steps to protect American citizens engaged in communications with non-US persons. We recommend important restrictions on the ability of the Foreign Intelligence Surveillance Court (FISC) to compel third parties (such as telephone service providers) to disclose private information to the government. We endorse similar restrictions on the issuance of National Security Letters (by which the Federal Bureau of Investigation now compels individuals and organizations to turn over certain otherwise private records), recommending prior judicial review except in emergencies, where time is of the essence.

We recommend concrete steps to promote transparency and accountability, and thus to promote public trust, which is essential in this domain. Legislation should be enacted requiring information about surveillance programs to be made available to the Congress and to the American people to the greatest extent possible (subject only to the need to protect classified information). We also recommend that legislation should be enacted authorizing telephone, Internet, and other providers to disclose publicly general information about orders they receive directing them to provide information to the government. Such information might disclose the number of orders that providers have received, the broad categories of information produced, and the number of users whose information has been produced. In the same vein, we recommend that the government should publicly disclose, on a regular basis, general data about the orders it has issued in programs whose existence is unclassified.

Surveillance of Non-US Persons

Significant steps should be taken to protect the privacy of non-US persons. In particular, any programs that allow surveillance of such persons even outside the United States should satisfy six separate constraints. They:

- 1) must be authorized by duly enacted laws or properly authorized executive orders;
- 2) must be directed *exclusively* at protecting national security interests of the United States or our allies;
- 3) must *not* be directed at illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries;
- 4) must not target any non-United States person based solely on that person's political views or religious convictions;
- 5) must not disseminate information about non-United States persons if the information is not relevant to protecting the national security of the United States or our allies; and
- 6) must be subject to careful oversight and to the highest degree of transparency consistent with protecting the national security of the United States and our allies.

We recommend that, in the absence of a specific and compelling showing, the US Government should follow the model of the Department of Homeland Security and apply the Privacy Act of 1974 in the same way to both US persons and non-US persons.

Setting Priorities and Avoiding Unjustified or Unnecessary Surveillance

To reduce the risk of unjustified, unnecessary, or excessive surveillance in foreign nations, including collection on foreign leaders, we recommend that the President should create a new process, requiring highest-level approval of all sensitive intelligence requirements and the methods that the Intelligence Community will use to meet them. This process should identify both the uses and the limits of surveillance on foreign leaders and in foreign nations.

We recommend that those involved in the process should consider whether (1) surveillance is motivated by especially important national security concerns or by concerns that are less pressing and (2) surveillance would involve leaders of nations with whom we share fundamental values and interests or leaders of other nations. With close reference to (2), we recommend that with a small number of closely allied governments, meeting specific criteria, the US Government should explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens (including, if and where appropriate, intentions, strictures, or limitations with respect to collections).

Organizational Reform

We recommend a series of organizational changes. With respect to the National Security Agency (NSA), we believe that the Director should be a Senate-confirmed position, with civilians eligible to hold that position; the President should give serious consideration to making the next Director of NSA a civilian. NSA should be clearly designated as a foreign intelligence organization. Other missions (including that of NSA's Information Assurance Directorate) should generally be assigned elsewhere. The head of the military unit, US Cyber Command, and the Director of NSA should not be a single official.

We favor a newly chartered, strengthened, independent Civil Liberties and Privacy Protection Board (CLPP Board) to replace the Privacy and Civil Liberties Oversight Board (PCLOB). The CLPP Board should have broad authority to review government activity relating to foreign intelligence and counterterrorism whenever that activity has implications for civil liberties and privacy. A Special Assistant to the President for Privacy should also be designated, serving in both the Office of Management and Budget and the National Security Staff. This Special Assistant should chair a Chief Privacy Officer Council to help coordinate privacy policy throughout the Executive branch.

With respect to the FISC, we recommend that Congress should create the position of Public Interest Advocate to represent the interests of privacy and civil liberties before the FISC. We also recommend that the government should take steps to increase the transparency of the FISC's

decisions and that Congress should change the process by which judges are appointed to the FISC.

Global Communications Technology

Substantial steps should be taken to protect prosperity, security, and openness in a networked world. A free and open Internet is critical to both self-government and economic growth. The United States Government should reaffirm the 2011 International Strategy for Cyberspace. It should stress that Internet governance must not be limited to governments, but should include all appropriate stakeholders, including businesses, civil society, and technology specialists.

The US Government should take additional steps to promote security, by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage. Among other measures relevant to the Internet, the US Government should also support international norms or agreements to increase confidence in the security of online communications.

For big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are statistically reliable, cost-effective, and protective of privacy and civil liberties.

Protecting What We Do Collect

We recommend a series of steps to reduce the risks associated with “insider threats.” A governing principle is plain: Classified information should be shared only with those who genuinely need to know. We recommend specific changes to improve the efficacy of the personnel vetting system. The use of “for-profit” corporations to conduct personnel investigations should be reduced or terminated. Security clearance levels should be further differentiated. Departments and agencies should institute a Work-Related Access approach to the dissemination of sensitive, classified information. Employees with high-level security clearances should be subject to a Personnel Continuous Monitoring Program. Ongoing security clearance vetting of individuals should use a risk-management approach and depend on the sensitivity and quantity of the programs and information to which individuals are given access.

The security of information technology networks carrying classified information should be a matter of ongoing concern by Principals, who should conduct an annual assessment with the assistance of a “second opinion” team. Classified networks should increase the use of physical and logical separation of data to restrict access, including through Information Rights Management software. Cyber-security software standards and practices on classified networks should be at least as good as those on the most secure private-sector enterprises.

Recommendations

Recommendation 1

We recommend that section 215 should be amended to authorize the Foreign Intelligence Surveillance Court to issue a section 215 order compelling a third party to disclose otherwise private information about particular individuals only if:

- (1) it finds that the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities” and
- (2) like a subpoena, the order is reasonable in focus, scope, and breadth.

Recommendation 2

We recommend that statutes that authorize the issuance of National Security Letters should be amended to permit the issuance of National Security Letters only upon a judicial finding that:

- (1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities” and
- (2) like a subpoena, the order is reasonable in focus, scope, and breadth.

Recommendation 3

We recommend that all statutes authorizing the use of National Security Letters should be amended to require the use of the same oversight, minimization, retention, and dissemination standards that currently govern the use of section 215 orders.

Recommendation 4

We recommend that, as a general rule, and without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes. Any program involving government collection or storage of such data must be narrowly tailored to serve an important government interest.

Recommendation 5

We recommend that legislation should be enacted that terminates the storage of bulk telephony meta-data by the government under section 215, and transitions as soon as reasonably possible to a system in which such meta-data is held instead either by private providers or by a private third party. Access to such data should be permitted only with a section 215 order from the Foreign Intelligence Surveillance Court that meets the requirements set forth in Recommendation 1.

Recommendation 6

We recommend that the government should commission a study of the legal and policy options for assessing the distinction between meta-data and other types of information. The study should include

technological experts and persons with a diverse range of perspectives, including experts about the missions of intelligence and law enforcement agencies and about privacy and civil liberties.

Recommendation 7

We recommend that legislation should be enacted requiring that detailed information about authorities such as those involving National Security Letters, section 215 business records, section 702, pen register and trap-and-trace, and the section 215 bulk telephony meta-data program should be made available on a regular basis to Congress and the American people to the greatest extent possible, consistent with the need to protect classified information. With respect to authorities and programs whose existence is unclassified, there should be a strong presumption of transparency to enable the American people and their elected representatives independently to assess the merits of the programs for themselves.

Recommendation 8

We recommend that:

- (1) legislation should be enacted providing that, in the use of National Security Letters, section 215 orders, pen register and trap-and-trace orders, 702 orders, and similar orders directing individuals, businesses, or other institutions to turn over information to the government, non-disclosure orders may be issued only upon a judicial finding that there are reasonable grounds to believe that disclosure would significantly threaten

the national security, interfere with an ongoing investigation, endanger the life or physical safety of any person, impair diplomatic relations, or put at risk some other similarly weighty government or foreign intelligence interest;

- (2) nondisclosure orders should remain in effect for no longer than 180 days without judicial re-approval; and
- (3) nondisclosure orders should never be issued in a manner that prevents the recipient of the order from seeking legal counsel in order to challenge the order's legality.

Recommendation 9

We recommend that legislation should be enacted providing that, even when nondisclosure orders are appropriate, recipients of National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders issued in programs whose existence is unclassified may publicly disclose on a periodic basis general information about the number of such orders they have received, the number they have complied with, the general categories of information they have produced, and the number of users whose information they have produced in each category, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

Recommendation 10

We recommend that, building on current law, the government should publicly disclose on a regular basis general data about National

Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders in programs whose existence is unclassified, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

Recommendation 11

We recommend that the decision to keep secret from the American people programs of the magnitude of the section 215 bulk telephony meta-data program should be made only after careful deliberation at high levels of government and only with due consideration of and respect for the strong presumption of transparency that is central to democratic governance. A program of this magnitude should be kept secret from the American people only if (a) the program serves a compelling governmental interest and (b) the efficacy of the program would be *substantially* impaired if our enemies were to know of its existence.

Recommendation 12

We recommend that, if the government legally intercepts a communication under section 702, or under any other authority that justifies the interception of a communication on the ground that it is directed at a non-United States person who is located outside the United States, and if the communication either includes a United States person as a participant or reveals information about a United States person:

- (1) any information about that United States person should be purged upon detection unless it either has foreign intelligence value or is necessary to prevent serious harm to others;
- (2) any information about the United States person may not be used in evidence in any proceeding against that United States person;
- (3) the government may not search the contents of communications acquired under section 702, or under any other authority covered by this recommendation, in an effort to identify communications of particular United States persons, except (a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism.

Recommendation 13

We recommend that, in implementing section 702, and any other authority that authorizes the surveillance of non-United States persons who are outside the United States, in addition to the safeguards and oversight mechanisms already in place, the US Government should reaffirm that such surveillance:

- (1) must be authorized by duly enacted laws or properly authorized executive orders;
- (2) must be directed *exclusively* at the national security of the United States or our allies;

- (3) must *not* be directed at illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries; and
- (4) must not disseminate information about non-United States persons if the information is not relevant to protecting the national security of the United States or our allies.

In addition, the US Government should make clear that such surveillance:

- (1) must not target any non-United States person located outside of the United States based solely on that person's political views or religious convictions; and
- (2) must be subject to careful oversight and to the highest degree of transparency consistent with protecting the national security of the United States and our allies.

Recommendation 14

We recommend that, in the absence of a specific and compelling showing, the US Government should follow the model of the Department of Homeland Security, and apply the Privacy Act of 1974 in the same way to both US persons and non-US persons.

Recommendation 15

We recommend that the National Security Agency should have a limited statutory emergency authority to continue to track known targets of counterterrorism surveillance when they first enter the United States,

until the Foreign Intelligence Surveillance Court has time to issue an order authorizing continuing surveillance inside the United States.

Recommendation 16

We recommend that the President should create a new process requiring high-level approval of all sensitive intelligence requirements and the methods the Intelligence Community will use to meet them. This process should, among other things, identify both the uses and limits of surveillance on foreign leaders and in foreign nations. A small staff of policy and intelligence professionals should review intelligence collection for sensitive activities on an ongoing basis throughout the year and advise the National Security Council Deputies and Principals when they believe that an unscheduled review by them may be warranted.

Recommendation 17

We recommend that:

- (1) senior policymakers should review not only the requirements in Tier One and Tier Two of the National Intelligence Priorities Framework, but also any other requirements that they define as sensitive;
- (2) senior policymakers should review the methods and targets of collection on requirements in any Tier that they deem sensitive; and
- (3) senior policymakers from the federal agencies with responsibility for US economic interests should participate in

the review process because disclosures of classified information can have detrimental effects on US economic interests.

Recommendation 18

We recommend that the Director of National Intelligence should establish a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers. To this end, the Director of National Intelligence should prepare an annual report on this issue to the National Security Advisor, to be shared with the Congressional intelligence committees.

Recommendation 19

We recommend that decisions to engage in surveillance of foreign leaders should consider the following criteria:

- (1) Is there a need to engage in such surveillance in order to assess significant threats to our national security?
- (2) Is the other nation one with whom we share values and interests, with whom we have a cooperative relationship, and whose leaders we should accord a high degree of respect and deference?
- (3) Is there a reason to believe that the foreign leader may be being duplicitous in dealing with senior US officials or is attempting to hide information relevant to national security concerns from the US?
- (4) Are there other collection means or collection targets that could reliably reveal the needed information?

- (5) What would be the negative effects if the leader became aware of the US collection, or if citizens of the relevant nation became so aware?

Recommendation 20

We recommend that the US Government should examine the feasibility of creating software that would allow the National Security Agency and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk-data collection.

Recommendation 21

We recommend that with a small number of closely allied governments, meeting specific criteria, the US Government should explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens (including, if and where appropriate, intentions, strictures, or limitations with respect to collections). The criteria should include:

- (1) shared national security objectives;
- (2) a close, open, honest, and cooperative relationship between senior-level policy officials; and
- (3) a relationship between intelligence services characterized both by the sharing of intelligence information and analytic thinking and by operational cooperation against critical targets of joint national security concern. Discussions of such understandings or arrangements should be done between relevant intelligence communities, with senior policy-level oversight.

Recommendation 22

We recommend that:

- (1) the Director of the National Security Agency should be a Senate-confirmed position;
- (2) civilians should be eligible to hold that position; and
- (3) the President should give serious consideration to making the next Director of the National Security Agency a civilian.

Recommendation 23

We recommend that the National Security Agency should be clearly designated as a foreign intelligence organization; missions other than foreign intelligence collection should generally be reassigned elsewhere.

Recommendation 24

We recommend that the head of the military unit, US Cyber Command, and the Director of the National Security Agency should not be a single official.

Recommendation 25

We recommend that the Information Assurance Directorate—a large component of the National Security Agency that is not engaged in activities related to foreign intelligence—should become a separate agency within the Department of Defense, reporting to the cyber policy element within the Office of the Secretary of Defense.

Recommendation 26

We recommend the creation of a privacy and civil liberties policy official located both in the National Security Staff and the Office of Management and Budget.

Recommendation 27

We recommend that:

- (1) The charter of the Privacy and Civil Liberties Oversight Board should be modified to create a new and strengthened agency, the Civil Liberties and Privacy Protection Board, that can oversee Intelligence Community activities for foreign intelligence purposes, rather than only for counterterrorism purposes;
- (2) The Civil Liberties and Privacy Protection Board should be an authorized recipient for whistle-blower complaints related to privacy and civil liberties concerns from employees in the Intelligence Community;
- (3) An Office of Technology Assessment should be created within the Civil Liberties and Privacy Protection Board to assess Intelligence Community technology initiatives and support privacy-enhancing technologies; and
- (4) Some compliance functions, similar to outside auditor functions in corporations, should be shifted from the National Security Agency and perhaps other intelligence agencies to the Civil Liberties and Privacy Protection Board.

Recommendation 28

We recommend that:

- (1) Congress should create the position of Public Interest Advocate to represent privacy and civil liberties interests before the Foreign Intelligence Surveillance Court;
- (2) the Foreign Intelligence Surveillance Court should have greater technological expertise available to the judges;
- (3) the transparency of the Foreign Intelligence Surveillance Court's decisions should be increased, including by instituting declassification reviews that comply with existing standards; and
- (4) Congress should change the process by which judges are appointed to the Foreign Intelligence Surveillance Court, with the appointment power divided among the Supreme Court Justices.

Recommendation 29

We recommend that, regarding encryption, the US Government should:

- (1) fully support and not undermine efforts to create encryption standards;
- (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and
- (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage.

Recommendation 30

We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are often called "Zero Day" attacks because developers have had zero days to address and patch the vulnerability. US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.

Recommendation 31

We recommend that the United States should support international norms or international agreements for specific measures that will increase confidence in the security of online communications. Among those measures to be considered are:

- (1) Governments should not use surveillance to steal industry secrets to advantage their domestic industry;
- (2) Governments should not use their offensive cyber capabilities to change the amounts held in financial accounts or otherwise manipulate the financial systems;

- (3) Governments should promote transparency about the number and type of law enforcement and other requests made to communications providers;
- (4) Absent a specific and compelling reason, governments should avoid localization requirements that (a) mandate location of servers and other information technology facilities or (b) prevent trans-border data flows.

Recommendation 32

We recommend that there be an Assistant Secretary of State to lead diplomacy of international information technology issues.

Recommendation 33

We recommend that as part of its diplomatic agenda on international information technology issues, the United States should advocate for, and explain its rationale for, a model of Internet governance that is inclusive of all appropriate stakeholders, not just governments.

Recommendation 34

We recommend that the US Government should streamline the process for lawful international requests to obtain electronic communications through the Mutual Legal Assistance Treaty process.

Recommendation 35

We recommend that for big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are

statistically reliable, cost-effective, and protective of privacy and civil liberties.

Recommendation 36

We recommend that for future developments in communications technology, the US should create program-by-program reviews informed by expert technologists, to assess and respond to emerging privacy and civil liberties issues, through the Civil Liberties and Privacy Protection Board or other agencies.

Recommendation 37

We recommend that the US Government should move toward a system in which background investigations relating to the vetting of personnel for security clearance are performed solely by US Government employees or by a non-profit, private sector corporation.

Recommendation 38

We recommend that the vetting of personnel for access to classified information should be ongoing, rather than periodic. A standard of Personnel Continuous Monitoring should be adopted, incorporating data from Insider Threat programs and from commercially available sources, to note such things as changes in credit ratings or any arrests or court proceedings.

Recommendation 39

We recommend that security clearances should be more highly differentiated, including the creation of "administrative access" clearances that allow for support and information technology personnel

to have the access they need without granting them unnecessary access to substantive policy or intelligence material.

Recommendation 40

We recommend that the US Government should institute a demonstration project in which personnel with security clearances would be given an Access Score, based upon the sensitivity of the information to which they have access and the number and sensitivity of Special Access Programs and Compartmented Material clearances they have. Such an Access Score should be periodically updated.

Recommendation 41

We recommend that the “need-to-share” or “need-to-know” models should be replaced with a Work-Related Access model, which would ensure that all personnel whose role requires access to specific information have such access, without making the data more generally available to cleared personnel who are merely interested.

Recommendation 42

We recommend that the Government networks carrying Secret and higher classification information should use the best available cyber security hardware, software, and procedural protections against both external and internal threats. The National Security Advisor and the Director of the Office of Management and Budget should annually report to the President on the implementation of this standard. All networks carrying classified data, including those in contractor corporations, should be subject to a Network Continuous Monitoring

Program, similar to the EINSTEIN 3 and TUTELAGE programs, to record network traffic for real time and subsequent review to detect anomalous activity, malicious actions, and data breaches.

Recommendation 43

We recommend that the President's prior directions to improve the security of classified networks, Executive Order 13587, should be fully implemented as soon as possible.

Recommendation 44

We recommend that the National Security Council Principals Committee should annually meet to review the state of security of US Government networks carrying classified information, programs to improve such security, and evolving threats to such networks. An interagency "Red Team" should report annually to the Principals with an independent, "second opinion" on the state of security of the classified information networks.

Recommendation 45

We recommend that all US agencies and departments with classified information should expand their use of software, hardware, and procedures that limit access to documents and data to those specifically authorized to have access to them. The US Government should fund the development of, procure, and widely use on classified networks improved Information Rights Management software to control the dissemination of classified data in a way that provides greater restrictions on access and use, as well as an audit trail of such use.

Recommendation 46

We recommend the use of cost-benefit analysis and risk-management approaches, both prospective and retrospective, to orient judgments about personnel security and network security measures.

Chapter I

Principles

1. The United States Government must protect, at once, two different forms of security: national security and personal privacy.

In the American tradition, the word “security” has had multiple meanings. In contemporary parlance, it often refers to *national security* or *homeland security*. Thus understood, it signals the immense importance of counteracting threats that come from those who seek to do the nation and its citizens harm. One of the government’s most fundamental responsibilities is to protect this form of security, broadly understood. Appropriately conducted and properly disciplined, surveillance can help to eliminate important national security risks. It has helped to save lives in the past. It will help to do so in the future.

In the aftermath of the terrorist attacks of September 11, 2001, it should not be necessary to belabor this point. By their very nature, terrorist attacks tend to involve covert, decentralized actors who participate in plots that may not be easy to identify or disrupt. Surveillance can protect, and has protected, against such plots. But protection of national security includes a series of additional goals, prominently including counter-intelligence and counter-proliferation. It also includes support for military operations. Amidst serious military conflicts, surveillance can be an indispensable means of protecting the lives of those who serve or fight for our nation, and also (and it is important to emphasize this point) for our friends and allies.

At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: “The right of the people to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated” (emphasis added). This form of security is a central component of the right of privacy, which Supreme Court Justice Louis Brandeis famously described as “the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.”¹ As Brandeis wrote, “The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man’s spiritual nature, of his feelings, and of his intellect. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations.”²

This protection is indispensable to the protection of security, properly conceived. In a free society, one that is genuinely committed to self-government, people are secure in the sense that they need not fear that their conversations and activities are being watched, monitored, questioned, interrogated, or scrutinized. Citizens are free from this kind of fear. In unfree societies, by contrast, there is no right to be let alone, and people struggle to organize their lives to avoid the government’s probing eye. The resulting unfreedom jeopardizes, all at once, individual liberty, self-government, economic growth, and basic ideals of citizenship.

¹ *Olmstead v. United States*, 277 US 438, 478 (Brandeis, J., dissenting).

² *Id.*

It might seem puzzling, or a coincidence of language, that the word “security” embodies such different values. But the etymology of the word solves the puzzle; there is no coincidence here. In Latin, the word “securus” offers the core meanings, which include “free from care, quiet, easy,” and also “tranquil; free from danger, safe.” People who are at physical risk because of a threat of external violence are by definition in danger; they are not safe. So too, people made insecure by their own government, in their persons, houses, papers, and effects, can hardly be “free from care” or “tranquil.” And indeed, the first sentence of the Constitution juxtaposes the two values, explicitly using the word “secure”:

“We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, *provide for the common defense*, promote the general Welfare, and *secure the Blessings of Liberty to ourselves and our Posterity*, do ordain and establish this Constitution for the United States of America” (emphasis added).

Some people believe that the two forms of security are in irreconcilable conflict with one another. They contend that in the modern era, with serious threats to the homeland and the rise of modern communications technologies, the nation must choose between them. We firmly reject this view. It is unsupported by the facts. It is inconsistent with our traditions and our law. Free societies can and must take the necessary steps to protect national security, by enabling public officials to counteract

and to anticipate genuine threats, while also ensuring that the people are secure “in their persons, houses, papers, and effects.”

2. The central task is one of risk management; multiple risks are involved, and all of them must be considered.

When public officials acquire information, they seek to reduce risks, above all risks to national security. If the government is able to obtain access to a great deal of information, it should be in a better position to mitigate serious threats of violence. And if the goal is to reduce such threats, a wide net seems far better than a narrow one, even if the government ends up acquiring a great deal of information that it does not need or want. As technologies evolve, it is becoming increasingly feasible to cast that wide net. In the future, the feasibility of pervasive surveillance will increase dramatically. From the standpoint of risk reduction, that prospect has real advantages.

The challenge, of course, is that multiple risks are involved. The government must consider all of those risks, not a subset, when it is creating sensible safeguards. In addition to reducing risks to national security, public officials must consider four other risks.

Risks to privacy. It is self-evident that as more information is acquired, the risk to privacy increases as well. One reason is that officials might obtain personal or private information that has nothing to do with threats of violence or indeed with criminality at all. History shows that the acquisition of information can create risks of misuse and abuse, perhaps in the form of intrusion into a legitimately private sphere. History also shows

that when government is engaged in surveillance, it can undermine public trust, and in that sense render its own citizens insecure. Privacy is a central aspect of liberty, and it must be safeguarded.

Risks to freedom and civil liberties on the Internet and elsewhere.

Liberty includes a range of values, such as freedom of speech, freedom of religion, and freedom of association, that go well beyond privacy. If people are fearful that their conversations are being monitored, expressions of doubt about or opposition to current policies and leaders may be chilled, and the democratic process itself may be compromised.

Along with many other nations, the United States has been committed to the preservation and expansion of the Internet as an open, global space for freedom of expression. The pursuit of Internet freedom represents the effort to protect human rights online. These rights include the right to speak out, to dissent, and to offer or receive information across national borders. Citizens ought to be able to enjoy these rights, free from fear that their words will result in punishment or threat. A particular concern involves preservation of the rights, and the security, of journalists and the press; their rights and their security are indispensable to self-government.

Risks to our relationships with other nations. Insofar as the information comes from other nations—whether their leaders or their citizens—its acquisition, dissemination, or use might seriously compromise our relationships with those very nations. It is important to consider the potential effects of surveillance on these relationships and, in particular, on

our close allies and others with whom we share values, interests, or both. Unnecessary or excessive surveillance can create risks that outweigh any gain. Those who do not live within our borders should be treated with dignity and respect, and an absence of such treatment can create real risks.

Risks to trade and commerce, including international commerce. Free trade, including free communications, is important to commerce and economic growth. Surveillance and the acquisition of information might have harmful effects on commerce, especially if it discourages people—either citizens of the United States or others—from using certain communications providers. If the government is working closely or secretly with specific providers, and if such providers cannot assure their users that their communications are safe and secure, people might well look elsewhere. In principle, the economic damage could be severe.

These points make it abundantly clear that if officials *can* acquire information, it does not follow that they *should* do so. Indeed, the fact that officials can *legally* acquire information (under domestic law) does not mean that they should do so. In view of growing technological capacities, and the possibility (however remote) that acquired information might prove useful, it is tempting to think that such capacities should be used rather than ignored. The temptation should be resisted. Officials must consider all relevant risks, not merely one or a subset.

To this point we add an additional consideration, which is the immense importance of maintaining public trust. Some reforms are justified as improvements of the system of risk management. Other reforms

are justified, not only or primarily on that ground, but as ways to promote a general sense, in the United States and abroad, that the nation's practices and decisions are worthy of trust.

3. The idea of "balancing" has an important element of truth, but it is also inadequate and misleading.

It is tempting to suggest that the underlying goal is to achieve the right "balance" between the two forms of security. The suggestion has an important element of truth. Some tradeoffs are inevitable; we shall explore the question of balance in some detail. But in critical respects, the suggestion is inadequate and misleading.

Some safeguards are not subject to balancing at all. In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, or gender. These prohibitions are foundational, and they apply both inside and outside our territorial borders.

The purposes of surveillance must be legitimate. If they are not, no amount of "balancing" can justify surveillance. For this reason, it is exceptionally important to create explicit prohibitions and safeguards, designed to reduce the risk that surveillance will ever be undertaken for illegitimate ends.

4. The government should base its decisions on a careful analysis of consequences, including both benefits and costs (to the extent feasible).

In many areas of policy, public officials are increasingly insistent on the need for careful analysis of the consequences of their decisions and on the importance of relying not on intuitions and anecdotes, but on evidence and data, including benefits and costs (to the extent feasible). In the context of government regulation, President Ronald Reagan established a national commitment to careful analysis of regulations in his Executive Order 12291, issued in 1981. In 2011, President Barack Obama issued Executive Order 13563, which renewed and deepened the commitment to quantitative, evidence-based analysis, and added a number of additional requirements to improve regulatory review, directing agencies “to use the best available techniques to quantify anticipated present and future benefits and costs as accurately as possible” in order to achieve regulatory ends.

A central component of Executive Order 13563 involves “retrospective analysis,” meant to ensure not merely prospective analysis of (anticipated) costs and benefits, but also continuing efforts to explore what policies have actually achieved, or failed to achieve, in the real world. In our view, both prospective and retrospective analyses have important roles to play in the domain under discussion, though they also present distinctive challenges, above all because of limits in available knowledge and challenges in quantifying certain variables.

Before they are undertaken, surveillance decisions should depend (to the extent feasible) on a careful assessment of the anticipated consequences,

including the full range of relevant risks. Such decisions should also be subject to continuing scrutiny, including retrospective analysis, to ensure that any errors are corrected.

As we have seen, there is always a possibility that acquisition of more information—whether in the US or abroad—might ultimately prove helpful. But that abstract possibility does not, by itself, provide a sufficient justification for acquiring more information. Because risk management is inevitably involved, the question is one of benefits and costs, which requires careful attention to the range of possible outcomes and also to the likelihood that they will actually occur. To the extent feasible, such attention must be based on the available evidence.

Where evidence is unavailable, public officials must acknowledge the limits of what they know. In some cases, public officials are reasonably attempting to reduce risks that are not subject to specification or quantification in advance. In such cases, experience may turn out to be the best teacher; it may show that programs are not working well, and that the benefits and costs are different from what was anticipated. Continued learning and constant scrutiny, with close reference to the consequences, is necessary to safeguard both national security and personal privacy, and to ensure proper management of the full range of risks that are involved.

Finally, in constructing oversight and monitoring of intelligence agencies and particularly of surveillance, the US Government must take

care to address perceptions of potential abuse, as well as any realities. To maintain and enhance the required level of public trust, especially careful oversight is advisable.

Chapter II

Lessons of History

A. The Continuing Challenge

For reasons that we have outlined, it is always challenging to strike the right balance between the often competing values of national security and individual liberty, but as history teaches, it is *particularly* difficult to reconcile these values in times of real or perceived national crisis. Human nature being what it is, there is inevitably a risk of overreaction when we act out of fear. At such moments, those charged with the responsibility for keeping our nation safe, supported by an anxious public, have too often gone beyond programs and policies that were in fact necessary and appropriate to protect the nation and taken steps that unnecessarily and sometimes dangerously jeopardized individual freedom.

This phenomenon is evident throughout American history. Too often, we have overreacted in periods of national crisis and then later, with the benefit of hindsight, recognized our failures, reevaluated our judgments, and attempted to correct our policies going forward. We must learn the lessons of history.

As early as 1798, Congress enacted the Sedition Act, now widely regarded as a violation of the most fundamental principles of freedom of expression. Nor is the historical verdict kind to a wide range of liberty-restricting measures undertaken in other periods of great national anxiety,

including the repeated suspensions of the writ of habeas corpus during the Civil War, the suppression of dissent during World War I, the internment of Japanese-Americans during World War II, the campaign to expose and harass persons suspected of “disloyalty” during the McCarthy era, and the widespread and unlawful spying on critics of the government’s policies during the Vietnam War.³

It is true that when the nation is at risk, or engaged in some kind of military conflict, the argument for new restrictions may seem, and even be, plausible. Serious threats may tip preexisting balances. But it is also true that in such periods, there is a temptation to ignore the fact that risks are on all sides of the equation, and to compromise liberty at the expense of security. One of our central goals in this Report is to provide secure foundations for future decisions, when public fears may heighten those dangers.

With respect to surveillance in particular, the nation’s history is lengthy and elaborate, but the issues in the modern era can be traced back directly to the Vietnam War. Presidents Lyndon Johnson and Richard Nixon encouraged government intelligence agencies to investigate alleged “subversives” in the antiwar movement. The Federal Bureau of Investigation (FBI) engaged in extensive infiltration and electronic surveillance of individuals and organizations opposed to the war; the

³ See Frank J. Donner, *The Age of Surveillance: The Aims and Methods of America’s Political Intelligence System* (Knopf 1980); Peter Irons, *Justice at War* (Oxford 1983); William H. Rehnquist, *All the Laws But One: Civil Liberties in Wartime* (Knopf 1998); James Morton Smith, *Freedom’s Fetters: The Alien and Sedition Laws and American Civil Liberties* (Cornell 1956); Geoffrey R. Stone, *Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism* (W.W. Norton 2004).

Central Intelligence Agency (CIA) monitored a broad array of antiwar organizations and activities, accumulating information on more than 300,000 people; and Army intelligence initiated its own domestic spying operation, gathering information on more than 100,000 opponents of the Vietnam War, including Members of Congress, civil rights leaders, and journalists. The government sought not only to investigate its critics on a massive scale, but also to expose, disrupt, and neutralize their efforts to affect public opinion.⁴

As some of this information came to light, Congress authorized investigating committees to probe more deeply. One Senate committee made the following findings:

The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts. . . . The Government, operating primarily through secret informants, . . . has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous—and even of groups suspected of associating with potentially dangerous organizations—have continued for decades, despite the fact that those groups did not engage in unlawful activity⁵. . . .

⁴ See *Detailed Staff Reports of the Intelligence Activities and the Rights of Americans*: Book III, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, 94th (Apr. 29, 1976); Robert Justin Goldstein, *Political Repression in Modern America: From 1870 to the Present* (Schenckman 1978); Geoffrey R. Stone, *Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism*, 487-500, (W.W. Norton) 2004; Athan Theoharis, *Spying on Americans: Political Surveillance from Hoover to the Huston Plan* (Temple 1978).

⁵ See *Final Report of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*. S. Rep. No. 755, 94th Cong., 2d Sess., at 5 (April 29, 1976) (Church Committee Report).

In 1976, President Gerald Ford formally prohibited the CIA from using electronic or physical surveillance to collect information about the domestic activities of Americans and banned the National Security Agency from intercepting any communication made within, from, or to the United States, except lawful electronic surveillance under procedures approved by the Attorney General.⁶ That same year, Attorney General Edward Levi imposed new restrictions on the investigative activities of the FBI. In these guidelines, the Attorney General prohibited the FBI from investigating any group or individual on the basis of protected First Amendment activity in the absence of “specific and articulable facts” justifying a criminal investigation. Attorney General Levi adopted these guidelines without regard to whether such investigations violated the Constitution. He justified them as sound public policy and contended that the protection of civil liberties demands not only compliance with the Constitution, but also a restrained use of government power, undertaking what we would describe as a form of risk management.⁷

* * * * *

The United States has made great progress over time in its protection of “the Blessings of Liberty” – even in times of crisis. The major restrictions of civil liberties that have blackened our past would be unthinkable today.

⁶ See Executive Order 11905, United States Foreign Intelligence Activities, 41 Fed. Reg. 7703 (Feb. 18, 1976).

⁷ The Attorney General’s Guidelines on Domestic Security Investigations are reprinted in FBI Domestic Security Guidelines: Oversight Hearing Before the Committee on the Judiciary, H.R., 98th Cong., 1st Sess. 67 (Apr. 27, 1983); see also Office of the Inspector General, Special Report: The Federal Bureau of Investigation’s Compliance with the Attorney General’s Investigative Guidelines ch. 2 (Sept. 2005); Geoffrey R. Stone, *Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism*, pp. 496-497 (W.W. Norton 2004).

This is an important national achievement, and one we should not take for granted. But it is much easier to look back on past crises and find our predecessors wanting than it is to make wise judgments when we ourselves are in the eye of the storm. As time passes, new dangers, new technologies, and new threats to our freedom continually emerge. Knowing what we did right—and wrong—in the past is a useful, indeed indispensable, guide, but it does not tell us how to get it right in the future. One of the central goals of this Report is to suggest reforms that will reduce the risk of overreaction in the future.

B. The Legal Framework as of September 11, 2001

In the wake of the disclosures in the 1970s, several congressional committees examined the failures that led to the abuses. The most influential of those committees was the Senate's Select Committee to Study Governmental Operations with Respect to Intelligence Activities, which issued its comprehensive Final Report in April of 1976. Known as the Church Committee, after its chairman, Senator Frank Church, this Report has shaped much of our nation's thinking about foreign intelligence surveillance for the past 40 years⁸

At the outset, the Committee stated unequivocally that espionage, sabotage, and terrorist acts "can seriously endanger" both the security of the nation and "the rights of Americans," that "carefully focused intelligence investigations can help prevent such acts," and that "properly controlled and lawful intelligence is vital to the nation's interest." At the

⁸ *Church Committee Report* (April 26, 1976).

same time, the Committee emphasized the dangers that “intelligence collection . . . may pose for a society grounded in democratic principles.” Echoing former Attorney General and Supreme Court Chief Justice Harlan Fiske Stone, the Committee warned that an intelligence agency operating in secret can “become a menace to a free government . . . because it carries with it the possibility of abuses of power which are not always quickly apprehended or understood.” The “critical question,” the Committee explained, is “to determine how the fundamental liberties of the people can be maintained in the course of the Government’s effort to protect their security.”⁹

Looking back over the preceding decades, the Committee noted that “too often . . . intelligence activities have invaded individual privacy and violated the rights of lawful assembly and political expression.”¹⁰ This danger, the Committee observed, is inherent in the very essence of government intelligence programs, because the “natural tendency of Government is toward abuse of power” and because “men entrusted with power, even those aware of its dangers, tend, particularly when pressured, to slight liberty.”¹¹ Moreover, because abuse thrives on secrecy, there is a natural “tendency of intelligence activities to expand beyond their initial scope” and to “generate ever-increasing demands for new data.”¹² And to

⁹ *Id.*, at v, vii, 1, 3.

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

make matters worse, “once intelligence has been collected there are strong pressures to use it.”¹³

In reviewing “the overwhelming . . . excesses” of the past, the Church Committee found not only that those excesses violated the rights of Americans by invading their privacy and “undermining the democratic process,” but also that their “usefulness” in “serving the legitimate goal of protecting society” was often “questionable.”¹⁴ Those abuses, the Committee reasoned, “were due in large measure to the fact that the system of checks and balances—created in our Constitution to limit abuse of Governmental power—was seldom applied to the Intelligence Community.”¹⁵

The absence of checks and balances occurred both because government officials failed to exercise appropriate oversight and because intelligence agencies systematically concealed “improper activities from their superiors in the Executive branch and from the Congress.”¹⁶ Although recognizing that “the excesses of the past do not . . . justify depriving the United States” of the capacity to “anticipate” and prevent “terrorist violence,” the Committee made clear that “clear legal standards and effective oversight are necessary to ensure” that “intelligence activity does not itself undermine the democratic system it is intended to protect.”¹⁷

¹³ *Id.*, at 4, 291-292.

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*, at 14-15, 18, 20.

In looking to the future, the Committee was especially concerned with the impact of new and emerging technologies. The Committee expressly invoked Justice Louis Brandeis' famous dissenting opinion in *Olmstead v. United States*,¹⁸ in which the Supreme Court held in 1928, over the objections of Justices Brandeis and Oliver Wendell Holmes, that wiretapping was not a "search" within the meaning of the Fourth Amendment. In his dissenting opinion, Justice Brandeis cautioned that, since the adoption of the Constitution, "subtler and more far-reaching means of invading privacy have become available to the government . . . [and] the progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping."¹⁹ The Committee observed that Brandeis' warning applied "with obvious force to the technological developments that allow NSA to monitor an enormous number of communications each year."²⁰

"Personal privacy," the Committee added, is "essential to liberty and the pursuit of happiness" and is necessary to ensure "that all our citizens may live in a free and decent society."²¹ Indeed, "when Government infringes the right of privacy, the injury spreads far beyond the particular citizens targeted to untold numbers of other Americans who may be intimidated." The Committee added that, in the words of former Attorney General and Supreme Court Justice Robert H. Jackson, without clear legal limitations, "a federal investigative agency would 'have enough on enough

¹⁸ *Olmstead v. United States*, 277 US 438, at 473 and 478 (1928) (Brandeis, J., dissenting).

¹⁹ *Id.*, at 473-474 (Brandeis, J. dissenting).

²⁰ *Id.*, at 202.

²¹ *Id.*

people' so that 'even if it does not elect to prosecute them' the Government would . . . still 'find no opposition to its policies.'"²² Indeed, Jackson added, "even those who are supposed to supervise [our intelligence agencies] are likely to fear [them]."²³

With this warning in mind, the Committee cautioned that, "in an era where the technological capability of Government relentlessly increases, we must be wary about the drift toward 'big brother government.'" Because "the potential for abuse is awesome," it demands "special attention to fashioning restraints which not only cure past problems but anticipate and prevent the future misuse of technology." To this end, "those within the Executive Branch and the Congress . . . must be fully informed" if they are to "exercise their responsibilities wisely." Moreover, "the American public . . . should know enough about intelligence activities to be able to apply its good sense to the underlying issues of policy and morality." "Knowledge," the Committee insisted, "is the key to control." Thus, "secrecy should no longer be allowed to shield the existence of constitutional, legal, and moral problems from the scrutiny of the three branches of government or from the American people themselves."²⁴

The Committee called for "a comprehensive legislative charter defining and controlling the intelligence activities of the Federal

²² *Id.*

²³ *Church Committee Report, (April 1976)* pp. at 290-291, quoting Robert H. Jackson, *The Supreme Court in the American System of Government*, 70-71 (New York: Harper Torchbook 1955).

²⁴ *Id.*, at 289 and 292.

Government.”²⁵ The Committee set forth a series of specific principles and recommendations, including the following:

- * “There is no inherent constitutional authority for the President or any intelligence agency to violate the law.”
- * “Government action which directly infringes the rights of free speech and association must be prohibited.”
- * “No intelligence agency may engage” in “federal domestic security activities . . . unless authorized by statute.”
- * The NSA “should not monitor domestic communications, even for foreign intelligence purposes.”
- * To the extent the NSA inadvertently monitors the communications of Americans, it must “make every practicable effort to eliminate or minimize the extent to which the communications are intercepted, selected, or monitored.”
- * To the extent the NSA inadvertently monitors the communications of Americans, it should be prohibited “from disseminating such communications, or information derived therefrom, . . . unless the communication indicates evidence of hostile foreign intelligence or terrorist activity, or felonious criminal conduct, or contains a threat of death or serious bodily harm.”
- * “NSA should not request from any communications carrier any communication which it could not otherwise obtain pursuant to these recommendations.”
- * “The responsibility and authority of the Attorney General for oversight of federal domestic security activities must be clarified

²⁵ *Id.*, at 293.

and general counsels and inspectors general of intelligence agencies strengthened.”

* “Each year the . . . intelligence agencies . . . should be required to seek annual statutory authorization for their programs.”

* Congress should establish a “scheme which will afford effective redress to people who are injured by improper federal intelligence activity.”

* There should be “vigorous” congressional “oversight to review the conduct of domestic security activities through new permanent intelligence oversight committees.”

* Because “American citizens should not lose their constitutional rights to be free from improper intrusion by their Government when they travel overseas,” the “rights of Americans” must be protected “abroad as well as at home.”²⁶

* * * * *

In 1978, Congress enacted the Foreign Intelligence Surveillance Act (FISA) to implement the recommendations of the Church Committee and other congressional committees.²⁷ A central issue concerned the legality of electronic surveillance for the purpose of foreign intelligence. In 1928, the Supreme Court had held in *Olmstead*²⁸ that a wiretap is not a “search” within the meaning of the Fourth Amendment because it does not involve a *physical* intrusion into an individual’s personal property. Despite the holding in *Olmstead*, in the 1934 Communications Act Congress limited the

²⁶ *Id.*, at 295-339.

²⁷ 50 U.S.C. ch. 36.

²⁸ 277 US 438 (1928).

circumstances in which government officials could lawfully engage in wiretaps in the context of criminal investigations.²⁹

In 1967, in *Katz v. United States*,³⁰ the Court overruled *Olmstead*, noting that the Fourth Amendment “protects people not places.” The Court reasoned that, in light of the realities of modern technology, the Fourth Amendment must be understood to protect the individual’s and society’s “reasonable expectations of privacy.” It was this holding that led to the conclusion that the Fourth Amendment prohibits the government from using wiretapping unless it first obtains a search warrant from a neutral and detached magistrate based on a finding of probable cause to believe that the interception will produce evidence of criminal conduct.

It remained unclear, however, whether that same rule would apply when the government investigates “the activities of *foreign powers*, within or without this country.”³¹ The general assumption was that the President has broad constitutional authority to protect the nation in the realm of foreign intelligence surveillance without complying with the usual requirements of the Fourth Amendment. It was against this background that Congress considered FISA.

FISA attempted to safeguard the nation against the kinds of abuses that had been documented by the Church Committee, while at the same time preserving the nation’s ability to protect itself against external threats. FISA was a carefully designed compromise between those who wanted to

²⁹ 47 U.S.C. § 151 et seq.

³⁰ 389 US. 347, 351 (1967).

³¹ *United States v. United States District Court for the Eastern District of Michigan*, 407 US 297, 308 (1972).

preserve maximum flexibility for the intelligence agencies and those who wanted to place foreign intelligence surveillance under essentially the same restrictions as ordinary surveillance activities (at least insofar as the rights of Americans were concerned).

To that end, FISA brought foreign intelligence surveillance within a legal regime involving strict rules and structured oversight by all three branches of the government, but also granted the government greater freedom in the realm of foreign intelligence surveillance than it had in the context of others types of surveillance.³²

FISA restricted the government's authority to use electronic surveillance *inside the United States* to obtain foreign intelligence from "foreign powers." The term "foreign powers" was defined to include not only foreign nations, but also the agents of foreign nations and any "group engaged in international terrorism."³³ FISA established the Foreign Intelligence Surveillance Court (FISC), consisting of seven (now eleven) federal judges appointed by the Chief Justice of the United States to serve staggered terms on the FISC. FISA provided that any government agency seeking to use electronic surveillance for foreign intelligence purposes inside the United States had to obtain a warrant from the FISC. For such a warrant to be issued, the government had to show "probable cause to

³² 124 Cong. Rev. 34,845 (1978).

³³ The Act defines "foreign power" as including, among other things, "a foreign government or any component thereof," "a faction of a foreign nation," "an entity that is openly acknowledged by a foreign government . . . to be directed and controlled by such foreign government," "a group engaged in international terrorism," "a foreign-based political organization," and "an entity . . . that is engaged in the international proliferation of weapons of mass destruction." 50 U.S.C. § 1801(a).

believe that the target of the electronic surveillance” is an agent of a foreign power.³⁴

It is important to note several significant elements to this approach. First, by requiring the government to obtain a warrant from the FISC, FISA denied the President the previously assumed authority to engage in foreign intelligence surveillance inside the United States without judicial supervision. This was a major innovation.

Second, Congress created the FISC so it could deal with classified information and programs involved in foreign intelligence surveillance. Ordinary federal courts lacked the facilities and clearances to deal with such matters. A special court was therefore necessary if such classified matters were to be brought under the rule of law.

Third, FISA did not deal with the President’s authority to engage in foreign intelligence activities *outside the United States*. FISA did not require the government to obtain a FISA warrant from the FISC before it could legally wiretap a telephone conversation between two Russians in Moscow or between a US citizen in France and a US citizen in England. In such circumstances, FISA left the issue, as in the past, to the Executive Branch, operating under the National Security Act of 1947,³⁵ the National Security Agency Act of 1959,³⁶ and the US Constitution.

Fourth, FISA did not limit the government’s use of electronic surveillance in the foreign intelligence context to those situations in which

³⁴ 50 U.S.C. § 1805.

³⁵ 50 U.S.C. ch. 15.

³⁶ 50 U.S.C. § 3601.

the government has probable cause to believe that criminal activity is afoot. Rather, FISA permitted the government to engage in electronic surveillance in the United States to obtain foreign intelligence information as long as the government can establish to the satisfaction of the FISC that it has probable cause to believe that the “target” of the surveillance is an “agent of a foreign power.”

These features of the system established by FISA reflect Congress’ understanding at the time of the central differences between electronic surveillance for foreign intelligence purposes and electronic surveillance for traditional criminal investigation purposes. But in light of past abuses, the possibility of politicization, and the decision to authorize foreign intelligence surveillance of individuals, including American citizens, for whom there is no probable cause to suspect criminal conduct, FISA instituted a broad range of safeguards to prevent misuse of this authority.

For example, FISA requires the Attorney General to approve all applications for FISA warrants; it requires the Attorney General to report to the House and Senate Intelligence Committees every six months on the FISA process and the results of FISA-authorized surveillance; it requires the Attorney General to make an annual report to Congress and the public about the total number of applications made for FISA warrants and the total number of applications granted, modified, or denied; and it expressly provides that no United States citizen or legal resident of the United States may be targeted for surveillance under FISA “solely upon the basis of activities protected by the first amendment to the Constitution of the

United States.” Finally, FISA requires the use of “minimization” procedures to protect the privacy rights of individuals who are not themselves “targets” of FISA surveillance but whose conversations or personal information are *incidentally* picked up in the course of electronic surveillance of legitimate targets under the Act.³⁷

FISA changed only modestly from 1978 until the events of September 11, 2001. Although FISA originally applied only to electronic surveillance, Congress gradually widened its scope to other methods of investigation. In 1995, it was extended to physical searches; in 1998, it was extended to pen register and trap-and-trace orders (which enable the government to obtain lists of the telephone numbers and e-mails contacted by an individual after the issuance of the order); and in that same year it was extended to permit access to limited forms of business records, including documents kept by common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.³⁸

From 1978 until 2001, FISA offered an important legal framework designed to maintain the balance between the nation’s commitment both to “provide for the common defence” and to “secure the Blessings of Liberty.”

* * * * *

FISA is not the only legal authority governing foreign intelligence activities. Other statutes and Executive Orders address other facets of the

³⁷ 50 U.S.C. § 1801.

³⁸ *See* 50 U.S.C. § 1842 (2008) (pen register and trap- and- trace); 50 U.S.C. § 1862(a) (2001) (business records).

operations of the Intelligence Community. The National Security Act³⁹ and other laws relating to specific agencies, such as the Central Intelligence Agency Act⁴⁰ and the National Security Agency Act,⁴¹ regulate what agencies can do, and the Intelligence Community is also governed by laws such as the Privacy Act⁴² and the Electronic Communications Privacy Act.⁴³

Executive Order 12333 is the principal Executive Branch authority for foreign intelligence activities *not governed by FISA*.⁴⁴ Executive Order 12333 specifies the missions and authorities of each element of the Intelligence Community; sets forth the principles designed to strike an appropriate balance between the acquisition of information and the protection of personal privacy; and governs the collection, retention, and dissemination of information about United States Persons (American citizens and non-citizens who are legal residents of the United States).

Executive Order 12333 authorizes the Attorney General to promulgate guidelines requiring each element of the Intelligence Community to have in place procedures prescribing how it can collect, retain, and disseminate information about US persons. The guidelines define each agency's authorities and responsibilities. With respect to

³⁹ 50 U.S.C. ch. 15.

⁴⁰ 50 U.S.C. § 403a.

⁴¹ 50 U.S.C. § 3601.

⁴² 5 U.S.C. § 552(a).

⁴³ 18 U.S.C. §§ 2510–2522.

⁴⁴ Exec. Order No. 12333, 40 Fed. Reg. 235 (December 4, 1981), as amended by Executive Order 13284 (Jan. 23, 2003), and by Executive Order 13355 (Aug. 27, 2004), and further amended by Executive Order 13470 (July 30, 2008). Executive Order 12333 was first issued by President Gerald Ford as Executive Order 11905 and then replaced by President Jimmy Carter as Executive Order 12036, the current *United States Intelligence Activities* was signed on December 4, 1981 as Executive Order 12333 by President Ronald Reagan and updated by President George W. Bush in 2008.

National Security Agency (NSA), for example, Executive Order 12333 designates NSA as the manager for Signals Intelligence (SIGINT) for the Intelligence Community, and the Attorney General's Guidelines define how SIGINT may be conducted for collection activities not governed by FISA.⁴⁵

Section 2.4 of Executive Order 12333 prohibits specific elements of the Intelligence Community from engaging in certain types of activities inside the United States. The CIA, for example, is generally prohibited from engaging in electronic surveillance, and members of the Intelligence Community other than the FBI are generally prohibited from conducting non-consensual physical searches inside the United States.

As the principal governing authority for United States intelligence activities *outside the United States*, Executive Order 12333 requires that the collection of foreign intelligence information conform to established intelligence priorities. Under this authority, electronic surveillance of non-US Persons who are outside the United States must meet a separate set of standards. These standards and priorities are discussed in Chapter IV of this Report.

⁴⁵ These Guidelines are captured in the Department of Defense Directive 5240.1-R entitled, "DOD Activities that May Affect US Persons," including a classified appendix particularized for NSA. The guidelines are further enunciated within NSA through an internal directive, US Signals Intelligence Directive 18, commonly referred to as USSID-18.

C. September 11 and its Aftermath

The September 11 attacks were a vivid demonstration of the need for detailed information about the activities of potential terrorists. This was so for several reasons.

First, some information, which could have been useful, was not collected and other information, which could have helped to prevent the attacks, was not shared among departments.

Second, the scale of damage that 21st-century terrorists can inflict is far greater than anything that their predecessors could have imagined. We are no longer dealing with threats from firearms and conventional explosives, but with the possibility of weapons of mass destruction, including nuclear devices and biological and chemical agents. The damage that such attacks could inflict on the nation, measured in terms of loss of life, economic and social disruption, and the consequent sacrifice of civil liberties, is extraordinary. The events of September 11 brought this home with crystal clarity.

Third, 21st-century terrorists operate within a global communications network that enables them both to hide their existence from outsiders and to communicate with one another across continents at the speed of light. Effective safeguards against terrorist attacks require the technological capacity to ferret out such communications in an international communications grid.

Fourth, many of the international terrorists that the United States and other nations confront today cannot realistically be deterred by the fear of

punishment. The conventional means of preventing criminal conduct—the fear of capture and subsequent punishment—has relatively little role to play in combating some contemporary terrorists. Unlike the situation during the Cold War, in which the Soviet Union was deterred from launching a nuclear strike against the United States in part by its fear of a retaliatory counterattack, the terrorist enemy in the 21st-century is not a nation state against which the United States and its allies can retaliate with the same effectiveness. In such circumstances, detection in advance is essential in any effort to “provide for the common defence.”

Fifth, the threat of massive terrorist attacks involving nuclear, chemical, or biological weapons can generate a chilling and destructive environment of fear and anxiety among our nation’s citizens. If Americans came to believe that we are infiltrated by enemies we cannot identify and who have the power to bring death, destruction, and chaos to our lives on a massive scale, and that preventing such attacks is beyond the capacity of our government, the quality of national life would be greatly imperiled. Indeed, if a similar or even more devastating attack were to occur in the future, there would almost surely be an impulse to increase the use of surveillance technology to prevent further strikes, despite the potentially corrosive effects on individual freedom and self-governance.

In the years after the attacks of September 11, a former cabinet member suggested a vivid analogy. He compared “the task of stopping” the next terrorist attack “to a goalie in a soccer game who ‘must stop every shot,’” for if the enemy “scores a single goal,” the terrorists succeed. To

make matters worse, “the goalie cannot see the ball – it is invisible. So are the players—he doesn’t know how many there are, or where they are, or what they look like.”⁴⁶ Indeed, the invisible players might shoot the ball “from the front of the goal, or from the back, or from some other direction – the goalie just doesn’t know.”⁴⁷

Although the analogy might be overstated, it is no surprise that after the September 11, 2001 terrorist attacks the government turned to a much more aggressive form of surveillance in an effort to locate and identify potential terrorists and prevent future attacks before they could occur. One thing seemed clear: If the government was overly cautious in its efforts to detect and prevent terrorist attacks, the consequences for the nation could be disastrous. The challenge was, and remains, how to obtain information without compromising other values, including the freedoms that Americans, and citizens of many other nations, hold most dear.

D. The Intelligence Community

Executive Order 12333 sets forth the central objective of the nation’s Intelligence Community: “Accurate and timely information about the capabilities, intentions and activities of foreign powers, organizations or persons and their agents is essential to informed decisionmaking in the areas of national defense and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution

⁴⁶ Jack Goldsmith, *The Terror Presidency: Law and Judgment Inside the Bush Administration* pp. 73-74 (W.W. Norton 2007).

⁴⁷ *Id.*

and applicable law and respectful of the principles upon which the United States was founded.”⁴⁸ Although the Review Group was not charged with the task of undertaking a comprehensive evaluation of all of the many and varied elements and activities of the Intelligence Community, we can offer a few general observations.

First, the collection of foreign intelligence is a vital component of protecting the national security, including protection from terrorist threats. Indeed, foreign intelligence may be more important today than ever before in our history. This is so in part because the number of significant national security and foreign policy issues facing the United States in the 21st century is large and perhaps unprecedented. These issues include the threats of international terrorism, the proliferation of weapons of mass destruction, cyber espionage and warfare, the risk of mass atrocities, and the international elements of organized crime and narcotics and human trafficking. They include as well the challenges associated with winding down the war in Afghanistan, profound and revolutionary change in the Middle East, and successfully managing our critically important relationships with China and Russia.

Most of these challenges have a significant intelligence component. Policymakers cannot understand the issues, cannot make policy with regard to those issues, and cannot successfully implement that policy without reliable intelligence. Any expert with access to open sources can provide insight on questions such as the Eurozone crisis and Japanese

⁴⁸ Executive Order 12333 § 2.1.

politics, but insights on the plans, intentions, and capabilities of al-Qa'ida, on the status of the Iranian nuclear weapons program, and on the development of cyber warfare tools by other nations are simply not possible without reliable intelligence.

A wide range of intelligence collectors, including NSA, have made important contributions to protecting the nation's security. Notwithstanding recent controversies, and the importance of significant reforms, the national security of the United States depends on the continued capacity of NSA and other agencies to collect essential information. In considering proposals for reform, now and for the future, policymakers should avoid the risk of overreaction and take care in making changes that could undermine the capabilities of the Intelligence Community.

Second, although recent disclosures and commentary have created the impression in some quarters that NSA surveillance is indiscriminate and pervasive across the globe, that is not the case. NSA focuses on collecting foreign intelligence information that is relevant to protecting the national security of the United States and its allies. Moreover, much of what NSA collects is shared with the governments of many other nations for the purpose of enhancing their national security and the personal security of their citizens.

Third, FISA put in place a system of oversight, review, and checks-and-balances to reduce the risk that elements of the Intelligence Community would operate outside of the law. We offer many

recommendations to improve the existing procedures, but it is important to note that they now include a wide range of inspectors general, privacy oversight boards, minimization procedures,⁴⁹ intensive training requirements, mandatory reviews by the Attorney General and the Director of National Intelligence, judicial oversight by the FISA Court, and regular reporting to Congress. Appendix C provides information on these oversight mechanisms.

Significantly, and in stark contrast to the pre-FISA era, the Review Group found no evidence of illegality or other abuse of authority for the purpose of targeting domestic political activity. This is of central importance, because one of the greatest dangers of government surveillance is the potential to use what is learned to undermine democratic governance. On the other hand, as discussed later in this Report, there have been serious and persistent instances of noncompliance in the Intelligence Community's implementation of its authorities. Even if unintentional, these instances of noncompliance raise serious concerns about the Intelligence Community's capacity to manage its authorities in an effective and lawful manner.

Fourth, many of the rules governing the actions of the Intelligence Community were amended in the wake of the attacks of September 11. Predictably, and quite properly, they were amended to give the

⁴⁹ Minimization procedures govern the implementation of electronic surveillance to ensure that it conforms to its authorized purpose and scope. They require the government to "minimize" the retention and dissemination of US person information acquired by inadvertent collection. Under FISA, minimization procedures are adopted by the Attorney General and reviewed by the FISA Court. *See* 50 U.S.C.A. § 1801(h). *See* generally David S. Kris and J. Douglas Wilson, I *National Security Investigations and Prosecutions 2d* pp. 321-353 (West 2012).

Intelligence Community much broader authority to take action to ensure that the United States could prevent similar attacks in the future. But because we were acting in a moment of crisis, there was always the risk that the new rules—and the new authorities granted to the Intelligence Community—might have gone too far.

It is now time to step back and take stock. With the benefit of experience, and as detailed below, we conclude that some of the authorities that were expanded or created in the aftermath of September 11 unduly sacrifice fundamental interests in individual liberty, personal privacy, and democratic governance. We believe that our recommended modifications of those authorities strike a better balance between the competing interests in providing for the common defense and securing “the Blessings of Liberty to ourselves and our Posterity.”

We make these recommendations with a profound sense of caution, humility, and respect, and with full awareness that they will require careful deliberation and close attention to consequences. There is no doubt that the degree of safety and security our nation has enjoyed in the years since September 11 has been made possible in no small part by the energetic, determined, and effective actions of the Intelligence Community. For that, all Americans should be both proud and grateful. But even that degree of success does not mean that we cannot strike a better balance for the future.

This page has been intentionally left blank.

Chapter III

Reforming Foreign Intelligence Surveillance Directed at United States Persons

A. Introduction

A central concern of this Report is the need to define an appropriate balance between protecting the privacy interests of United States persons and protecting the nation's security. In this chapter, we focus primarily on section 215 of FISA and related issues, such as the FBI's use of national security letters, because those issues have received particular attention in recent months as a result of disclosures relating to business records.

The central issue concerns the authority of the government in general, and the Intelligence Community in particular, to require third-parties, such as telephone and Internet companies, to turn over their business records to the government. Because the data contained in those records can reveal significant information about the private lives of United States persons, it is essential to think carefully about the circumstances in which the government should have access to those records.

This chapter also deals with the collection of business records containing meta-data. To what extent does the disclosure of information about the telephone numbers or e-mails an individual contacts, which constitute meta-data, implicate significant privacy interests? In addition, this chapter offers recommendations addressing more general questions about transparency and secrecy in the activities of the Intelligence

Community. A central goal of our recommendations is to increase transparency and to decrease unnecessary secrecy, in order to enhance both accountability and public trust.

B. Section 215: Background

Only a week after the September 11 terrorist attacks, the Bush Administration proposed the PATRIOT Act to Congress. That legislation, which was adopted by an overwhelming vote, made several significant changes in FISA.⁵⁰ Among the most important was the addition of section 215, which substantially expanded the scope of permissible FISA orders to compel third parties to turn over to the government business records and other tangible objects.

As originally enacted in 1978, FISA did not grant the government any authority to compel the production of such records. In 1998, however, after the Oklahoma City and first World Trade Center bombings, Congress amended FISA to authorize the FISC to issue orders compelling the production of a narrow set of records from “a common carrier, public accommodation facility, physical storage facility or vehicle rental facility” for use in “an investigation to gather foreign intelligence information or an investigation concerning international terrorism” upon a showing of “specific and articulable facts giving reason to believe that the person to

⁵⁰ See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (“USA PATRIOT Act”) Act of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861(a)(1)) (2006 & Supp. V 2011).

whom the records pertain is a foreign power or an agent of a foreign power.”⁵¹

Section 215 of the PATRIOT Act substantially expanded this authority in two important ways. First, it eliminated the limitation on the types of entities that could be compelled to produce these records and authorized the FISC to issue orders compelling the production of “any tangible things including books, records, papers, documents, and other items.” Second, it changed the standard for the issuance of such orders. Instead of requiring the government to demonstrate that it has “specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power,”⁵² section 215 authorized the FISC to issue such orders whenever the government sought records for an authorized “investigation to protect against international terrorism or clandestine intelligence activities.”⁵³

This formulation was criticized as being too open-ended, however, and Congress thereafter amended section 215 in the USA PATRIOT Improvement and Reauthorization Act of 2005, which authorized the FISC to issue such orders only if the government provides “a statement of facts showing that there are reasonable grounds to believe that the tangible objects sought are relevant” to an authorized investigation intended to

⁵¹ Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, § 602, 112 Stat. 2396, 2410 (1998).

⁵² *Id.*

⁵³ See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (“USA PATRIOT Act”) Act of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861(a)(1)) (2006 & Supp. V 2011).

protect “against international terrorism or clandestine intelligence activities.”⁵⁴

* * * * *

Is section 215 consistent with the Fourth Amendment? There are two concerns. First, section 215 does not require a showing of probable cause. The Supreme Court has long held, however, that the “Fourth Amendment was not intended to interfere with the power of courts to compel, through a subpoena, the production” of evidence, as long as the order compelling the production of records or other tangible objects meets the general test of “reasonableness.”⁵⁵ In theory, section 215 extends the principle of the subpoena from the traditional criminal investigation into the realm of foreign intelligence.

Second, in many instances section 215 is used to obtain records that implicate the privacy interests of individuals whose personal information is contained in records held by a third party. This is so, for example, when the government seeks to obtain financial information about a particular individual from her bank, or telephone calling data about a particular individual from her telephone company. In a series of decisions in the 1970s, the Supreme Court held that individuals have no “reasonable expectation of privacy” in information they voluntarily share with third

⁵⁴ USA PATRIOT Improvement and Reauthorization Act of 2005 § 106, 120 Stat. 196 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)). Section 215 provides that such investigations of United States persons may not be “conducted solely on the basis of activities protected by the first amendment to the Constitution.” For certain materials, such as library records, book sales records, firearms sales records, tax return records, educational records, and medical records with information identifying an individual, only the Director of the FBI, the Deputy Director of the FBI, or the Executive Assistant for National Security may make the application. *See* 50 U.S.C. § 1863(a)(3) (2006).

⁵⁵ *Hale v. Henkel*, 201 US 43, 76 (1906).

parties, such as banks and telephone companies, explaining that “what a person knowingly exposes” to third parties “is not a subject of Fourth Amendment protection.” In *Miller v. United States*⁵⁶ the Court applied this reasoning to bank records and in *Smith v. Maryland*⁵⁷ it extended it to an individual’s telephone calling records.

Those decisions led to the enactment of section 215. In 1978, relying on *Miller* and *Smith*, Congress enacted the Right to Financial Privacy Act of 1978.⁵⁸ Although the Right to Financial Privacy Act generally prohibited financial institutions from disclosing personal financial records, it expressly authorized them to disclose such records in response to lawful subpoenas and search warrants.⁵⁹ In the national security context, Congress relied upon *Miller* and *Smith* to give the government important new tools to collect foreign intelligence information.

In 1998, for example, Congress amended FISA to grant the government “pen register” and “trap-and-trace” authority.⁶⁰ A trap-and-trace device identifies the sources of incoming calls and a pen register indicates the numbers called from a particular phone number. The 1998 amendment authorized the FISC to issue orders compelling telephone service providers to permit the government to install these devices upon a

⁵⁶ 425 US 435 (1976).

⁵⁷ 442 US 735 (1979).

⁵⁸ Section 1114, Pub. L. 95-630, 92 Stat. 3706 (1978).

⁵⁹ *Id.*

⁶⁰ 50 U.S.C. § 1842.

showing that the government seeks to obtain information “relevant” to a foreign intelligence investigation.⁶¹

That same year, as noted earlier, Congress enacted the precursor of section 215, which, as amended, authorizes the FISC to issue orders compelling the production of records and other tangible objects from third parties whenever the government has “reasonable grounds to believe” that the records or “objects sought are relevant” to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities.”⁶² The PATRIOT Act later expanded this authority to include sender/addressee information relating to e-mail and other forms of electronic communications.⁶³

Although these authorities were made possible by *Miller* and *Smith*, there is some question today whether those decisions are still good law. In its 2012 decision in *United States v. Jones*,⁶⁴ the Court held that long-term surveillance of an individual’s location effected by attaching a GPS device to his car constituted a trespass and therefore a “search” within the meaning of the Fourth Amendment. In reaching this result, five of the Justices suggested that the surveillance might have infringed on the driver’s “reasonable expectations of privacy” even if there had been no technical trespass and even though an individual’s movements in public

⁶¹ *Id.* This is similar to the authority federal law grants to federal and state prosecutors and local police officials to obtain court orders for the installation of pen registers and trap-and-trace devices upon certification that the information sought is relevant to an ongoing criminal investigation. See 18 U.S.C. § 3122.

⁶² 50 U.S.C. § 1861(a)(1).

⁶³ See 115 Stat. § 288-291 (2001).

⁶⁴ 132 S.Ct. 945 (2012).

are voluntarily exposed to third parties. As Justice Sonia Sotomayor observed in her concurring opinion, “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to [others] for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.”⁶⁵

Similarly, Justice Samuel Alito, in a concurring opinion joined by Justices Ruth Bader Ginsburg, Stephen Breyer, and Elena Kagan, declared that “we must assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.”⁶⁶ Noting that modern technological advances can seriously undermine our traditional expectations of privacy, Justice Alito argued that the Fourth Amendment must take account of such changes. Although the Court in *Jones* did not overrule *Miller* and *Smith*, and left that issue for another day, a majority of the Justices clearly indicated an interest in considering how the principle recognized in those decisions should apply in a very different technological society from the one that existed in the 1970s.

However the Supreme Court ultimately resolves the Fourth Amendment issue, that question is not before us. Our charge is not to interpret the Fourth Amendment, but to make recommendations about

⁶⁵ *Id.*, at 957 (Sotomayor, J., concurring).

⁶⁶ *Id.*, at 950 (Alito, J., concurring), quoting *Kyllo v. United States*, 533 US 27, 34 (2001).

sound public policy. In his concurring opinion in *Jones*, Justice Alito noted that “concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions.” Indeed, he added, at a time of “dramatic technological change,” the “best solution to privacy concerns may be legislative,” because a “legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.”⁶⁷

C. Section 215 and “Ordinary” Business Records

Recommendation 1

We recommend that section 215 should be amended to authorize the Foreign Intelligence Surveillance Court to issue a section 215 order compelling a third party to disclose otherwise private information about particular individuals only if:

- (1) it finds that the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities” and**
- (2) like a subpoena, the order is reasonable in focus, scope, and breadth.**

As written, section 215 confers essentially subpoena-like power on the FISC, granting it the authority to order third parties to turn over to federal investigators records and other tangible objects if the government presents “a statement of facts showing that there are reasonable grounds to

⁶⁷ *Id.*, at 964 (Alito, J., concurring).

believe that the tangible objects sought are relevant” to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities.”⁶⁸ Section 215 makes clear that, in order for records and other objects to be obtained under its authority, they must be things that “could be obtained with a subpoena issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things.”⁶⁹

There are several points of comparison between the traditional subpoena and section 215: (1) section 215 deals with national security investigations rather than criminal investigations; (2) section 215 involves orders issued by the FISC, whereas subpoenas are issued in other federal district court proceedings; (3) because of the sensitive nature of national security investigations, the section 215 process involves a high degree of secrecy; and (4) section 215’s “relevance” and minimization requirements effectively embody a “reasonableness” standard similar to that employed in the use of subpoenas. Assuming that the traditional subpoena is an appropriate method of gathering evidence, and that it strikes a reasonable balance between the interests of privacy and public safety in the context of criminal investigations, it might seem that, when used in a similar manner, section 215 is also an appropriate method of collecting information in the

⁶⁸ See 50 U.S.C. § 1861(b)(2)(A). Section 215 provides that such investigations of United States persons may not be “conducted solely on the basis of activities protected by the first amendment to the Constitution.”

⁶⁹ 50 U.S.C. § 1861(c)(2)(D).

context of authorized investigations to protect “against international terrorism or clandestine intelligence activities.”

We do not agree. Whereas the subpoena is typically used to obtain records pertaining to an individual or entity relevant to a particular criminal investigation, section 215 authorizes the FISC to order the production of records or other tangible objects whenever there are “reasonable grounds to believe that the tangible things sought are relevant to authorized investigations . . . to protect against international terrorism or clandestine intelligence activities.” The analogue in the subpoena context would be a court order directing banks and credit card companies to turn over financial information whenever *the police* conclude that they have “reasonable grounds to believe that the tangible things sought are relevant to authorized investigations” of a drug cartel.

This formulation leaves extremely broad discretion in the hands of government officials to decide for themselves *whose* records to obtain. The shift from the 1998 standard to the 2005 standard, which was adopted in the wake of the terrorist attacks of September 11, 2001, leaves too little authority in the FISC to define the appropriate parameters of section 215 orders. We believe that, as a matter of sound public policy, it is advisable for a neutral and detached judge, rather than a government investigator engaged in the “competitive enterprise” of ferreting out suspected terrorists,⁷⁰ to make the critical determination whether the government has reasonable grounds for intruding upon the legitimate privacy interests of

⁷⁰ *California v. Acevedo*, 500 US 565, 568 (1991). (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948).

any *particular* individual or organization. The requirement of an explicit judicial finding that the order is “reasonable in focus, scope, and breadth” is designed to ensure this critical element of judicial oversight.

D. National Security Letters

Recommendation 2

We recommend that statutes that authorize the issuance of National Security Letters should be amended to permit the issuance of National Security Letters only upon a judicial finding that:

- (1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities” and
- (2) like a subpoena, the order is reasonable in focus, scope, and breadth.

Recommendation 3

We recommend that all statutes authorizing the use of National Security Letters should be amended to require the use of the same oversight, minimization, retention, and dissemination standards that currently govern the use of section 215 orders.

Shortly after the decision in *Miller*, Congress created the National Security Letter (NSL) as a form of administrative subpoena.⁷¹ NSLs, which

⁷¹ Administrative subpoenas are authorized by many federal statutes and may be issued by most federal agencies. Most statutes authorizing administrative subpoenas authorize an agency to require the production of certain records for civil rather than criminal matters.

are authorized by five separate federal statutory provisions,⁷² empower the FBI and other government agencies in limited circumstances to compel individuals and organizations to turn over to the FBI in the course of national security investigations many of the same records that are covered by section 215 and that criminal prosecutors can obtain through subpoenas issued by a judge or by a prosecutor in the context of a grand jury investigation. NSLs are used primarily to obtain telephone toll records, e-mail subscriber information, and banking and credit card records. Although NSLs were initially used sparingly, the FBI issued 21,000 NSLs in Fiscal Year 2012, primarily for subscriber information. NSLs are most often used early in an investigation to gather information that might link suspected terrorists or spies to each other or to a foreign power or terrorist organization.

When NSLs were first created, the FBI was empowered to issue an NSL only if it was authorized by an official with the rank of Deputy Assistant Director or higher in the Bureau's headquarters, and only if that official certified that there were "specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or an agent of a foreign power."⁷³ The PATRIOT Act of 2001 significantly expanded the FBI's authority to issue NSLs. First, the PATRIOT Act authorized every Special Agent in Charge of any of the Bureau's 56 field offices around the country to issue NSLs. NSLs therefore no longer have to be issued by high-level officials at FBI headquarters.

⁷² 12 U.S.C. § 3414, 15 U.S.C. § 1681(u), 15 U.S.C. § 1681(v), 18 U.S.C. § 2709, and 50 U.S.C. § 436.

⁷³ 50 U.S.C. § 1801.

Second, the PATRIOT Act eliminated the need for any *particularized* showing of individualized suspicion.⁷⁴ Under the PATRIOT Act, the FBI can issue an NSL whenever an authorized FBI official certifies that the records sought are “relevant to an authorized investigation.” Third, the PATRIOT Act empowered the FBI to issue nondisclosure orders (sometimes referred to as “gag orders”) that prohibit individuals and institutions served with NSLs from disclosing that fact, and it provided for the first time for judicial enforcement of those nondisclosure orders.⁷⁵ In contemplating the power granted to the FBI in the use of NSLs, it is important to emphasize that NSLs are issued directly by the FBI itself, rather than by a judge or by a prosecutor acting under the auspices of a grand jury.⁷⁶ Courts ordinarily enter the picture only if the recipient of an NSL affirmatively challenges its legality.⁷⁷

NSLs have been highly controversial. This is so for several reasons. First, as already noted, NSLs are issued by FBI officials rather than by a judge or by a prosecutor in the context of a grand jury investigation. Second, as noted, the standard the FBI must meet for issuing NSLs is very low. Third, there have been serious compliance issues in the use of NSLs. In 2007, the Department of Justice’s Office of the Inspector General detailed

⁷⁴ Pub. L. 107-56, 115 Stat. 365 (2001).

⁷⁵ See 18 U.S.C. § 3511.

⁷⁶ It should be noted that there are at least two distinctions between NSLs and federal grand jury subpoenas. First, where the FBI believes that records should be sought, it can act directly by issuing NSLs, but to obtain a grand jury subpoena the FBI must obtain approval by a prosecutor at the Department of Justice. Second, and except in exceptional circumstances, witnesses who appear before a grand jury ordinarily are not under nondisclosure orders preventing them from stating that they have been called as witnesses.

⁷⁷ See David S. Kris and J. Douglas Wilson, I *National Security Investigations and Prosecutions 2d*, pp. 727-763 (West 2012).

extensive misuse of the NSL authority, including the issuance of NSLs without the approval of a properly designated official and the use of NSLs in investigations for which they had not been authorized.⁷⁸ Moreover, in 2008, the Inspector General disclosed that the FBI had “issued [NSLs] . . . after the FISA Court, citing First Amendment concerns, had twice declined to sign Section 215 orders in the same investigation.”⁷⁹ Fourth, the oversight and minimization requirements governing the use of NSLs are much less rigorous than those imposed in the use of section 215 orders.⁸⁰ Fifth, nondisclosure orders, which are used with 97 percent of all NSLs, interfere with individual freedom and with First Amendment rights.⁸¹

There is one final—and important— issue about NSLs. For all the well-established reasons for requiring neutral and detached judges to decide when government investigators may invade an individual’s privacy, there is a strong argument that NSLs should not be issued by the FBI itself. Although administrative subpoenas are often issued by administrative agencies, foreign intelligence investigations are especially likely to implicate highly sensitive and personal information and to have potentially severe consequences for the individuals under investigation.

⁷⁸ See Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation’s Use of National Security Letters (Unclassified)* (March 2007). *Note: Subsequent reports from the IG have noted the FBI and DOJ have resolved many of the compliance incidents.*

⁷⁹ United States Department of Justice, Office of the Inspector General, *A Review of the FBI’s Use of Section 215 Orders for Business Records in 2006* 5 (March 2008), quoted in Kris & Wilson, *National Security Investigations and Prosecutions* at 748. In recent years, the FBI has put in place procedures to reduce the risk of noncompliance.

⁸⁰ 18 U.S.C. § 1861(g).

⁸¹ In *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2008), the court held that the FBI’s use of nondisclosure orders violated the First Amendment. In response, the FBI amended its procedures to provide that if a recipient of an NSL objects to a non-disclosure order, the FBI must obtain a court order based on a demonstrated need for secrecy in order for it to enforce the non-disclosure order.

We are unable to identify a principled reason why NSLs should be issued by FBI officials when section 215 orders and orders for pen register and trap-and-trace surveillance must be issued by the FISC.

We recognize, however, that there are legitimate practical and logistical concerns. At the current time, a requirement that NSLs must be approved by the FISC would pose a serious logistical challenge. The FISC has only a small number of judges and the FBI currently issues an average of nearly 60 NSLs per day. It is not realistic to expect the FISC, as currently constituted, to handle that burden. This is a matter that merits further study. Several solutions may be possible, including a significant expansion in the number of FISC judges, the creation within the FISC of several federal magistrate judges to handle NSL requests, and use of the Classified Information Procedures Act⁸² to enable other federal courts to issue NSLs.

We recognize that the transition to this procedure will take some time, planning, and resources, and that it would represent a significant change from the current system. We are not suggesting that the change must be undertaken immediately and without careful consideration. But it should take place as soon as reasonably possible. Once the transition is complete, NSLs should not issue without prior judicial approval, in the absence of an emergency where time is of the essence.⁸³ We emphasize the importance of the last point: In the face of a genuine emergency, prior

⁸² 18 U.S.C. app. 3 §§ 1-16.

⁸³ It is essential that the standards and processes for issuance of NSLs match as closely as possible the standards and processes for issuance of section 215 orders. Otherwise, the FBI will naturally opt to use NSLs whenever possible in order to circumvent the more demanding - and perfectly appropriate - section 215 standards. We reiterate that if judicial orders are required for the issuance of NSLs, there should be an exception for emergency situations when time is of the essence.

judicial approval would not be required under standard and well-established principles.

E. Section 215 and the Bulk Collection of Telephony Meta-data

1. The Program

One reading of section 215 is that the phrase “reasonable grounds to believe that the tangible things sought are *relevant* to an authorized investigation” means that the order must specify with reasonable particularity the records or other things that must be turned over to the government. For example, the order might specify that a credit card company must turn over the credit records of a particular individual who is reasonably suspected of planning or participating in terrorist activities, or that a telephone company must turn over to the government the call records of any person who called an individual suspected of carrying out a terrorist act within a reasonable period of time preceding the terrorist act. This interpretation of “relevant” would be consistent with the traditional understanding of “relevance” in the subpoena context.

In May 2006, however, the FISC adopted a much broader understanding of the word “relevant.”⁸⁴ It was that decision that led to the collection of bulk telephony meta-data under section 215. In that decision, and in thirty-five decisions since, fifteen different FISC judges have issued orders under section 215 directing specified United States telecommunications providers to turn over to the FBI and NSA, “on an

⁸⁴ See *In re Application of the Federal Bureau of Investigation for an Order Requiring the Prod. Of Tangible Things from [Telecommunications Providers] Relating to [Redacted version]*, Order No. BR-05 (FISC May 24, 2006).

ongoing daily basis,” for a period of approximately 90 days, “all call detail records or ‘telephony meta-data’ created by [the provider] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.”⁸⁵

The “telephony meta-data” that must be produced includes “comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile Station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.”⁸⁶ The orders expressly provide that the meta-data to be produced “does not include the substantive content of any communication . . . or the name, address, or financial information of a subscriber or customer,” nor does it include “cell site location information.”⁸⁷ The orders also contain a nondisclosure provision directing that, with certain exceptions, “no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order.”⁸⁸

The FISC authorized the collection of bulk telephony meta-data under section 215 in reliance “on the assertion of the [NSA] that having access to all the call records ‘is vital to NSA’s counterterrorism intelligence’ because ‘the only effective means by which NSA analysts are able

⁸⁵ *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR 13-109 (FISC Oct. 11, 2013) (hereinafter FISC order 10/11/2013).

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

continuously to keep track of” the activities, operatives, and plans of specific foreign terrorist organizations who “disguise and obscure their communications and identities” is “to obtain and maintain an archive of meta-data that will permit these tactics to be uncovered.”⁸⁹ The government has explained the rationale of the program as follows:

One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in this effort. It is imperative that we have the capability to rapidly identify any terrorist threat inside the United States. . . .

. . . By analyzing telephony meta-data based on telephone numbers or other identifiers associated with terrorist activity, trained expert analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the United States. . . . In this respect, the program helps to close critical intelligence gaps that were highlighted by the September 11, 2001 attacks.⁹⁰

⁸⁹ *In Re Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR-08-13 (FISC Dec. 12, 2008), quoting Application Exhibit A, Declaration of [Redacted version] (Dec. 11, 2008).

⁹⁰ Administration White Paper, *Bulk Collection of Telephony Meta-data Under Section 215 of the USA PATRIOT Act*, at 3-4 (August 9, 2013).

What this means, in effect, is that specified service providers must turn over to the government on an ongoing basis call records for every telephone call made in, to, or from the United States through their respective systems. NSA retains the bulk telephony meta-data for a period of five years. The meta-data are then purged automatically from NSA's systems on a rolling basis. As it currently exists, the section 215 program acquires a very large amount of telephony meta-data each day, but what it collects represents only a small percentage of the total telephony meta-data held by service providers. Importantly, in 2011 NSA abandoned a similar meta-data program for Internet communications.⁹¹

According to the terms of the FISC orders, the following restrictions govern the use of this telephony meta-data:

1. "NSA shall store and process the . . . meta-data in repositories with secure networks under NSA's control. The . . . meta-data shall carry unique markings such that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training," and

⁹¹ For several years, NSA used a similar meta-data program for Internet communications under the authority of FISA's pen register and trap-and-trace provisions rather than under the authority of section 215. NSA suspended this e-mail meta-data program in 2009 because of compliance issues (it came to light that NSA had inadvertently been collecting certain types of information that were not consistent with the FISC's authorization orders). After re-starting it in 2010, NSA Director General Keith Alexander decided to let the program expire at the end of 2011 because, for operational and technical reasons, the program was insufficiently productive to justify the cost. The possibility of revising and reinstating such a program was left open, however. This program posed problems similar to those posed by the section 215 program, and any effort to re-initiate such a program should be governed by the same recommendations we make with respect to the section 215 program.

“NSA shall restrict access to the . . . meta-data to authorized personnel who have received” such training.

2. “The government is . . . prohibited from accessing” the meta-data “for any purpose” other than to obtain “foreign intelligence information.”⁹²
3. “NSA shall access the . . . meta-data for purposes of obtaining foreign intelligence only through queries of the . . . meta-data to obtain contact chaining information . . . using selection terms approved as ‘seeds’ pursuant to the RAS approval process.” What this means is that NSA can access the meta-data only when “there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried,” that is, the specific phone number, “is associated with” a specific foreign terrorist organization. The government submits and the FISC approves a list of specific foreign terrorist organizations to which all queries must relate.
4. The finding that there is a reasonable, articulable suspicion that any particular identifier is associated with a foreign terrorist organization can be made initially by only one of 22 specially trained persons at NSA (20 line personnel and two supervisors). All RAS determinations must be made

⁹² Appropriately trained and authorized technical personnel may also access the meta-data “to perform those processes needed to make it usable for intelligence analysis,” and for related technical purposes, according to the FISC orders.

independently by at least two of these personnel and then approved by one of the two supervisors before any query may be made.

5. Before any selection term may be queried, NSA's Office of General Counsel (OGC) "must first determine" whether it is "reasonably believed to be used by a United States person."⁹³ If so, then the selection term may not be queried if the OGC finds that the United States person was found to be "associated with" a specific foreign terrorist organization "solely on the basis of activities that are protected by the First Amendment to the Constitution."
6. "NSA shall ensure, through adequate and appropriate technical and management controls, that queries of the . . . meta-data for intelligence analysis purposes will be initiated using only selection terms that have been RAS-approved. Whenever the . . . meta-data is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis tools, an auditable record of the activity shall be generated."
7. The determination that a particular selection term may be queried remains in effect for 180 days if the selection term is reasonably believed to be used by a United States person, and otherwise for one year.

⁹³ 50 U.S.C. 1801(i). A "United States person" is either a citizen of the United States or a non-citizen who is a legal permanent resident of the United States.

8. Before any of the results from queries may be shared outside NSA (typically with the FBI), NSA must comply with minimization and dissemination requirements, and before NSA may share any results from queries that reveal information about a United States person, a high-level official must additionally determine that the information “is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.”
9. The FISA court does not review or approve individual queries either in advance or after the fact. It does set the criteria for queries, however, and it receives reports every 30 days from NSA on the number of identifiers used to query the meta-data and on the results of those queries. The Department of Justice and the Senate and House Intelligence Committees also receive regular briefings on the program.
10. Both NSA and the National Security Division of the Department of Justice (NSD/DOJ) conduct regular and rigorous oversight of this program. For example:
 - NSA’s OGC and Office of the Director of Compliance (ODOC) “shall ensure that personnel with access to the . . . meta-data receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and

retention of the . . . meta-data and the results of queries of the . . . meta-data.”⁹⁴

- NSD/DOJ receives “all formal briefing and/or training materials.” NSA’s ODOC “shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information.”⁹⁵
- NSA’s OGC “shall consult with NSD/DOJ “on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority,” and at least once every ninety days NSA’s OGC, ODOC and NSD/DOJ “shall meet for the purpose of assessing compliance” with the FISC’s orders. The results of that meeting “shall be reduced to writing and submitted” to the FISC “as part of any application to renew or reinstate the authority.”⁹⁶
- At least once every 90 days “NSD/DOJ shall meet with NSA’s Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA’s compliance” with the FISC’s orders, and at least once every 90 days NSA’s OGC and NSD/DOJ “shall review a

⁹⁴ *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR 13-158 (FISC, Dec. 2011).

⁹⁵ *Id.*, at 14.

⁹⁶ *Id.*, at 14-15.

sample of the justifications for RAS approvals for selection terms used to query the . . . meta-data.”⁹⁷

- Approximately every 30 days, NSA must file with the FISC “a report that includes a discussion of NSA’s application of the RAS standard,” “a statement of the number of instances . . . in which NSA has shared, in any form, results from queries of the . . . meta-data that contain United States person information, in any form, with anyone outside NSA,” and an attestation for each instance in which United States information has been shared that “the information was related to counterterrorism information and necessary to understand counterterrorism or to assess its importance.”⁹⁸

How does the section 215 bulk telephony meta-data program work in practice? In 2012, NSA queried 288 unique identifiers, each of which was certified by NSA analysts to meet the RAS standard. When an identifier, or “seed” phone number, is queried, NSA receives a list of every telephone number that either called or was called by the seed phone number in the past five years. This is known as the “first hop.” For example, if the seed phone number was in contact with 100 different phone numbers in the past five years, NSA would have a list of those phone numbers. Given that NSA

⁹⁷ *Id.*, at 15.

⁹⁸ *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR 13-109 (FISC Oct. 11, 2013) (hereinafter FISC order 10/11/2013).

has reasonable articulable suspicion to believe that the seed phone number is associated with a foreign terrorist organization, it then seeks to determine whether there is any reason to believe that any of the 100 numbers are *also* associated with a foreign terrorist organization. If so, the query has uncovered possible connections to a potential terrorist network that merits further investigation. Conversely, if none of the 100 numbers in the above hypothetical is believed to be associated with possible terrorist activity, there is less reason to be concerned that the potential terrorist is in contact with co-conspirators in the United States.

In most cases, NSA makes a second "hop." That is, it queries the database to obtain a list of every phone number that called or was called by the 100 numbers it obtained in the first hop. To continue with the hypothetical: If we assume that the average telephone number called or was called by 100 phone numbers over the course of the five-year period, the query will produce a list of 10,000 phone numbers (100×100) that are two "hops" away from the person reasonably believed to be associated with a foreign terrorist organization. If one of those 10,000 phone numbers is thought to be associated with a terrorist organization, that is potentially useful information not only with respect to the individuals related to the first and third hops, but also with respect to individuals related to the second hop (the middleman). In a very few instances, NSA makes a third "hop," which would expand the list of numbers to approximately one million ($100 \times 100 \times 100$).

In 2012, NSA's 288 queries resulted in a total of twelve "tips" to the FBI that called for further investigation. If the FBI investigates a telephone number or other identifier tipped to it through the section 215 program, it must rely on other information to identify the individual subscribers of any of the numbers retrieved. If, through further investigation, the FBI is able to develop probable cause to believe that an identifier in the United States is conspiring with a person engaged in terrorist activity, it can then seek an order from the FISC authorizing it to intercept the *contents* of future communications to and from that telephone number.

NSA believes that on at least a few occasions, information derived from the section 215 bulk telephony meta-data program has contributed to its efforts to prevent possible terrorist attacks, either in the United States or somewhere else in the world. More often, negative results from section 215 queries have helped to alleviate concern that particular terrorist suspects are in contact with co-conspirators in the United States. Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders. Moreover, there is reason for caution about the view that the program is efficacious in alleviating concern about possible terrorist connections, given the fact that the meta-data captured by the program covers only a portion of the records of only a few telephone service providers.

* * * * *

The bulk telephony meta-data collection program has experienced several significant compliance issues. For example, in March 2009, the FISC learned that for two-and-a-half years NSA had searched all incoming phone meta-data using an “alert list” of phone numbers of possible terrorists that had been created for other purposes. Almost 90 percent of the numbers on the alert list did *not* meet the “reasonable, articulable suspicion” standard.⁹⁹

FISC Judge Reggie Walton concluded that the minimization procedures had been “so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively.”¹⁰⁰ Although finding that the noncompliance was unintentional, and was due to misunderstandings on the part of analysts about the precise rules governing their use of the meta-data, Judge Walton concluded “that the government’s failure to ensure that responsible officials adequately understood NSA’s alert list process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the government and the FISC from taking steps to remedy daily violations of the minimization procedures set forth in FISC orders and designed to protect . . . call details pertaining to telephone communications of US persons located within the United States who are not the subject of

⁹⁹ *In Re Production of Tangible Things From [Undisclosed Service Provider]*, Docket Number: BR 08-13 (March 2, 2009).

¹⁰⁰ *Id.*

any . . . investigation and whose call detail information could not otherwise have been legally captured in bulk.”¹⁰¹

Judge Walton found additional compliance issues involving incidents in which inadequately trained analysts “had queried the . . . meta-data . . . ‘without being aware they were doing so.’”¹⁰² As a result, “NSA analysts used 2,373 foreign telephone identifiers to query the . . . meta-data without first determining that the reasonable, articulable suspicion standard had been satisfied.” Judge Walton concluded that “the minimization procedures” that had been “approved and adopted as binding by the orders of the FISC have been so frequently and systematically violated that it can fairly be said that this critical element of the overall [bulk telephony meta-data] regime has never functioned effectively.”¹⁰³

Although NSA maintained that, upon learning of these noncompliance incidents, it had taken remedial measures to prevent them from recurring, Judge Walton rejected the government’s argument that, in light of these measures, “the Court need not take any further remedial action.” Because it had become apparent that “NSA’s data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures,” NSA Director General Keith Alexander conceded that “there was no single person who had a complete understanding of the [section 215] FISA system architecture.”¹⁰⁴

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ *Id.*

¹⁰⁴ *Id.*

In light of that concession and other information, Judge Walton held that “the Court will not permit the government to access the data collected until such time as the government is able to restore the Court’s confidence that the government can and will comply with [the] approved procedures for accessing such data.” Until such time, the government would be permitted to access the data only subject to a FISC order authorizing a specific query “on a case-by-case” basis premised on a RAS finding by the FISC itself.¹⁰⁵

Judge Walton lifted this restriction in September 2009 after NSA demonstrated to his satisfaction that the causes of the noncompliance had been corrected and that additional safeguards had been instituted to reduce the possibility of similar incidents of noncompliance in the future.¹⁰⁶

* * * * *

It is noteworthy that, after the bulk telephony meta-data program came to light in the summer of 2013, some commentators argued that the program is both unconstitutional and beyond the scope of what Congress authorized. The constitutional argument turns largely on whether *Miller* and *Smith* are still good law and on whether they should control the collection of bulk telephony meta-data. In a recent FISC opinion, Judge Mary A. McLaughlin acknowledged that the “Supreme Court may someday revisit the third-party disclosure principle in the context of twenty-first century communications technology,” but concluded that until that day arrives, “*Smith* remains controlling with respect to the acquisition

¹⁰⁵ See *In re Production of Tangible Things From [Redacted version]*, No. BR-09-13 (FISC, September 3, 2009).

¹⁰⁶ *Id.*

by the government from service providers of non-content telephony meta-data.”¹⁰⁷

The statutory objection asserts that the FISC’s interpretation of section 215 does violence to the word “relevant.” Some commentators have noted that, although courts have upheld relatively broad subpoenas in the context of civil actions, administrative proceedings and grand jury investigations, “no single subpoena discussed in a reported decision is as broad as the FISC’s telephony meta-data orders.”¹⁰⁸ Nonetheless, in a recent FISC decision, Judge Claire V. Eagen concluded that the bulk telephony meta-data program meets what she described as “the low statutory hurdle set out in Section 215.”¹⁰⁹ Our charge is not to resolve these questions, but to offer guidance from the perspective of sound public policy as we look to the future.

2. The Mass Collection of Personal Information

Recommendation 4

We recommend that, as a general rule, and without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes. Any program involving government collection or storage of such data must be narrowly tailored to serve an important government interest.

¹⁰⁷ *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted version]*, Docket No. BR 13-158 (FISC Oct. 11, 2013), pp. 5-6.

¹⁰⁸ David S. Kris, *On the Bulk Collection of Tangible Things*, 1 Lawfare Research Paper Series 4 at 26 (Sept. 29, 2013).

¹⁰⁹ *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted version]*, Docket No. BR 13-109 (FISC Aug. 29, 2013).

We will turn shortly to the section 215 bulk telephony meta-data program. But to orient that discussion and to establish governing principles, we begin with a broader question, which involves the production not only of telephone calling records, but also of every other type of record or other tangible thing that could be obtained through a traditional subpoena, including bank records, credit card records, medical records, travel records, Internet search records, e-mail records, educational records, library records, and so on.

Our focus, then, is on genuinely mass collections of all undigested, non-public personal information about individuals – those collections that involve not a selected or targeted subset (such as airline passenger lists), but far broader collections. Although the government has expressly disclaimed any interest in such mass collection of personal information under section 215,¹¹⁰ nothing in the statute, as interpreted by the FISC, would necessarily preclude such a program. The question is whether such a program, even if consistent with the Fourth Amendment and section 215, would be sound public policy.

Because international terrorists inevitably leave footprints when they recruit, train, finance, and plan their operations, government acquisition and analysis of such personal information might provide useful clues about their transactions, movements, behavior, identities and plans. It might, in

¹¹⁰ See Kris, *On the Bulk Collection of Tangible Things*, p. 34. Indeed, the government has suggested that “communications meta-data is different from many other kinds of records because it is inter-connected and the connections between individual data points, which can be reliably identified only through analysis of a large volume of data, are particularly important to a broad range of investigations of international terrorism.” *Administration White Paper*, p. 2.

other words, help the government find the proverbial needles in the haystack. But because such information overwhelmingly concerns the behavior of ordinary, law-abiding individuals, there is a substantial risk of serious invasions of privacy.

As a report of the National Academy of Sciences (NAS) has observed, the mass collection of such personal information by the government would raise serious “concerns about the misuse and abuse of data, about the accuracy of the data and the manner in which the data are aggregated, and about the possibility that the government could, through its collection and analysis of data, inappropriately influence individuals’ conduct.”¹¹¹ According to the NAS report, “data and communication streams” are ubiquitous:

[They] concern financial transactions, medical records, travel, communications, legal proceedings, consumer preferences, Web searches, and, increasingly, behavior and biological information. This is the essence of the information age—. . . everyone leaves personal digital tracks in these systems whenever he or she makes a purchase, takes a trip, uses a bank account, makes a phone call, walks past a security camera, obtains a prescription, sends or receives a package, files income tax forms, applies for a loan, e-mails a friend, sends a fax, rents a video, or engages in just about any other activity Gathering and analyzing [such data] can play major roles

¹¹¹ National Research Council of the National Academy of Science, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, pp. 2-3 (National Academies Press 2008).

in the prevention, detection, and mitigation of terrorist attacks. . . . [But even] under the pressures of threats as serious as terrorism, the privacy rights and civil liberties that are cherished core values of our nation must not be destroyed. . . .

One . . . concern is that law-abiding citizens who come to believe that their behavior is watched too closely by government agencies . . . may be unduly inhibited from participating in the democratic process, may be inhibited from contributing fully to the social and cultural life of their communities, and may even alter their purely private and perfectly legal behavior for fear that discovery of intimate details of their lives will be revealed and used against them in some manner.¹¹²

Despite these concerns, several arguments can be made in support of allowing the government to collect and access *all* of this information. First, one might argue, building on the logic of *Miller* and *Smith*, that individuals are not concerned about the privacy of such matters because, if they were, they would not voluntarily make the information available to their banks, credit card companies, Internet service providers, telephone companies, health-care providers, and so on.

Whatever the logic of this argument in the Fourth Amendment context, it seems both unrealistic and unsound as a matter of public policy. In modern society, individuals, for practical reasons, have to use banks,

¹¹² *Id.*

credit cards, e-mail, telephones, the Internet, medical services, and the like. Their decision to reveal otherwise private information to such third parties does not reflect a lack of concern for the privacy of the information, but a necessary accommodation to the realities of modern life. What they want—and reasonably expect—is *both* the ability to use such services *and* the right to maintain their privacy when they do so. As a matter of sound public policy in a free society, there is no reason why that should not be possible.

Second, one might argue that there is nothing to fear from such a program because the government will query the information database only when it has good reasons for doing so. Assume, for example, that the government has legal authority to query the hypothetical mass information database only when it can demonstrate facts that give rise to a reasonable, articulable suspicion that the target of the query is associated with a foreign terrorist organization. That restriction certainly reduces the concern about widespread invasions of privacy because it would deny the government legal authority to query the database to obtain private information about individuals for other, less worthy—and perhaps illegitimate—reasons.

But this does not eliminate the concern. For one thing, under any such standard there will inevitably be many queries of individuals who are not in fact involved with terrorist organizations. This is the false positive—or inadvertent acquisition—problem. Whenever the government investigates individuals on grounds less demanding than absolute certainty of guilt, there will inevitably be false positives. Even when the government has a warrant based on a judicial finding of probable cause,

innocent persons will often be searched because probable cause is a far cry from absolute certainty.

One way to mitigate this concern would be to elevate the standard for lawful queries under section 215 from reasonable articulable suspicion to probable cause. But even that would leave privacy at risk. This is so because, in traditional searches, the government does not discover *everything* there is to know about an individual. The enormity of the breach of privacy caused by queries of the hypothetical mass information database dwarfs the privacy invasion occasioned by more traditional forms of investigation. For the innocent individual who is unlucky enough to be queried under even a probable cause standard, virtually *everything* about his life instantly falls into the hands of government officials. The most intimate details of his life are laid bare.

Moreover, and perhaps more important, there is the lurking danger of abuse. There is always a risk that the rules, however reasonable in theory, will not be followed in practice. This might happen because an analyst with access to the information decides to query an innocent individual for any number of possible reasons, ranging from personal animosity to blackmail to political opposition. Although the safeguards in place under section 215 attempt to prevent such abuse, no system is perfect. We have seen that even under section 215, with all of its safeguards, there have been serious issues of noncompliance. A breach of privacy might also happen because an outsider manages to invade the database, thereby accessing and then either using or publicly disclosing reams of information

about particular individuals or, in the nightmare scenario, making the entire system transparent to *everyone*.

Finally, we cannot discount the risk, in light of the lessons of our own history, that at some point in the future, high-level government officials will decide that this massive database of extraordinarily sensitive private information is there for the plucking. Americans must never make the mistake of wholly “trusting” our public officials. As the Church Committee observed more than 35 years ago, when the capacity of government to collect massive amounts of data about individual Americans was still in its infancy, the “massive centralization of . . . information creates a temptation to use it for improper purposes, threatens to ‘chill’ the exercise of First Amendment rights, and is inimical to the privacy of citizens.”¹¹³

Third, one might argue that, despite these concerns, the hypothetical mass collection of personal information would make it easier for the government to protect the nation from terrorism, and it should therefore be permitted. We take this argument seriously. But even if the premise is true, the conclusion does not necessarily follow. Every limitation on the government’s ability to monitor our conduct makes it more difficult for the government to prevent bad things from happening. As our risk-management principle suggests, the question is not whether granting the government authority makes us incrementally safer, but whether the additional safety is worth the sacrifice in terms of individual privacy, personal liberty, and public trust.

¹¹³ *Church Committee Report* at 778 (April 1976).

Although we might be safer if the government had ready access to a massive storehouse of information about every detail of our lives, the impact of such a program on the quality of life and on individual freedom would simply be too great. And this is especially true in light of the alternative measures available to the government. Specifically, even if the government cannot collect and store for future use massive amounts of personal information about our lives, it would still be free under section 215 to obtain *specific* information relating to *specific* individuals or *specific* terrorist threats from banks, telephone companies, credit card companies, and the like—when it can demonstrate to the FISC that it has *reasonable grounds* to access such information.

3. Is Meta-data Different?

Recommendation 5

We recommend that legislation should be enacted that terminates the storage of bulk telephony meta-data by the government under section 215, and transitions as soon as reasonably possible to a system in which such meta-data is held instead either by private providers or by a private third party. Access to such data should be permitted only with a section 215 order from the Foreign Intelligence Surveillance Court that meets the requirements set forth in Recommendation 1.

Under section 215 as interpreted by the FISC, NSA is authorized to collect bulk telephony meta-data and to store the call records of *every* telephone call made in, to, or from the United States, and it is then permitted to query that meta-data if it has a reasonable, articulable

suspicion that a particular phone number, or “seed,” usually a telephone number belonging to a person outside the United States, is associated with a foreign terrorist organization. Section 215 as interpreted authorizes the collection and retention only of *telephony* meta-data. Should that limitation make the program permissible?

We do not believe so. There are two distinctions between the hypothetical and actual versions of section 215. First, the total amount of data collected and retained in the hypothetical version of section 215 is *much* greater than the total amount of data collected and retained in the actual version. This means that the possible harm caused by the collection and the possible benefit derived from the collection are *both* reduced. Everything else being equal, this suggests that the balance between costs and benefits is unchanged.¹¹⁴

Second, and more important, it is often argued that the collection of bulk telephony meta-data does not seriously threaten individual privacy, because it involves only transactional information rather than the content of the communications. Indeed, this is a central argument in defense of the existing program. It does seem reasonable to assume that the intrusion on privacy is greater if the government collects the content of every telephone call made in, to, or from the United States than if it collects only the call information, or meta-data. But as critics of the bulk collection of telephony meta-data have observed, the record of every telephone call an individual

¹¹⁴ It is possible, of course, for the government carefully to target its collection and retention of data in a way that maximizes the benefit and minimizes the cost, thereby substantially altering the balance of costs and benefits. But there is no reason to believe that this describes the decision to collect bulk telephony meta-data, in particular.

makes or receives over the course of several years can reveal an enormous amount about that individual's private life.

We do not mean to overstate either the problem or the risks. In our review, we have not uncovered any official efforts to suppress dissent or any intent to intrude into people's private lives without legal justification. NSA is interested in protecting the national security, not in personal details unrelated to that concern. But as Justice Sotomayor observed about GPS monitoring of locational information in *Jones*, telephone calling data can reveal "a wealth of detail" about an individual's "familial, political, professional, religious, and sexual associations."¹¹⁵ It can reveal calls "to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar, and on and on."¹¹⁶

Knowing that the government has ready access to one's phone call records can seriously chill "associational and expressive freedoms," and knowing that the government is one flick of a switch away from such information can profoundly "alter the relationship between citizen and government in a way that is inimical to society."¹¹⁷ That knowledge can significantly undermine public trust, which is exceedingly important to the well-being of a free and open society.

¹¹⁵ *United States v. Jones*, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring).

¹¹⁶ *Id.*

¹¹⁷ *Id.* at 956 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (C.A. 7, 2011) (Flaum, J., concurring)).

Moreover, and importantly, even without collecting and storing bulk telephony meta-data itself, there are alternative ways for the government to achieve its legitimate goals, while significantly limiting the invasion of privacy and the risk of government abuse. As originally envisioned when section 215 was enacted, the government can query the information directly from the relevant service providers after obtaining an order from the FISC. Although this process might be less efficient for the government, NSA Director General Keith Alexander informed the Review Group that NSA itself has seriously considered moving to a model in which the data are held by the private sector. This change would greatly reduce the intake of telephony meta-data by NSA, and it would therefore also dramatically (and in our view appropriately) reduce the risk, both actual and perceived, of government abuse.

We recognize that there might be problems in querying multiple, privately held data bases simultaneously and expeditiously. In our view, however, it is likely that those problems can be significantly reduced by creative engineering approaches. We also recognize that there might be issues about the length of time that some carriers ordinarily would retain such meta-data and about the financial costs that might be placed on telephony providers by the approach we recommend. But we think that it would be in the interests of the providers and the government to agree on a

voluntary system that meets the needs of both. If a voluntary approach is not successful, then implementing legislation might be required.¹¹⁸

If reliance on government queries to individual service providers proves to be so inefficient that it seriously undermines the effectiveness of the program, and if the program is shown to be of substantial value to our capacity to protect the national security of the United States and our allies, then the government might authorize a specially designated private organization to collect and store the bulk telephony meta-data. NSA could then query the meta-data from that independent entity in the same manner that it could query the meta-data from the service providers. The use of such a private organization to collect and store bulk telephony meta-data should be implemented only if expressly authorized by Congress.

In light of these alternatives, we conclude that there is no sufficient justification for allowing the government itself to collect and store bulk telephony meta-data.¹¹⁹ We recommend that this program should be terminated as soon as reasonably practicable.

¹¹⁸ For example, Congress might enact legislation requiring relevant telephone providers to retain the data for a specified period of time to ensure that it will be available if and when the government needs to query it. In that case, the government should reimburse the providers for the cost of retaining the data. Based on our review, an appropriate period of time would seem to be no more than two years. A Federal Communications Commission (FCC) regulation already requires providers to hold such information for 18 months, so it seems feasible to change the retention period for telephone records. The FCC's rule on retention of telephone toll records is 47 C.F.R. § 42.6: "Retention of telephone toll records. Each carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time, and length of the call. Each carrier shall retain this information for toll calls that it bills whether it is billing its own toll service customers for toll calls or billing customers for another carrier. 60 Fed. Reg. 2d 1529 (1986); 51 FR 32651, corrected, 51 FR 39536.

¹¹⁹ It is noteworthy that the section 215 telephony meta-data program has made only a modest contribution to the nation's security. It is useful to compare it, for example, to the section 702 program, which we discuss in the next Part of our Report. Whereas collection under section 702 has produced

Recommendation 6

We recommend that the government should commission a study of the legal and policy options for assessing the distinction between meta-data and other types of information. The study should include technological experts and persons with a diverse range of perspectives, including experts about the missions of intelligence and law enforcement agencies and about privacy and civil liberties.

Are there any circumstances in which the government should be permitted to collect and retain meta-data in which it could not collect and retain other information? One question concerns the meaning of “meta-data.” In the telephony context, “meta-data” refers to technical information about the phone numbers, routing information, duration of the call, time of the call, and so forth. It does not include information about the contents of the call. In the e-mail context, “meta-data” refers to the “to” and “from” lines in the e-mail and technical details about the e-mail, but not the subject line or the content. The assumption behind the argument that meta-data is meaningfully different from other information is that the collection of meta-data does not seriously invade individual privacy.

As we have seen, however, that assumption is questionable. In a world of ever more complex technology, it is increasingly unclear whether the distinction between “meta-data” and other information carries much

significant information in many, perhaps most, of the 54 situations in which signals intelligence has contributed to the prevention of terrorist attacks since 2007, section 215 has generated relevant information in only a small number of cases, and there has been no instance in which NSA could say with confidence that the outcome would have been different without the section 215 telephony meta-data program. Moreover, now that the existence of the program has been disclosed publicly, we suspect that it is likely to be less useful still.

weight.¹²⁰ The quantity and variety of meta-data have increased. In contrast to the telephone call records at issue in the 1979 case of *Smith v. Maryland*,¹²¹ today's mobile phone calls create meta-data about a person's location. Social networks provide constant updates about who is communicating with whom, and that information is considered meta-data rather than content. E-mails, texts, voice-over-IP calls, and other forms of electronic communication have multiplied. For Internet communications in general, the shift to the IPv6 protocol is well under way. When complete, web communications will include roughly 200 data fields, in addition to the underlying content. Although the legal system has been slow to catch up with these major changes in meta-data, it may well be that, as a practical matter, the distinction itself should be discarded.

The question about how to govern content and meta-data merits further study. Such a study should draw on the insights of technologists, due to the central role of changing technology. Economists and other social scientists should help assess the costs and benefits of alternative approaches. The study should include diverse persons, with a range of perspectives about the mission of intelligence and law enforcement agencies and also with expertise with respect to privacy and civil liberties.

¹²⁰ See *International Principles on the Application of Human Rights to Communications Surveillance*, 10 July 2013, available at <http://en.necessaryandproportionate.org/text>.

¹²¹ 442 US 735 (1979).

F. Secrecy and Transparency

Recommendation 7

We recommend that legislation should be enacted requiring that detailed information about authorities such as those involving National Security Letters, section 215 business records, section 702, pen register and trap-and-trace, and the section 215 bulk telephony meta-data program should be made available on a regular basis to Congress and the American people to the greatest extent possible, consistent with the need to protect classified information. With respect to authorities and programs whose existence is unclassified, there should be a strong presumption of transparency to enable the American people and their elected representatives independently to assess the merits of the programs for themselves.

Recommendation 8

We recommend that:

- (1) legislation should be enacted providing that, in the use of National Security Letters, section 215 orders, pen register and trap-and-trace orders, 702 orders, and similar orders directing individuals, businesses, or other institutions to turn over information to the government, non-disclosure orders may be issued only upon a judicial finding that there are reasonable grounds to believe that disclosure would significantly threaten the national security, interfere with an ongoing investigation, endanger the life or physical safety of any person, impair

diplomatic relations, or put at risk some other similarly weighty government or foreign intelligence interest;

- (2) nondisclosure orders should remain in effect for no longer than 180 days without judicial re-approval; and
- (3) nondisclosure orders should never be issued in a manner that prevents the recipient of the order from seeking legal counsel in order to challenge the order's legality.

Recommendation 9

We recommend that legislation should be enacted providing that, even when nondisclosure orders are appropriate, recipients of National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders issued in programs whose existence is unclassified may publicly disclose on a periodic basis general information about the number of such orders they have received, the number they have complied with, the general categories of information they have produced, and the number of users whose information they have produced in each category, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

Recommendation 10

We recommend that, building on current law, the government should publicly disclose on a regular basis general data about National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders in programs whose

existence is unclassified, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

Recommendation 11

We recommend that the decision to keep secret from the American people programs of the magnitude of the section 215 bulk telephony meta-data program should be made only after careful deliberation at high levels of government and only with due consideration of and respect for the strong presumption of transparency that is central to democratic governance. A program of this magnitude should be kept secret from the American people only if (a) the program serves a compelling governmental interest and (b) the efficacy of the program would be *substantially* impaired if our enemies were to know of its existence.

A free people can govern themselves only if they have access to the information that they need to make wise judgments about public policy. A government that unnecessarily shields its policies and decisions from public scrutiny therefore undermines the most central premise of a free and self-governing society. As James Madison observed, "A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both."¹²²

There is no doubt that in the realm of national security, the nation needs to keep secrets. The question, though, is what information must be

¹²² Letter from James Madison to W.T. Barry (Aug. 4, 1822) in *The Writings of James Madison* at 103 (Gaillard Hunt, ed., G.P. Putnam's Sons) 1910.

kept secret. The reasons why government officials want secrecy are many and varied. They range from the truly compelling to the patently illegitimate. Sometimes government officials want secrecy because they rightly fear that the disclosure of certain information might seriously undermine the nation's security. Sometimes they want secrecy because they do not want to have to deal with public criticism of their decisions or because they do not want the public, Congress, or the courts to override their decisions, which they believe to be wise. Sometimes they want secrecy because disclosure will expose their own incompetence, noncompliance, or wrongdoing. Some of those reasons for secrecy are obviously more worthy of deference than others.

Adding to the complexity, the contribution of any particular disclosure to informed public discourse may vary widely depending upon the nature of the information. The disclosure of some confidential information may be extremely valuable to public debate (for example, the revelation of unwise or even unlawful government programs). The disclosure of other confidential information, however, may be of little or no legitimate value to public debate (for example, publication of the identities of covert American agents). The most vexing problems arise when the public disclosure of secret information is *both* harmful to national security *and* valuable to informed self-governance.

There is a compelling need today for a serious and comprehensive reexamination of the balance between secrecy and transparency. In considering this question, the Public Interest Declassification Board (PIDB)

recently observed: "A Democratic society is grounded in the informed participation of the citizenry, and their informed participation requires access to Government information. An open record of official decisions is essential to educate and inform the public and enable it to assess the policies of its elected leaders. If officials are to be accountable for their actions and decisions, secrecy must be kept to the minimum required to meet legitimate national security considerations. . . . Better access to Government records and internal history will help both policymakers and the American public meet their mutual responsibilities to address national security and foreign policy challenges consistent with democratic values." The PIDB concluded that it is necessary for the United States to make the reforms necessary "to transform current classification and declassification guidance and practice."¹²³

Another dimension to the secrecy vs. transparency issue concerns the role of whistle-blowers. Although an individual government employee or contractor should not take it upon himself to decide on his own to "leak" classified information because he thinks it would be better for the nation for the information to be disclosed, it is also the case that a free and democratic nation needs safe, reliable, and fair-minded processes to enable such individuals to present their concerns to responsible and independent officials. After all, their concerns might be justified. It does not serve the nation for our government to prevent information that should be disclosed from being disclosed. Although such mechanisms exist, they can certainly

¹²³ Public Interest Declassification Board, *Transforming the Security Classification System*, 1-2 (2012), pp.1-2.

be strengthened and made more accessible.¹²⁴ Appendix D sets forth existing mechanisms for whistle-blowing.

The secrecy vs. transparency issue also has serious repercussions today for the freedom of the press. It is the responsibility of our free press to expose abuse, over-reaching, waste, undue influence, corruption, and bad judgment on the part of our elected officials. A robust and fearless freedom of the press is essential to a flourishing self-governing society. It will not do for the press to be fearful, intimidated, or cowed by government officials. If they are, it is "We the People" who will suffer. Part of the responsibility of our free press is to ferret out and expose information that government officials would prefer to keep secret when such secrecy is unwarranted. This point raises fundamental issues about press shield laws, spying on members of the press and their sources, investigating members of the press, and attempting to intimidate members of the press.

At the same time, the potential danger of leaks is more serious than ever, especially in light of the fact that information can be spread instantly across the globe. The fact that classified information can now be stolen, either by insiders or outsiders, in massive quantities, creates

¹²⁴ On October 10, 2012, President Obama issued Presidential Policy Directive/PPD-19, which prohibits any retaliatory employment action against any government employee with access to classified information who reports any instance of "waste, fraud, and abuse," including violations "of any law, rule, or regulation," to "a supervisor in the employee's direct chain of command up to and including the head of the employing agency, to the Inspector General of the employing agency or Intelligence Community Element, to the Director of National Intelligence, to the Inspector General of the Intelligence Community." *Id.* Although this is an important step in the right direction, it does not go far enough. First, it covers only government employees and not government contractors. Second, it requires the would-be whistle-blower to report to a person in his "direct chain of command," rather than to an independent authority. We discuss whistle-blowing in Chapter VI.

unprecedented dangers. Put simply, the stakes on both sides—national security and effective self-governance—are high.

At the very least, we should always be prepared to question claims that secrecy is necessary. That conclusion needs to be demonstrated rather than merely assumed. When it is possible to promote transparency without appreciably sacrificing important competing interests, we should err on the side of transparency.

Thus, in implementing NSLs, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders in programs whose existence is unclassified, the government should, to the greatest extent possible, report publicly on the total number of requests made and the number of individuals whose records have been requested. These totals inform Congress and the public about the overall size and trends in a program, and are especially informative when there are major changes in the scale of a program. In addition, providers have shown a strong interest in providing periodic transparency reports about the number of requests to which they have responded. Reports from providers can be a useful supplement to reports from the government—the existence of multiple sources of information reduces the risk of inaccurate reporting by any one source. Reports from providers are also an important way for providers to assure customers and the general public that they are careful stewards of their users' records. As discussed in Chapter VII, such transparency reports from providers should be permitted and encouraged by governments throughout the world, and the US Government should work with allies to

enable accurate reporting about government requests in other countries as well as in the United States.

In some instances, over-reporting can also be a problem. This might occur when there are duplicative reports, which burden agencies with redundant requirements. To address this concern, the government should catalog the current reporting requirements on FISA, NSLs, and other intelligence-related statistics, and document how frequently these reports are made and to whom. As shown in Appendix C, multiple oversight mechanisms exist for reporting to Congress and within the Executive Branch. A catalog of existing reports would create a more informed basis for deciding what changes in reporting might be appropriate. Moreover, in some instances public reports can unintentionally harm the national security by inadvertently revealing critical information. For instance, detailed reports by small Internet service providers about government requests for information might inadvertently tip off terrorists or others who are properly under surveillance. To reduce this risk, reporting requirements should be less detailed in those situations in which reporting about a small number events might reveal critical information to those under surveillance.¹²⁵

¹²⁵ Similarly, in the context of the non-disclosure orders addressed in Recommendation 9, the government should be able to act without prior judicial authority in cases of emergency.

Chapter IV

Reforming Foreign Intelligence Surveillance Directed at Non-United States Persons

A. Introduction

To what extent should the United States accord non-United States persons the same privacy protections it recognizes for United States persons? At one level, it is easy to say that “all persons are created equal” and that every nation should accord all persons the same rights, privileges and immunities that it grants to its own citizens. But, of course, no nation follows such a policy. Nations see themselves as distinct communities with particular obligations to the members of their own community. On the other hand, there are certain fundamental rights and liberties that all nations should accord to all persons, such as the international prohibition on torture.

In this chapter, we explore the non-United States person issue in the specific content of foreign intelligence surveillance. International law recognizes the right of privacy as fundamental,¹²⁶ but the concrete meaning of that right must be defined. Certainly, a nation can choose to grant its own citizens a greater degree of privacy than international law requires.

We focus specifically on foreign intelligence collection under section 702 of FISA and Executive Order 12333. The central question we address is: What is the *minimum* degree of privacy protection the United States should

¹²⁶ The Universal Declaration of Human Rights, Art. 12 states, “No one shall be subjected to arbitrary interference with his privacy...”

grant to non-United States persons in the realm of foreign intelligence surveillance? We conclude that the United States should grant greater privacy protection to non-United States persons than we do today.

B. Foreign Intelligence Surveillance and Section 702

In general, the federal government is prohibited from intercepting the contents of private telephone calls and e-mails of *any* person, except in three circumstances. First, in the context of criminal investigations, Title III of the Electronic Communications Privacy Act authorizes the government to intercept such communications if a federal judge issues a warrant based on a finding that there is probable cause to believe that an individual is committing, has committed, or is about to commit a federal crime and that communications concerning that crime will be seized as a result of the proposed interception.¹²⁷

Second, as enacted in 1978, FISA authorized the federal government to intercept electronic communications if a judge of the FISC issues a warrant based on a finding that the purpose of the surveillance is to obtain *foreign intelligence information*, the interception takes place *inside the United States*, and there is probable cause to believe that the target of the surveillance is an agent of a foreign power (which includes, among other things, individuals engaged in international terrorism, the international proliferation of weapons of mass destruction, and clandestine intelligence activities).

¹²⁷ See 18 U.S.C. § 2518(3).

Third, there is foreign intelligence surveillance that takes place *outside the United States*. At the time FISA was enacted, Congress expressly decided not to address the issue of electronic surveillance of persons located outside the United States, including American citizens, noting that the “standards and procedures for overseas surveillance may have to be different than those provided in this bill for electronic surveillance within the United States.”¹²⁸ It was apparently assumed that intelligence collection activities outside the United States would be conducted under the Executive Branch’s inherent constitutional authority and the statutory authorizations granted to each Intelligence Community agency by Congress, and that it would be governed by presidential Executive Orders and by procedures approved by the Attorney General. To that end, in 1981 President Ronald Reagan issued Executive Order 12333, discussed above, which (as amended) specifies the circumstances in which the nation’s intelligence agencies can engage in foreign intelligence surveillance outside the United States.¹²⁹

Although Congress did not take up this issue in the immediate aftermath of the terrorist attacks of September 11, 2001, several developments brought the question to the fore. First, technological

¹²⁸ H. Rep. No. 95-1283 (I) at 50-51 (June 5, 1978).

¹²⁹ Executive Order 12333, which governs the use of electronic surveillance by the Intelligence Community outside the United States, provides that “timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, persons, and their agents, is essential to the national security of the United States.” It declares that “special emphasis should be given to detecting and countering” espionage, terrorism, and the development, possession, proliferation, or use of weapons of mass destruction. The executive order directs that “such techniques as electronic surveillance” may not be used “unless they are in accordance with procedures . . . approved by the Attorney General” and that “such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes.”

advances between 1978 and the early 21st century complicated the implementation of the original FISA rules. The distinction FISA drew between electronic surveillance conducted inside the United States and electronic surveillance conducted outside the United States worked reasonably well in 1978, because then-existing methods of communication and collection made that distinction meaningful. But the development of a global Internet communications grid with linchpins located within the United States undermined the distinction.

By the early twenty-first century, a large percentage of the world's electronic communications passed through the United States, and foreign intelligence collection against persons located outside the United States was therefore increasingly conducted with the assistance of service providers inside the United States. Unless the legislation was amended, this new state of affairs meant that the government would have to go to the FISC to obtain orders authorizing electronic surveillance for foreign intelligence purposes even of individuals who were in fact *outside* the United States, a state of affairs Congress had not anticipated at the time it enacted FISA in 1978.

Second, in late 2005 it came to light that, shortly after the attacks of September 11, President George W. Bush had secretly authorized NSA to conduct foreign intelligence surveillance of individuals who were *inside* the United States without complying with FISA. Specifically, the President authorized NSA to monitor electronic communications (e.g., telephone calls and e-mails) between people inside the United States and people

outside the United States whenever NSA had “a reasonable basis to conclude that one party to the communication” was affiliated with or working in support of al-Qa’ida.

Because this secret program did not require the government either to obtain a warrant from the FISC or to demonstrate that it had probable cause that the target of the surveillance was an agent of a foreign power—even when the target was inside the United States—it clearly exceeded the bounds of what Congress had authorized in FISA. The Bush administration maintained that this program was nonetheless lawful, invoking both Congress’ 2001 Authorization to Use Military Force and the President’s inherent constitutional authority as commander-in-chief.

In light of these developments, Congress decided to revisit FISA. In 2007, Congress amended FISA in the Protect America Act (PAA), which provided, among other things, that FISA was inapplicable to any electronic surveillance that was “directed at a person reasonably believed to be located outside the United States.”¹³⁰ In effect, the PAA excluded from the protections of FISA warrantless monitoring of international communications if the target of the surveillance was outside the United States, even if the target was an American citizen. The PAA was sharply criticized on the ground that it gave the government too much authority to target the international communications of American citizens.

The following year, Congress revised the law again in the FISA Amendments Act of 2008 (FAA). The FAA adopted different rules for

¹³⁰ The Protect America Act of 2007, Pub. L. 111-55 (Aug. 5, 2007) which amended 50 U.S.C. § 1803 et. seq., by adding §§ 1803 a-c.

international communications depending on whether the target of the surveillance was a “*United States person*” (a category that was defined to include both American citizens and non-citizens who are legal permanent residents of the United States)¹³¹ or a “*non-United States person*.”¹³² The FAA provides that if the government targets a United States person who is outside the United States, the surveillance must satisfy the traditional requirements of FISA. That is, the surveillance is permissible only if it is intended to acquire foreign intelligence information and the FISC issues a warrant based on a finding that there is probable cause to believe that the United States person is an agent of a foreign power, within the meaning of FISA. Thus, if the target of the surveillance is a United States person, the same FISA procedures apply—without regard to whether the target is inside or outside the United States.

On the other hand, the FAA provided in section 702 that if the target of foreign intelligence surveillance is a *non-United States person* who is “reasonably believed to be located outside the United States,” the government need not have probable cause to believe that the target is an agent of a foreign power and need not obtain an individual warrant from the FISC, even if the interception takes place *inside* the United States. Rather, section 702 authorized the FISC to approve annual certifications submitted by the Attorney General and the Director of National Intelligence (DNI) that identify certain *categories* of foreign intelligence targets whose communications may be collected, subject to FISC-approved

¹³¹ See 50 U.S.C. § 1881(c).

¹³² See 50 U.S.C. § 1881(a).

targeting and minimization procedures. The categories of targets specified by these certifications typically consist of, for example, international terrorists and individuals involved in the proliferation of weapons of mass destruction.

Under section 702, the determination of which *individuals* to target pursuant to these FISC-approved certifications is made by NSA without any additional FISC approval. In implementing this authority, NSA identifies specific “identifiers” (for example, e-mail addresses or telephone numbers) that it reasonably believes are being used by non-United States persons located outside of the United States to communicate foreign intelligence information within the scope of the approved categories (*e.g.*, international terrorism, nuclear proliferation, and hostile cyber activities). NSA then acquires the content of telephone calls, e-mails, text messages, photographs, and other Internet traffic using those identifiers from service providers in the United States.¹³³

Illustrative identifiers might be an e-mail account used by a suspected terrorist abroad or other means used by high-level terrorist leaders in two separate countries to pass messages. The number of identifiers for which NSA collects information under section 702 has gradually increased over time.

Section 702 requires that NSA’s certifications attest that a “significant purpose” of any acquisition is to obtain foreign intelligence information

¹³³ See 50 U.S.C. §1881. Service providers who are subject to these orders are entitled to compensation and are immune from suit for their assistance. They may petition the FISC to set aside or modify the directive if they think that it is unlawful. If a provider is uncooperative, the Attorney General may petition the FISC for an order to enforce the directive.

(i.e. directed at international terrorism, nuclear proliferation, or hostile cyber activities), that it does not intentionally target a United States person, that it does not intentionally target any person known at the time of acquisition to be in the United States, that it does not target any person outside the United States for the purpose of targeting a person inside the United States, and that it meets the requirements of the Fourth Amendment.¹³⁴ The annual certification provided to the FISC must attest that the Attorney General and the Director of National Intelligence have adopted guidelines to ensure compliance with these and other requirements under section 702, including that the government does not intentionally use section 702 authority to target United States persons, inside or outside the United States.¹³⁵ The FISC annually reviews the targeting and minimization procedures to ensure that they satisfy all statutory and constitutional requirements.

Other significant restrictions govern the use of section 702:

- If a section 702 acquisition inadvertently obtains a communication of or concerning a United States person, section 702's minimization procedures require that any information about such a United States person must be destroyed unless there are compelling reasons to retain it, for example, if the information reveals a communications security vulnerability or an imminent threat of serious harm to life or property.

¹³⁴ See generally 50 U.S.C. 1881a.

¹³⁵ *Id.*

- If a target reasonably believed to be a non-United States person located outside the United States either enters the United States or is discovered to be a United States person, acquisition must immediately be terminated.
- Any information collected after a non-United States person target enters the United States must promptly be destroyed, unless it constitutes evidence of criminal conduct or has significant foreign intelligence value.
- Any information collected prior to the discovery that a target believed to be a non-United States person is in fact a United States person must be promptly destroyed, unless it constitutes evidence of criminal conduct or has significant foreign intelligence value.
- The dissemination of any information about a United States person collected during the course of a section 702 acquisition is prohibited, unless it is necessary to understand foreign intelligence or assess its importance, is evidence of criminal conduct, or indicates an imminent threat of death or serious bodily injury.

Section 702 imposes substantial reporting requirements on the government in order to enable both judicial and congressional oversight, in addition to the oversight conducted within the Executive Branch by the Department of Justice (DOJ), the Office of the Director of National

Intelligence (ODNI), and the Inspectors General of the various agencies that make up the Intelligence Community:

- Approximately every 15 days, a team of attorneys from the National Security Division (NSD) of the DOJ and ODNI reviews the documentation underlying every new identifier tasked by NSA for collection. The team makes two judgments about each identifier: (1) Is the target a non-United States person reasonably believed to be located outside the United States? (2) Is the target within the categories of targets certified by the Attorney General and the DNI for collection under section 702?
- Section 702 requires the Attorney General and the DNI to provide semiannual assessments of the implementation of section 702 both to the oversight committees in Congress and to the FISC.
- The Inspector General of any intelligence agency that conducts an acquisition under section 702 must regularly review the agency's use of section 702 and provide copies of that review to the Attorney General, the DNI, and the congressional oversight committees.
- The head of any intelligence agency that conducts an acquisition under section 702 must perform an annual review of the agency's implementation of section 702 and provide copies of that review to the FISC, the Attorney

General, the DNI, and the congressional oversight committees.

- The Attorney General must make semiannual reports to the congressional intelligence and judiciary committees on the implementation of section 702.
- The Attorney General must make semiannual reports to the congressional intelligence and judiciary committees that include summaries of all significant legal decisions made by the FISC and copies of all decisions, orders, or opinions of the FISC that involve a significant interpretation of any provision of FISA, including section 702.
- The FISC requires the intelligence agencies to immediately report to the court any compliance incidents and the government reports quarterly to the FISC about the status of any previously reported compliance issues.
- An annual Inspector General assessment is provided to Congress reporting on compliance issues, the number of disseminations relating to United States persons, and the number of targets found to be located inside the United States.

In 2012, Senator Diane Feinstein (D-CA), the Chair of the Senate Select Committee on Intelligence, reported that a review of the assessments, reports, and other information available to the Committee

“demonstrate that the government implements [section 702] in a responsible manner with relatively few incidents of non-compliance. Where such incidents have arisen, they have been the inadvertent result of human error or technical defect and have been promptly reported and remedied.” Indeed, since the enactment of section 702, the Committee “has not identified a single case in which a government official engaged in a willful effort to circumvent or violate the law.”¹³⁶

Although compliance issues under section 702 have been infrequent, they have been vexing when they arise. In one instance, the FISC held that, for technical reasons concerning the manner in which the collection occurred, the minimization procedures that applied to NSA’s upstream collection¹³⁷ of electronic communications did not satisfy the requirements of either FISA or the Fourth Amendment. This was so because NSA’s use of upstream collection often involves the inadvertent acquisition of multi-communication transactions (MCTs),¹³⁸ many of which do not fall within the parameters of section 702. Judge John Bates of the FISC noted that the “government’s revelations regarding the scope of NSA’s upstream collection implicate 50 U.S.C. § 1809(a), which makes it a crime (1) to ‘engage[] in electronic surveillance under color of law except as authorized’ by statute. . . .”¹³⁹

¹³⁶ S. Rep. 112-174 (June 7, 2012).

¹³⁷ The term “upstream collection” refers to NSA’s interception of Internet communications as they transit the facilities of an Internet backbone carrier.

¹³⁸ MCTs arise in situations in which many communications are bundled together within a single Internet transmission and when the lawful interception of one communication in the bundle results in the interception of them all.

¹³⁹ *In Re DNI/AG 702(g)*, Docket Number 702(i)-11-01 (FISC October 3, 2011) (hereinafter cited as FISC Oct. 3, 2011 opinion).

Judge Bates observed that “NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702” and that the vast majority of those communications are “not at issue here.”¹⁴⁰ But, he added, the upstream collection represents “approximately 9 percent of the total Internet communications being acquired by NSA under Section 702,” and those acquisitions inadvertently sweep in “tens of thousands of wholly domestic communications” because they happen to be contained within an MCT that includes a targeted selector.¹⁴¹

In such circumstances, Judge Bates noted that the “fact that NSA’s technical measures cannot prevent NSA from acquiring transactions containing wholly domestic communications . . . does not render NSA’s acquisition of those transactions ‘unintentional.’”¹⁴² Judge Bates concluded that “NSA’s minimization procedures, as applied to MCTs,” did not meet the requirements of either FISA or the Fourth Amendment. He therefore refused to approve NSA’s continuing acquisition of MCTs.¹⁴³ Thereafter, the government substantially revised its procedures for handling MCTs, and in November 2011 Judge Bates approved the future acquisition of such communications subject to the new minimization standards.¹⁴⁴ In addition, NSA took the additional step of deleting all previously acquired upstream communications.

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.*

¹⁴³ *Id.*

¹⁴⁴ *In re DNI/AG 702(g)*, Docket Number 702(i)-11-01 (FISC November 30, 2011) (Redacted version).

According to NSA, section 702 “is the most significant tool in NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the US and around the world.” To cite just one example, collection under section 702 “was critical to the discovery and disruption” of a planned bomb attack in 2009 against the New York City subway system” and led to the arrest and conviction of Najibullah Zazi and several of his co-conspirators.¹⁴⁵

According to the Department of Justice and the Office of the Director of National Intelligence in a 2012 report to Congress:

Section 702 enables the Government to collect information effectively and efficiently about foreign targets overseas and in a manner that protects the privacy and civil liberties of Americans. Through rigorous oversight, the Government is able to evaluate whether changes are needed to the procedures or guidelines, and what other steps may be appropriate to safeguard the privacy of personal information. In addition, the Department of Justice provides the joint assessments and other reports to the FISC. The FISC has been actively involved in the review of section 702 collection. Together, all of these mechanisms ensure thorough and continuous oversight of section 702 activities. . . .

Section 702 is vital to keeping the nation safe. It provides information about the plans and identities of terrorists,

¹⁴⁵ National Security Agency, *The National Security Agency: Missions, Authorities, Oversight and Partnerships* (August 9, 2013).

allowing us to glimpse inside terrorist organizations and obtain information about how those groups function and receive support. In addition, it lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States.¹⁴⁶

In reauthorizing section 702 for an additional five years in 2012, the Senate Select Committee on Intelligence concluded:

[T]he authorities provided [under section 702] have greatly increased the government's ability to collect information and act quickly against important foreign intelligence targets. The Committee has also found that [section 702] has been implemented with attention to protecting the privacy and civil liberties of US persons, and has been the subject of extensive oversight by the Executive branch, the FISC, as well as the Congress. . . . [The] failure to reauthorize [section 702] would "result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities."¹⁴⁷

Our own review is not inconsistent with this assessment. During the course of our analysis, NSA shared with the Review Group the details of 54

¹⁴⁶ Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of the Director of National Intelligence (ODNI), Appendix to Senate Select Committee on Intelligence, *Report on FAA Sunsets Extension Act of 2012*, 112th Congress, Cong., 2d Session (June 7, 2012).

¹⁴⁷ Senate Select Committee on Intelligence, *Report on FAA Sunsets Extension Act of 2012*, 112th Congress, 2d Session (June 7, 2012).

counterterrorism investigations since 2007 that resulted in the prevention of terrorist attacks in diverse nations and the United States. In all but one of these cases, information obtained under section 702 contributed in some degree to the success of the investigation. Although it is difficult to assess precisely how many of these investigations would have turned out differently without the information learned through section 702, we are persuaded that section 702 does in fact play an important role in the nation's effort to prevent terrorist attacks across the globe.

* * * * *

Although section 702 has clearly served an important function in helping the United States to uncover and prevent terrorist attacks both in the United States and around the world (and thus helps protect our allies), the question remains whether it achieves that goal in a way that unnecessarily sacrifices individual privacy and damages foreign relations. Because the effect of section 702 on United States persons is different from its effect on non-United States persons, it is necessary to examine this question separately for each of these categories of persons.

**C. Privacy Protections for United States Persons Whose
Communications are Intercepted Under Section 702**

Recommendation 12

We recommend that, if the government legally intercepts a communication under section 702, or under any other authority that justifies the interception of a communication on the ground that it is directed at a non-United States person who is located outside the United

States, and if the communication either includes a United States person as a participant or reveals information about a United States person:

- (1) any information about that United States person should be purged upon detection unless it either has foreign intelligence value or is necessary to prevent serious harm to others;
- (2) any information about the United States person may not be used in evidence in any proceeding against that United States person;
- (3) the government may not search the contents of communications acquired under section 702, or under any other authority covered by this recommendation, in an effort to identify communications of particular United States persons, except (a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism.

Section 702 affords United States persons the same protection against foreign intelligence surveillance when they are outside the United States that FISA affords them when they are inside the United States. That is, a United States person may not lawfully be targeted for foreign intelligence surveillance unless the FISC issues a warrant based on a finding that there is probable cause to believe that the targeted United States person is an agent of a foreign power (as defined in FISA).

Section 702 has a potentially troubling impact on the privacy of communications of United States persons because of the risk of *inadvertent*

interception. The government cannot lawfully target the communications of a United States person, whether she is inside or outside the United States, without satisfying the *probable cause* requirements of both FISA and the Fourth Amendment. But in determining whether the target of any particular interception is a non-United States person who is located outside the United States, section 702 requires only that the government *reasonably believe* the target to be such a person. Because United States persons are appreciably more likely to have their constitutionally protected communications *inadvertently* intercepted under the reasonable belief standard than under the probable cause standard, the reasonable belief standard provides less protection to US persons than ordinarily would be the case.

Exacerbating that concern is the risk of *incidental interception*. This occurs when the government acquires the communications of a legally targeted individual under section 702 who is communicating with United States persons who cannot themselves be lawfully targeted for surveillance. The issue of incidental acquisition can arise whenever the government engages in electronic surveillance.

For example, if the government has probable cause to wiretap an individual's phone because he is suspected of dealing drugs, it may incidentally intercept the suspect's conversations with completely innocent persons who happen to speak with the suspect during the duration of the wiretap. In such circumstances, the standard practice in criminal law enforcement is for the government to purge from its records any reference

to the innocent person unless it reveals evidence of criminal conduct by the innocent person or provides relevant information about the guilt or innocence of the suspect.¹⁴⁸

Following a similar approach, when incidental acquisition occurs in the course of section 702 surveillance, existing minimization procedures require that any intercepted communication with a United States person, and any information obtained about a United States person in the course of a section 702 acquisition, must be destroyed—unless it has foreign intelligence value, indicates an imminent threat of death or serious bodily harm, or is evidence of a crime.¹⁴⁹

In our view, this approach does not adequately protect the legitimate privacy interests of United States persons when their communications are *incidentally* acquired under section 702. This is so for three reasons. First, when a United States person (whether inside or outside the United States) communicates with a legally targeted non-United States person who is outside the United States, there is a significantly greater risk that his communication will be acquired under section 702 than (a) if they communicated with one another when they were both inside the United States or (b) if FISA treated non-United States persons outside the United States the same way it treats United States persons outside the United States. Thus, when an American in Chicago e-mails a foreign friend abroad, there is a significantly greater chance that his e-mail will be acquired under 702 than if he e-mails an American in Paris or a foreigner in New York.

¹⁴⁸ 28 C.F.R. ch. I, Part 23.

¹⁴⁹ NSA's Section 702 Minimization Procedures.

This is so because section 702 allows the government to target the foreign friend abroad under a lower standard than if the target was the American in Paris or the foreigner in New York. For this reason, incidental interception is significantly more likely to occur when the interception takes place under section 702 than in other circumstances.

Second, it is often difficult to determine whether the e-mail address, Internet communication, or telephone number of the non-targeted participant in a legally acquired communication belongs to a United States person, because that information often is not apparent on the face of the communication. In such circumstances, there is a significant risk that communications involving United States persons will not be purged and, instead, will be retained in a government database.

Third, the very concept of information of "foreign intelligence value" has a degree of vagueness and can easily lead to the preservation of private information about even known United States persons whose communications are incidentally intercepted in the course of a legal section 702 interception.

For all of these reasons, there is a risk that, after the government incidentally collects communications of or about United States persons in the course of legal section 702 acquisitions, it will later be able to search through its database of communications in a way that invades the legitimate privacy interests of United States persons. Because the underlying rationale of section 702 is that United States persons are entitled to the full protection of their privacy even when they communicate with

non-United States persons who are outside the United States, they should not lose that protection merely because the government has legally targeted non-United States persons who are located outside the United States *under a standard that could not legally be employed to target a United States person who participates in that communication*. The privacy interests of United States persons in such circumstances should be accorded substantial protection, particularly because section 702 is not designed or intended to acquire the communications of United States persons.

Our recommended approach would leave the government free to use section 702 to obtain the type of information it is designed and intended to acquire—information about non-United States persons who are the legal targets of these investigations, while at the same time (a) more fully preserving the privacy of United States persons who are *not* the targets of these interceptions and (b) reducing the incentive the government might otherwise have to use section 702 in an effort to gather evidence against United States persons in a way that would circumvent the underlying values of both FISA and the Fourth Amendment.¹⁵⁰

¹⁵⁰ Recommendation 12(2) is designed to address this latter concern. If the government cannot use the evidence in any legal proceeding against the US person, it is less likely to use section 702 in an effort to obtain such information. On the other hand, we do not recommend prohibiting the use of the “fruits” of such interceptions. We draw the line as we do because, unlike most “fruit of the poisonous tree” situations, the interception in this situation is not itself unlawful unless it was *actually* motivated by a desire to obtain information about the US person.

D. Privacy Protections for Non-United States Persons

Recommendation 13

We recommend that, in implementing section 702, and any other authority that authorizes the surveillance of non-United States persons who are outside the United States, in addition to the safeguards and oversight mechanisms already in place, the US Government should reaffirm that such surveillance:

- (1) must be authorized by duly enacted laws or properly authorized executive orders;
- (2) must be directed *exclusively* at the national security of the United States or our allies;
- (3) must *not* be directed at illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries; and
- (4) must not disseminate information about non-United States persons if the information is not relevant to protecting the national security of the United States or our allies.

In addition, the US Government should make clear that such surveillance:

- (1) must not target any non-United States person located outside of the United States based solely on that person's political views or religious convictions; and

(2) must be subject to careful oversight and to the highest degree of transparency consistent with protecting the national security of the United States and our allies.

Because section 702 is directed specifically at non-United States persons, it raises the question whether it sufficiently respects the legitimate privacy interests of such persons. At the outset, it is important to note that, when non-citizens are *inside* the United States, our law accords them the full protection of the Fourth Amendment. They have the same right to be free of unreasonable searches and seizures as American citizens. Moreover, non-citizens who have made a commitment to our community by establishing legal residence in the United States are designated “United State persons” and, as such, are treated the same way as American citizens in terms of government surveillance—even when they are *outside* the United States. These are important protections for individuals who are not citizens of the United States.

What, though, of *non-United States* persons who are *outside* the United States? We begin by emphasizing that, contrary to some representations, section 702 does *not* authorize NSA to acquire the content of the communications of masses of ordinary people. To the contrary, section 702 authorizes NSA to intercept communications of non-United States persons who are outside the United States *only* if it reasonably believes that a particular “identifier” (for example, an e-mail address or a telephone number) is being used to communicate foreign intelligence information related to such matters as international terrorism, nuclear proliferation, or

hostile cyber activities. NSA's determinations are subjected to constant, ongoing, and independent review by all three branches of the federal government to ensure that NSA targets *only* identifiers that meet these criteria.

That still leaves the question, however, whether section 702 adequately respects the legitimate privacy interests of non-United States persons when they are in their home countries or otherwise outside the United States. If section 702 were designed to intercept the communications of United States persons, it would clearly violate the Fourth Amendment.¹⁵¹ Does it also violate the Fourth Amendment insofar as it is directed at non-United States persons who are located outside the United States? The Supreme Court has definitively answered this question in the negative.¹⁵²

Wholly apart from the Fourth Amendment, how *should* the United States treat non-United States persons when they are outside the United States? To understand the legal distinction between United States persons and non-United States persons, it is important to recognize that the special protections that FISA affords United States persons grew directly out of a distinct and troubling era in American history. In that era, the United States

¹⁵¹ Although the Supreme Court has never directly addressed this question, "every court of appeals to have considered the question" has held "that the Fourth Amendment applies to searches conducted by the United States Government against United States citizens abroad." *United States v. Verdugo-Urquidez*, 494 US 259, 283 n.7 (1990) (Brennan, J., dissenting). See *In re Terrorist Bombings of US. Embassies in East Africa*, 552 F.3d 157 (2010); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 270-271 (S.D.N.Y. 2000), *aff'd*, 552 F.3d 157 (2d Cir. 2008); David S. Kris & J. Douglas Wilson, I, *National Security Investigations and Prosecutions 2d* at 596-597 (West 2012).

¹⁵² See *United States v. Verdugo-Urquidez*, 494 US. 259, 265-266 (1990). Noting that the Fourth Amendment protects the right of "the people," the Court held that this "refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."

government improperly and sometimes unlawfully targeted American citizens for surveillance in a pervasive and dangerous effort to manipulate domestic political activity in a manner that threatened to undermine the core processes of American democracy. As we have seen, that concern was the driving force behind the enactment of FISA.

Against that background, FISA's especially strict limitations on government surveillance of United States persons reflects not only a respect for individual privacy, but also—and fundamentally—a deep concern about potential government abuse *within our own political system*. The special protections for United States persons must therefore be understood as a crucial safeguard of democratic accountability and effective self-governance within the American political system. In light of that history and those concerns, there is good reason for every nation to enact *special* restrictions on government surveillance of those persons who participate directly in its own system of self-governance.

As an aside, we note that the very existence of these protections in the United States can help promote and preserve democratic accountability across the globe. In light of the global influence of the United States, any threat to effective democracy in the United States could have negative and far-reaching consequences in other nations as well. By helping to maintain an effective system of checks and balances within the United States, the special protections that FISA affords United States persons can therefore contribute to sustaining democratic ideals abroad.

That brings us back, however, to the question of how the United States should treat non-United States persons who are not themselves either a part of our community or physically located in the United States. As a general rule, nations quite understandably treat their own citizens differently than they treat the citizens of other nations. On the other hand, there are sound, indeed, compelling reasons to treat the citizens of other nations with dignity and respect. As President Franklin Delano Roosevelt observed, the United States should be a “good neighbor.” Sometimes this is simply a matter of national self-interest. If the United States wants other nations to treat our citizens well, we must treat their citizens well. But there are other reasons for being a “good neighbor.”

If we are too aggressive in our surveillance policies under section 702, we might trigger serious economic repercussions for American businesses, which might lose their share of the world’s communications market because of a growing distrust of their capacity to guarantee the privacy of their international users. Recent disclosures have generated considerable concern along these lines.

Similarly, unrestrained American surveillance of non-United States persons might alienate other nations, fracture the unity of the Internet, and undermine the free flow of information across national boundaries. This, too, is a serious concern that cuts in favor of restraint.

Perhaps most important, however, is the simple and fundamental issue of respect for personal privacy and human dignity – wherever people may reside. The right of privacy has been recognized as a basic human

right that all nations should respect. Both Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights proclaim that “No one shall be subjected to arbitrary or unlawful interference with his privacy. . . .” Although that declaration provides little guidance about what is meant by “arbitrary or unlawful interference,” the aspiration is clear. The United States should be a leader in championing the protection by all nations of fundamental human rights, including the right of privacy, which is central to human dignity.

At this moment in history, one of the gravest dangers to our national security is international terrorism. Faced with that continuing and grave threat, the United States must find effective ways to identify would-be terrorists who are not located in the United States, who move freely across national borders, and who do everything in their power to mask their identities, intentions, and plans. In such circumstances, the challenge of striking a sound balance between protecting the safety and security of our own citizens and respecting the legitimate interests of the citizens of other nations is especially daunting. Our recommendations have been designed to achieve that balance.

With our recommendations in place, there would be three primary differences between the standards governing the acquisition of communications of United States persons and non-United States persons under section 702 when they are outside the United States. First, United States persons can be targeted only upon a showing of probable cause,

whereas non-United States persons can be targeted upon a showing of reasonable belief. Second, United States persons can be targeted only if there is a judicial warrant from the FISC, whereas non-United States persons can be targeted without such a warrant, but with careful after-the-fact review and oversight. Third, the minimization requirements for communications of United States persons would not extend fully to non-United States persons located outside the United States, but importantly, information collected about such persons would not be disseminated unless it is relevant to the national security of the United States or our allies.

In our judgment, these differences are warranted by the *special* obligation the United States Government owes to “the people” of the United States, while at the same time more than upholding our international obligation to ensure that no person “shall be subjected to arbitrary or unlawful interference with his privacy.” We encourage all nations to abide by these same limitations.¹⁵³

Recommendation 14

We recommend that, in the absence of a specific and compelling showing, the US Government should follow the model of the Department of Homeland Security, and apply the Privacy Act of 1974 in the same way to both US persons and non-US persons.

¹⁵³ It is important to note that although the government should not target a non-US person outside the United States for surveillance *solely* because of his political or religious activity or expression, it may target such an individual for surveillance if it has reason to believe that he poses a threat to US national security.

The Privacy Act of 1974¹⁵⁴ provides what are known as “privacy fair information practices” for systems of records held by federal agencies. These practices, designed to safeguard personal privacy, include a set of legal requirements meant to ensure both the accuracy and the security of personally identifiable information in a system of records. Perhaps most important, individuals have the right to have access to those records and to make corrections, if needed.

Since its enactment, the Act has applied only to United States persons. In 2009, the Department of Homeland Security (DHS) updated its 2007 “Privacy Policy Guidance Memorandum.”¹⁵⁵ This memorandum governs privacy protections for “mixed systems” of records—systems that collect or use information in an identifiable form and that contain information about both United States and non-United States persons.¹⁵⁶

Today, DHS policy applies the Privacy Act in the same way to both US persons and non-US persons. As stated in the Memorandum, “As a matter of law the Privacy Act . . . does not cover visitors or aliens. As a matter of DHS policy, any personally identifiable information (PII) that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a US citizen, legal permanent resident, visitor, or alien.”¹⁵⁷

¹⁵⁴ 5 U.S.C. § 552(a).

¹⁵⁵ Department of Homeland Security: Privacy Policy Guidance Memorandum No. 2007-1 (January 7, 2007) (amended on January 19, 2007).

¹⁵⁶ *Id.*

¹⁵⁷ *Id.*

The consequence of this policy is that DHS now handles non-US person PII held in mixed systems in accordance with the fair information practices set forth in the Privacy Act. Non-US persons have the right of access to their PII and the right to amend their records, absent an exemption under the Privacy Act. Because of statutory limitations, the policy does not extend or create a right of judicial review for non-US persons.

Intelligence agencies today are covered by the Privacy Act, with exemptions to accommodate the need to protect matters that are properly classified or law-enforcement sensitive/investigatory in nature. For instance, NSA has filed twenty-six systems of records notices advising the public about data collections, including from applicants seeking employment, contractors doing business with the agency, and in order to conduct background investigations.

NSA also completes privacy impact assessments under the E-Government Act of 2002¹⁵⁸ for its non-National Security Systems that collect, maintain, use, or disseminate PII about members of the public. CIA provides protections under the Privacy Act in contexts including collection directly from the individual; records describing individuals' exercise of First Amendment rights; and the Act's general prohibition on disclosure absent express written consent of the individual. The FBI applies the Privacy Act in the same manner for national security investigations as it does for other records covered by the Act.

¹⁵⁸ 44 U.S.C. § 101.

Unless the agencies provide specific and persuasive reasons not to do so, we recommend that the DHS policy should be extended to the mixed systems held in intelligence and other federal agencies. DHS policy has existed for several years for major record systems of records, including passenger name records and immigration records, and implementation experience from DHS can guide similar privacy protections for PII held in intelligence and other federal agencies.

Appropriate exception authority appears to exist under the Act, including for National Security Systems and law enforcement investigatory purposes. The previous lack of Privacy Act protections has been a recurring complaint from European and other allies. This reform is manageable based on the DHS experience. It will both affirm the legitimate privacy rights of citizens of other nations and strengthen our relations with allies.

Recommendation 15

We recommend that the National Security Agency should have a limited statutory emergency authority to continue to track known targets of counterterrorism surveillance when they first enter the United States, until the Foreign Intelligence Surveillance Court has time to issue an order authorizing continuing surveillance inside the United States.

Under current law, a problem arises under current law when known targets of counterterrorism surveillance enter the United States. Surveillance of a target has been legally authorized under the standards that apply overseas, under Section 702 or Executive Order 12333. Suddenly, the target is found to be in the United States, where surveillance

is permitted only under stricter legal standards. Under current law, NSA must cease collecting information as soon as it determines that the individual is within the United States. The surveillance can begin again only once there is new authorization under FISA. The irony of this outcome is that surveillance must cease at precisely the moment when the target has entered the United States and thus is in position to take hostile action. Colloquially, there can be a costly fumble in the hand-off from overseas to domestic surveillance.

To address this gap in coverage, legislation has been proposed that would amend 50 U.S.C. § 1805 to give the Director of NSA emergency authority to acquire foreign intelligence information in such circumstances for up to 72 hours. We believe that some such authority is appropriate. A similar gap occurs where the target of surveillance overseas was originally thought to be a non-US person and then is found actually to be a US person. At the moment the target is being investigated for counterterrorism purposes, the authorities that permitted the surveillance no longer apply.

The gap in coverage arises due to the different legal standards that apply at home and abroad. Surveillance under Section 702 is permitted if there is a reasonable belief that the person is not a US person and is located outside of the US, and if the purpose is to acquire foreign intelligence information subject to an existing certification. Surveillance under Executive Order 12333 is done so long as it is related to foreign intelligence. By contrast, a traditional FISA order for surveillance within the US requires probable cause that the person is an agent of a foreign power. In order to

target a US person who is outside of the US under FISA section 704, the government must show facts for reasonably believing that the person is outside of the US and is an agent of a foreign power. It can take time and effort to upgrade the factual findings from what enabled the surveillance within NSA under Section 702 or Executive Order 12333 to the findings that the Department of Justice needs to meet under a traditional FISA order or one under section 704.

The precise scope of this hand-off authority deserves careful thought. The proposed legislation would allow seventy-two hours for surveillance on order of the NSA Director, followed by additional days of emergency authority by authorization of the Attorney General. There has been discussion of whether to limit the scope to situations where there is an imminent threat of death or serious bodily harm, or to go somewhat broader and allow the hand-off authority for any counterterrorism investigation. Additional facts and public discussion would be helpful to assessing such questions.

However these questions of scope are resolved, it can be difficult in our era of mobile phones and e-mail addresses to determine when a communication is made within the United States. Where the communication unexpectedly is within our borders, or someone thought to be a non-US person is found to be a US person, there should be a capacity to respond to an emergency situation.

Chapter V

Determining What Intelligence Should Be Collected and How

The United States led the defense of the Free World in the Cold War. After having been targeted by terrorist groups, it led the global community's efforts to combat violent extremism. Over time, the United States has developed a large Intelligence Community with unparalleled collection capabilities. The Intelligence Community collects information essential not only to our national security but also to that of many allied and friendly nations. The unsurpassed prowess of US technical intelligence collection is a major component of the maintenance of peace and security of the United States and many other nations.

Intelligence collection is designed to inform policymakers, warfighters, and law enforcement officers who are responsible for making decisions and taking actions to protect the United States and its allies. Intelligence collection is not an end in itself. Intelligence collection should not occur because it is possible, but only because it is *necessary*.

Intelligence, particularly signals intelligence, is as necessary now as ever to combat violent extremism, prevent the proliferation of nuclear weapons, combat international criminal groups, prevent atrocities, and enforce UN sanctions and other international regimes. With the passage of a dozen years since the attacks of September 11, 2001, the threat from al-Qa'ida and similar groups has changed, but it remains significant. For

example, recent years have seen the spread of al-Qa'ida-related groups to large swaths of Africa and the Middle East. We have also witnessed a rise in "Lone Wolf" terrorism, including in the United States. There is a continuing need for appropriate intelligence collection, data analysis, and information-sharing with appropriate personnel. So, too, there is a need for appropriate controls and oversight on intelligence collection to ensure that we act in ways that are both consistent with our values and reflective of our security requirements.

To ascertain those requirements, the US Government has created a process known as the National Intelligence Priorities Framework (NIPF). While this process to produce intelligence priorities is the most robust ever used by the Intelligence Community, we believe that the NIPF system can and should be strengthened to ensure that what we seek to collect is truly needed and that our methods of collection are consistent with our values and policies.

A. Priorities and Appropriateness

To ascertain what intelligence is necessary to collect, policy officials and intelligence officers interact to establish intelligence needs or requirements and then priorities within those requirements. This process has been formalized into the NIPF.

The NIPF divides all intelligence collection needs identified by policymakers into five categories or tiers in increasing degrees of importance. Tiers One and Two reflect the priorities of the nation, as articulated by the President, following priority identification and review by

sub-Cabinet-level officials in the National Security Council (NSC) Deputies Committee and then by Cabinet-level officials in the NSC Principals Committee. Tiers Three, Four, and Five reflect information needed by other government agencies and programs to carry out their legal mandates. The review process for Tiers Three through Five is coordinated by the Director of National Intelligence and involves policy officials at levels below the Principals and Deputies.

The NIPF is reviewed, approved, and issued annually. Once an intelligence priority is approved, it is converted into a specific collection plan. Coordination of the collection is conducted by the Office of the Director of National Intelligence.

Many intelligence priorities result in collection on a global basis. For example, an intelligence priority to monitor al-Qa'ida threats may mean collecting information not only in Afghanistan and Pakistan, where al-Qa'ida is headquartered, but also in scores of nations to which al-Qa'ida and its supporters have moved or emerged and which they might threaten.

Enforcement of UN and other sanctions, stopping the proliferation of materials needed for nuclear weapons, halting the trafficking in persons, combating illicit drugs and criminal cartels, reducing the risk of mass atrocities, detecting the systematic violation of ethnic minority rights, and the detection of war crimes are all examples of intelligence priorities that require the collection of information in many nations. Often other governments will not have the ability to collect information on these requirements within their borders. Sometimes, they will intentionally seek

to deny the international community information about these concerns. The United States regularly shares information about these issues with allied and cooperating governments, and with international organizations.

The United States is hardly alone in collecting such intelligence. Most nations collect intelligence, often limited only by their ability and resources. Indeed, the United States is an intelligence collection target of many nations, including friendly and even allied countries. The President's own communications are a collection target for many nations, friendly and otherwise.

One thing that makes United States intelligence collection unique is the degree of oversight and control by high-level officials, elected legislative members, and the judiciary (see Appendix C). No other intelligence services in the world are subjected to the degree of policy, legislative, and judicial review now applied to the US Intelligence Community. In our view, however, that oversight can be improved. The current NIPF process does not provide sufficient high-level oversight of a) lower-tier priorities; b) the specific means used to collect information on a priority; c) the locations where collection on a priority may occur; and d) developments that occur between annual reviews.

This NIPF process should be strengthened to assure that sensitive collection is undertaken only after consideration of all national interests and with the participation of those officials who have responsibility for those interests. The following should be added to the process: (1) senior-level "interagency" policy oversight of *all* sensitive requirements, rather

than only the requirements in Tier One and Tier Two; (2) participation in the process by all the departments and agencies with relevant concerns, including economic ones; and (3) senior-level knowledge of and approval of specific targets of collection whenever the target or collection means is a sensitive one. We discuss below what constitutes a “sensitive” collection activity.

The rationale behind these recommendations is simple. Senior policymakers should determine the activities of intelligence agencies; senior policymakers are the only participants with the breadth of experience to make such decisions; and any senior policymaker with relevant expertise and perspective should participate in policy formulation on sensitive collection.

B. Monitoring Sensitive Collection

Recommendation 16

We recommend that the President should create a new process requiring high-level approval of all sensitive intelligence requirements and the methods the Intelligence Community will use to meet them. This process should, among other things, identify both the uses and limits of surveillance on foreign leaders and in foreign nations. A small staff of policy and intelligence professionals should review intelligence collection for sensitive activities on an ongoing basis throughout the year and advise the National Security Council Deputies and Principals when they believe that an unscheduled review by them may be warranted.

Recommendation 17

We recommend that:

- (1) senior policymakers should review not only the requirements in Tier One and Tier Two of the National Intelligence Priorities Framework, but also any other requirements that they define as sensitive;
- (2) senior policymakers should review the methods and targets of collection on requirements in any Tier that they deem sensitive; and
- (3) senior policymakers from the federal agencies with responsibility for US economic interests should participate in the review process because disclosures of classified information can have detrimental effects on US economic interests.

Recommendation 18

We recommend that the Director of National Intelligence should establish a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers. To this end, the Director of National Intelligence should prepare an annual report on this issue to the National Security Advisor, to be shared with the Congressional intelligence committees.

We believe that the definition of what is “sensitive,” and therefore should be reviewed in this strengthened NIPF, will vary with time. Among the factors that might make something sufficiently “sensitive” to require

senior interagency-level review are 1) the means that would be employed to collect information, 2) the specific people subject to collection, 3) the nation where the collection would occur, 4) international events such as a head-of-state meeting or negotiations, or 5) a combination of these factors.

Intelligence collection managers may not always be aware that what they are doing or planning might fall into a category that makes it sensitive in the eyes of policymakers. Senior policymakers may not be aware that a collection effort they previously approved has become “sensitive” over time.

We recommend that a standing group or office should review collection activities for “sensitive” activities on an ongoing basis. This Sensitive Activities Office should include both policymakers and intelligence collection managers, assigned perhaps for 12-18 month rotations. The Sensitive Activities Office would nominate collection efforts for senior-level consideration if necessary between annual NIPF reviews.

The Sensitive Activities Office should include staff from non-traditional national security organizations such as the National Economic Council, Treasury, Commerce, and the Trade Representative. In addition, any department should be able to request a review of ongoing intelligence collection by the Sensitive Activities Office at any time, in light of new developments or evolving situations of which they are aware. The Sensitive Activities Office should be housed and supported by the ODNI, but should report regularly, through the DNI, to a policy-level official in the National Security Staff (NSS).

The goal of this strengthened NIPF is to ensure that the United States collects all of the information it legitimately needs and as little more than that as possible, and that we collect not because we can, but because we must for our national security, that of our allies, and in support of the international community.

Toward that end, the Principals reviewing intelligence collection should re-institute use of the so-called "Front-Page Rule." That informal precept, long employed by the leaders of US administrations, is that we should not engage in any secret, covert, or clandestine activity if we could not persuade the American people of the necessity and wisdom of such activities were they to learn of them as the result of a leak or other disclosure. The corollary of that rule is that if a foreign government's likely negative reaction to a revealed collection effort would outweigh the value of the information likely to be obtained, then do not do it.

C. Leadership Intentions

Recommendation 19

We recommend that decisions to engage in surveillance of foreign leaders should consider the following criteria:

- (1) Is there a need to engage in such surveillance in order to assess significant threats to our national security?**
- (2) Is the other nation one with whom we share values and interests, with whom we have a cooperative relationship, and whose leaders we should accord a high degree of respect and deference?**

- (3) Is there a reason to believe that the foreign leader may be being duplicitous in dealing with senior US officials or is attempting to hide information relevant to national security concerns from the US?**
- (4) Are there other collection means or collection targets that could reliably reveal the needed information?**
- (5) What would be the negative effects if the leader became aware of the US collection, or if citizens of the relevant nation became so aware?**

The United States, like all governments, seeks to learn the real intentions of leaders of many nations. Historically, some national leaders may have told the United States one thing in diplomatic channels, and then secretly ordered a very different set of actions. Often the “easiest” way to determine or verify intentions may seem to be to monitor leadership communications.

We believe, however, that any decision to engage in surveillance of the leaders of a foreign nation must be taken with great care. For a variety of reasons, the stakes in such decisions can be quite high. Although general principles may not themselves resolve close and difficult cases, they can help to ensure a proper focus on the relevant considerations and a degree of consistency in our judgments. Here as elsewhere, risk management is central. The decision to engage in surveillance of foreign leaders must address and manage multiple risks.

The first task in this inquiry must be to consider the various purposes for which such information might be sought. In some instances, information might be sought in order to reduce significant risks to national security or to learn the views of foreign leaders regarding critical national security issues, where those views have not been shared with the United States. In other instances, information might be sought in order to learn about the intentions of the leaders of other nations, even when no threat to our national security is involved. The latter instances might involve an interest in acquiring information that might prove useful as United States officials plan for meetings and discussions with other nations on bilateral economic issues. In such circumstances, it might be helpful to know in advance about another nation's internal concerns and priorities or about its planned negotiating strategy but it is not critical to national security. Different interests have different weights.

The second task is to consider the nations from whom information might be collected. In some instances, we might seek to collect information from the leaders of nations with whom the United States has a hostile relationship. Other nations are our friends and allies, and we may have close and supportive relationships with them.

In making judgments about whether to engage in surveillance of foreign leaders, we suggest that these questions should be considered: (1) Is there a need to engage in such surveillance in order to assess significant threats to our national security? (2) Is the other nation one with whom we share values and interests, with whom we have a cooperative relationship,

and whose leaders we should accord a high degree of respect and deference? (3) Is there a reason to believe the foreign leader may be being duplicitous in dealing with senior US officials or is attempting to hide information relevant to national security concerns from the US? (4) Are there other collection means or collection targets that could reliably reveal the needed information? (5) What would be the negative effects if the leader became aware of the US collection, or if citizens of the relevant nation became so aware? These questions can helpfully orient sensitive judgments.

Recommendation 20

We recommend that the US Government should examine the feasibility of creating software that would allow the National Security Agency and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk-data collection.

In the course of our review, we have been struck by the fact that the nature of IT networks and current intelligence collection technology is such that it is often necessary to ingest large amounts of data in order to acquire a limited amount of required data. E-mails, telephone calls, and other communications are moved on networks as a series of small packets, then reassembled at the receiving end. Often those packets are interspersed in transit with packets from different originators. To intercept one message, pieces of many other messages might be recorded and placed in government databases, at least temporarily. Frequently, too, it is more cost-effective and less likely to be detected by the transmitter if the collection of

a message occurs in transit, mixed up with many others, rather than at the source.

It might reduce budgetary costs and political risk if technical collection agencies could make use of artificial intelligence software that could be launched onto networks and would be able to determine in real time what precise information packets should be collected. Such smart software would be making the sorting decision online, as distinguished from the current situation in which vast amounts of data are swept up and the sorting is done after it has been copied on to data storages systems. We are unable to determine whether this concept is feasible or fantasy, but we suggest that it should be examined by an interagency information technology research team.

D. Cooperation with Our Allies

Recommendation 21

We recommend that with a small number of closely allied governments, meeting specific criteria, the US Government should explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens (including, if and where appropriate, intentions, strictures, or limitations with respect to collections). The criteria should include:

- (1) shared national security objectives;
- (2) a close, open, honest, and cooperative relationship between senior-level policy officials; and

(3) a relationship between intelligence services characterized both by the sharing of intelligence information and analytic thinking and by operational cooperation against critical targets of joint national security concern. Discussions of such understandings or arrangements should be done between relevant intelligence communities, with senior policy-level oversight.

We suggest that the US Government should work with closely allied nations to explore understanding or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens. It is important to emphasize that the United States has not entered into formal agreements with other nations not to collect information on each others' citizens. There are no such formal agreements. With a very small number of governments, however, there are bilateral arrangements or understandings on this issue (which include, in appropriate cases, intentions, strictures, and limitations with respect to collection). These bilateral relationships are based on decades of familiarity, transparency, and past performance between the relevant policy and intelligence communities.

The United States should be willing to explore the possibility of reaching similar arrangements and understandings with a small number of other closely allied governments. Such relationships should be entered into with care and require senior policy-level involvement. We anticipate that only a very few new such relationships are likely in the short to medium term.

In choosing with which nations to have such discussions, the US Government should have explicit criteria in mind and should share those criteria with interested governments. The criteria should include (1) shared national security policy objectives between the two governments; (2) a close, open, and honest relationship between the policy officials of the two nations; and (3) a close working relationships between the countries' intelligence services, including the sharing of a broad range of intelligence information; analytic and operational cooperation involving intelligence targets of common interest; and the ability to handle intelligence information with great care.

The US Government has indicated that it is considering disclosing publicly the procedures that the Intelligence Community follows in the handling of foreign intelligence information it collects pertaining to non-US persons. We encourage the Government to make such procedures known. The individual agencies' performance in implementing these procedures should be overseen both by the Director of National Intelligence—with regular reports to senior-level policy officials—and by the two Congressional Intelligence Committees.

Chapter VI

Organizational Reform in Light of Changing Communications Technology

A. Introduction

A central theme of this Report is the importance of achieving multiple goals, including: (1) combating threats to the national security; (2) protecting other national security and foreign policy interests; (3) assuring fundamental rights to privacy; (4) preserving democracy, civil liberties, and the rule of law; (5) supporting a robust, innovative, and free Internet; and (6) protecting strategic relationships. This chapter identifies organizational structures designed to achieve these goals in light of changes in communications technology.

For reasons deeply rooted in the history of the intelligence enterprise, the current organizational structure has been overwhelmingly focused on the goal of combating threats to national security. NSA grew out of signals intelligence efforts during World War II. From then until the end of the Cold War, NSA targeted its efforts on nation states, outside of the US, often in foreign combat zones that were distant from home.

By contrast, our intelligence efforts now target nonstate actors, including terrorist organizations for whom borders are often not an obstacle. As the Section 215 program illustrates, the traditional distinction between foreign and domestic has become less clear. The distinction between military and civilian has also become less clear, now that the same

communications devices, software, and networks are used both in war zones such as Iraq and Afghanistan and in the rest of the world. Similarly, the distinction between war and non-war is less clear, as the United States stays vigilant against daily cyber security attacks as well as other threats from abroad.

The organizational structure of the Intelligence Community should reflect these changes. Today, communications devices, software, and networks are often “dual-use”—used for both military and civilian purposes. Both military and civilian goals are thus implicated by signals intelligence and surveillance of communications systems. Chapter V addressed the need for a new policy process to oversee sensitive intelligence collections, drawing on multiple federal agencies and multiple national goals. This chapter identifies key organizational changes, including:

- Re-organization of NSA to refocus the agency on its core mission of foreign intelligence;
- Creation of a new Civil Liberties and Privacy Protection Board (CLPP Board) to expand beyond the statutory limits of the existing Privacy and Civil Liberties Oversight Board (PCLOB); and
- Changes to the FISC to create a Public Interest Advocate, increase transparency, and improve the appointment process.

B. The National Security Agency

We recommend major changes to the structure of the National Security Agency. There should be greater civilian control over the agency, including Senate confirmation for the Director and openness to having a civilian Director. NSA should refocus on its core function: the collection and use of foreign intelligence information. To distinguish the warfighting role from the intelligence role, the military Cyber-Command should not be led by the NSA Director. Because the defense of both civilian and government cyber-systems has become more important in recent years, we recommend splitting the defensive mission of NSA's Information Assurance Directorate into a separate organization.

Before discussing these recommendations, we offer some general observations. No other organization in the world has the breadth and depth of capabilities NSA possesses; its prowess in the realm of signals intelligence is extraordinary. Since World War II, NSA and its predecessors have worked to keep our nation and our allies safe from attack. SIGINT collected by NSA is used daily to support our warfighters and to combat terrorism, the proliferation of weapons of mass destruction, and international criminal and narcotics cartels. Its successes make it possible for the United States and our allies around the world to safeguard our citizens and prevent death, disaster, and destruction.

In addition to its leading-edge technological developments and operations, NSA employs large numbers of highly trained, qualified, and professional staff. The hard work and dedication to mission of NSA's work

force is apparent. NSA has increased the staff in its compliance office and addressed many concerns expressed previously by the FISC and others.

After the terrorist acts in the United States of September 11, 2001, many people in both the Legislative and Executive Branches of government believed that substantial new measures were needed to protect our national security. We have noted that if a similar or worse incident or series of attacks were to occur in the future, many Americans, in the fear and heat of the moment, might support new restrictions on civil liberties and privacy. The powerful existing and potential capabilities of our intelligence and law enforcement agencies might be unleashed without adequate controls. Once unleashed, it could be difficult to roll back these sacrifices of freedom.

Our recommendations about NSA are designed in part to create checks and balances that would make it more difficult in the future to impose excessive government surveillance. Of course, no structural reforms create perfect safeguards. But it is possible to make restraint more likely. Vigilance is required in every age to maintain liberty.

1. "Dual-Use" Technologies: The Convergence of Civilian Communications and Intelligence Collection

Our recommended organizational changes are informed by the recent history of communications technologies. For the most part, signals intelligence during World War II and the Cold War did not involve collection and use on the equipment and networks used by ordinary Americans. Signals intelligence today, by contrast, pervasively involves

the communications devices, software, and networks that are also used by ordinary Americans and citizens of other countries. When the equipment and networks were separate, there was relatively little reason for decisions about signals intelligence to be part of a wide-ranging policy inquiry into the interest of the United States. But when the devices, software, and networks are the same as those used by ordinary Americans (and ordinary citizens of other countries), then multiple and significant policy concerns come into play.

As a result of changing technology, key distinctions about intelligence and communications technology have eroded over time: state vs. nonstate, foreign vs. domestic, war vs. non-war, and military vs. civilian. As a result, many communications technologies today are “dual-use” – used for both civilian and military purposes. For ordinary civilians, this means that our daily communications get swept up into Intelligence Community databases. For the military, it means that what used to be purely military activities often now have important effects on private citizens.

1. *From nation-states to well-hidden terrorists.* During the Cold War, our intelligence efforts were directed against foreign powers, notably the Soviet Union, and agents of foreign powers, such as Soviet agents in the US who were placed under FISA wiretap orders. After the terrorist attacks of September 11, 2001, the emphasis shifted to fighting terrorism. In counterterrorism efforts, a major priority is to identify potential or actual

terrorists, who seek to hide their communications in the vast sea of other communications.

The Section 215 telephone database, for instance, was designed to find links between suspected terrorists and previously unknown threats. It is one of many databases created after the terrorist attacks of September 11, 2001 in order to “connect the dots” and discover terrorist threats. One result of the focus on counterterrorism has been that the Intelligence Community has broadened its focus from state actors to a large number of nonstate actors. Another result is that the communications of ordinary citizens are placed into intelligence databases, increasing the effects of SIGINT policy choices on individuals and businesses.

2. *From domestic to foreign.* For ordinary citizens, the distinction between domestic and foreign communications has eroded over time. As the Director of National Intelligence, General James Clapper, has testified before Congress,¹⁵⁹ much of the intelligence collection during the Cold War occurred in separate communications systems. Behind the Iron Curtain, the communications of the Soviet Union and its allies were largely separate from other nations. Direct communications from ordinary Americans to Communist nations were a tiny fraction of electronic communications. By contrast, the Internet is global. Terrorists and their allies use the same Internet as ordinary Americans.

¹⁵⁹ Potential Changes to the Foreign Intelligence Surveillance Act: Open Hearing Before the H.P. Select Comm. on Intelligence, 113 Cong. (October 29, 2013) (Statement of James R. Clapper, Director of National Intelligence).

During the Cold War, ordinary Americans used the telephone for many local calls, but they were cautious about expensive “long-distance” calls to other area codes and were even more cautious about the especially expensive “international” phone calls. Many people today, by contrast, treat the idea of “long-distance” or “international” calls as a relic of the past. We make international calls through purchases of inexpensive phone cards or free global video services. International e-mails are cost-free for users.

The pervasively international nature of communications today was the principal rationale for creating Section 702 and other parts of the FISA Amendments Act of 2008. In addition, any communication on the Internet might be routed through a location outside of the United States, in which case FISA does not apply and collection is governed under broader authorities such as Executive Order 12333. Today, and unbeknownst to US users, websites and cloud servers may be located outside the United States. Even for a person in the US who never knowingly sends communications abroad, there may be collection by US intelligence agencies outside of the US.¹⁶⁰ The cross-border nature of today’s communications suggests that when decisions are made about foreign surveillance, there is a need for greater consideration of policy goals involving the protection of civilian commerce and individual privacy.

¹⁶⁰ See Jonathan Mayer, “The Web is Flat” Oct. 30, 2013 (study showing “pervasive” flow of web browsing data outside of the US for US individuals using US-based websites), available at <http://webpolicy.org/2013/10/30/the-web-is-flat/>.

3. *From wartime to continuous responses to cyber and other threats.* In recent decades, the global nature of the Internet has enabled daily cyber-attacks on the communications of government, business, and ordinary Americans by hackers, organized crime, terrorists, and nation-states. As a result, the development of high-quality defenses against such attacks has become a priority for civilian as well as military systems. In wartime, the military anticipates that the adversary will try to jam communications and take other measures to interfere with its ability to carry out operations. For this reason, the military has long required an effective defensive capability for its communications, called an “information assurance” capability. With cyber-attacks, often launched from overseas, information assurance now is needed outside the military context as well.

The convergence of military and civilian systems for cyber security has three implications. First, information assurance for the military relies increasingly on information assurance in the civilian sector. With the use of commercial off-the-shelf hardware and software, many military systems are now the same as or similar to civilian systems. The military and the US Government rely on a broad range of critical infrastructure, which is mostly owned and operated by the civilian sector. Effective defense of civilian-side hardware, software, and infrastructure is critical to military and other government functions.

Second, the military chain of command does not apply to the civilian sector. For traditional information assurance, the military could depend on its own personnel and systems to fix communications problems caused by

the adversary—the military could secretly order its personnel how to respond to a problem. But that sort of chain of command does not work in the civilian sector, where patches and other defensive measures must be communicated to a multitude of civilian system owners. It is usually not possible to communicate effective defensive measures without also tipping off adversaries about our vulnerabilities and responses.

Third, these changes create a greater tension between offense and defense. When the military can keep secrets within the chain of command, then the offensive measures used in intelligence collection or cyber attacks can safely go forward. The offense remains useful, and the military can defend its own systems. Where there is no chain of command, however, there is no secret way for the defenders to patch their systems. Those charged with offensive responsibilities still seek to collect SIGINT or carry out cyber attacks. By contrast, those charged with information assurance have no effective way to protect the multitude of exposed systems from the attacks. The SIGINT function and the information assurance function conflict more fundamentally than before. This conclusion supports our recommendation to split the Information Assurance Directorate of NSA into a separate organization.

4. *From military combat zones to civilian communications.* An important change, which has received relatively little attention, concerns the military significance of the communications devices, software, and networks used by ordinary Americans. In certain ways the military nature of signals intelligence is well known—NSA is part of the Department of

Defense (DOD), the current Director of NSA is a general, and the military's Cyber Command is led by the same general. Much less appreciated are (1) the possible effect that active combat operations in Iraq and Afghanistan have had on decisions about what intelligence activities are appropriate and (2) the increasing overlap between signals intelligence for military purposes and the communications of ordinary Americans and citizens of other countries.

The convergence of military and civilian communications is important in light of the drastically different expectations of government surveillance. In wartime, during active military operations, signals intelligence directed at the enemy must be highly aggressive and largely unrestrained. The United States and its allies gained vital military intelligence during World War II by breaking German and Japanese codes. During the Cold War, the United States established listening stations on the edges of the Soviet Union in order to intercept communications. More recently, there are powerful arguments for strong measures to intercept communications to prevent or detect attacks on American troops in Iraq and Afghanistan. During military operations, the goal is information dominance, to protect the lives and safety of US forces and to meet military objectives. The same rules do not apply on the home front.

A significant challenge today is that a wide and increasing range of communications technologies is used in both military and civilian settings. The same mobile phones, laptops, and other consumer goods used in combat zones are often used in the rest of the world. The same is true for

software, such as operating systems, encryption protocols, and applications. Similarly, routers, fiber optic, and other networking features link combat zones with the rest of the global Internet. Today, no battlefield lines or Iron Curtain separates the communications in combat zones from the rest of the world. A vulnerability that can be exploited on the battlefield can also be exploited elsewhere. The policy challenge is how to achieve our military goals in combat zones without undermining the privacy and security of our communications elsewhere. In responding to this challenge, it remains vital to allow vigorous pursuit of military goals in combat zones and to avoid creating a chilling effect on the actions of our armed forces there.

The public debate has generally focused on the counterterrorism rationale for expanded surveillance since the terrorist attacks of September 11, 2001. We believe that the military missions in Iraq and Afghanistan have also had a large but difficult-to-measure impact on decisions about technical collection and communications technologies. Going forward, even where a military rationale exists for information collection and use, there increasingly will be countervailing reasons not to see the issue in purely military terms. The convergence of military and civilian communications supports our recommendations for greater civilian control of NSA as well as a separation of NSA from US Cyber Command. It is vital for our intelligence agencies to support our warfighters, but we must develop governance structures attuned to the multiple goals of US policy.

2. Specific Organizational Reforms

Recommendation 22

We recommend that:

- (1) the Director of the National Security Agency should be a Senate-confirmed position;
- (2) civilians should be eligible to hold that position; and
- (3) the President should give serious consideration to making the next Director of the National Security Agency a civilian.

The Director of NSA has not been a Senate-confirmed position; selection has been in the hands of the President alone. Because of the great impact of NSA actions, the need for public confidence in the Director, the value of public trust, and the importance of the traditional system of checks and balances, Senate confirmation is appropriate. Senate confirmation would increase both transparency and accountability.

When appointing the directors of other intelligence organizations, Presidents have exercised their discretion to choose from the ranks of both civilian and military personnel. Both active duty military officers and civilians have been selected to be the Director of the CIA and the Director of the National Reconnaissance (NRO). It is important to the future of NSA that it be understood by the American people to be acting under appropriate controls and supervision.

For this reason, civilians should be eligible for the position. The convergence of civilian and military communications technology makes it

increasingly important to have civilian leadership to complement NSA's military and intelligence missions. We believe that the President should seriously consider appointing a civilian to be the next Director of NSA, thus making it clear that NSA operates under civilian control. A senior (two or three-star) military officer should be among the Deputy Directors.

Recommendation 23

We recommend that the National Security Agency should be clearly designated as a foreign intelligence organization; missions other than foreign intelligence collection should generally be reassigned elsewhere.

NSA now has multiple missions and mandates, some of which are blurred, inherently conflicting, or both. Fundamentally, NSA is and should be a foreign intelligence organization. It should not be a domestic security service, a military command, or an information assurance organization. Because of its extraordinary capabilities, effective oversight must exist outside of the Agency.

In some respects, NSA is now both a military and a civilian organization. It has always been led by a military flag rank officer, and its incumbent also serves as the head of a combatant command (US Cyber Command). As matter of history, the evolution in the roles and missions of NSA is understandable; those roles have emerged as a result of a series of historical contingencies and perceived necessities and conveniences. But if the nation were writing on a blank slate, we believe it unlikely that we would create the current organization.

The President should make it clear that NSA's primary mission is the collection of foreign intelligence, including the support of our warfighters. Like other agencies, there are situations in which NSA does and should provide support to the Department of Justice, the Department of Homeland Security, and other law enforcement entities. But it should not assume the lead for programs that are primarily domestic in nature. Missions that do not involve the collection of foreign intelligence should generally be assigned elsewhere.

Recommendation 24

We recommend that the head of the military unit, US Cyber Command, and the Director of the National Security Agency should not be a single official.

As the Pentagon has recognized, it is essential for the United States military to have an effective combatant command for cyberspace activities. The importance of this command will likely grow over time, as specialized cyber capabilities become a growing part of both offense and defense. But the military organization created under Title 10 of the US Code (Defense and military organizations) should be separate from the foreign intelligence agencies created under Title 50 (Intelligence). Just as NSA has provided essential support to US Central Command in the recent wars in Iraq and Afghanistan, NSA should provide intelligence support to US Cyber Command. Nonetheless, there is a pressing need to clarify the distinction between the combat and intelligence collection missions. Standard military doctrine does not place the intelligence function in

control of actual combat. Because the two roles are complementary but distinct, the Director of NSA and the Commander of US Cyber Command in the future should not be the same person. Now that Cyber Command has grown past its initial stages, the risk increases that a single commander will not be the best way to achieve the two distinct functions.

Recommendation 25

We recommend that the Information Assurance Directorate—a large component of the National Security Agency that is not engaged in activities related to foreign intelligence—should become a separate agency within the Department of Defense, reporting to the cyber policy element within the Office of the Secretary of Defense.

In keeping with the concept that NSA should be a foreign intelligence agency, the large and important Information Assurance Directorate (IAD) of NSA should be organizationally separate and have a different reporting structure. IAD's primary mission is to ensure the security of the DOD's communications systems. Over time, the importance has grown of its other missions and activities, such as providing support for the security of other US Government networks and making contributions to the overall field of cyber security, including for the vast bulk of US systems that are outside of the government. Those are not missions of a foreign intelligence agency. The historical mission of protecting the military's communications is today a diminishing subset of overall cyber security efforts.

We are concerned that having IAD embedded in a foreign intelligence organization creates potential conflicts of interest. A chief goal

of NSA is to access and decrypt SIGINT, an offensive capability. By contrast, IAD's job is defense. When the offensive personnel find some way into a communications device, software system, or network, they may be reluctant to have a patch that blocks their own access. This conflict of interest has been a prominent feature of recent writings by technologists about surveillance issues.¹⁶¹

A related concern about keeping IAD in NSA is that there can be an asymmetry within a bureaucracy between offense and defense—a successful offensive effort provides new intelligence that is visible to senior management, while the steady day-to-day efforts on defense offer fewer opportunities for dramatic success.

Another reason to separate IAD from NSA is to foster better relations with the private sector, academic experts, and other cyber security stakeholders. Precisely because so much of cyber security exists in the private sector, including for critical infrastructure, it is vital to maintain public trust. Our discussions with a range of experts have highlighted a current lack of trust that NSA is committed to the defensive mission. Creating a new organizational structure would help rebuild that trust going forward.

There are, of course, strong technical reasons for information-sharing between the offense and defense for cyber security. Individual experts learn by having experience both in penetrating systems and in seeking to

¹⁶¹ Susan Landau, *Surveillance or Security: The Risks Posed by New Wiretapping Technologies* (MIT Press 2011); Jon M. Peha, *The Dangerous Policy of Weakening Security to Facilitate Surveillance*, Oct. 4, 2013, available at <http://ssrn.com/abstract=2350929>.

block penetration. Such collaboration could and must occur even if IAD is organizationally separate.

In an ideal world, IAD could form the core of the cyber capability of DHS. DHS has been designated as the lead cabinet department for cyber security defense. Any effort to transfer IAD out of the Defense Department budget, however, would likely meet with opposition in Congress.¹⁶² Thus, we suggest that IAD should become a Defense Agency, with status similar to that of the Defense Information Systems Agency (DISA) or the Defense Threat Reduction Agency (DTRA). Under this approach, the new and separate Defense Information Assurance Agency (DIAA) would no longer report through intelligence channels, but would be subject to oversight by the cyber security policy arm of the Office of the Secretary of Defense.

C. Reforming Organizations Dedicated to the Protection of Privacy and Civil Liberties

The Executive Branch should adopt structural reforms to protect privacy and civil liberties in connection with intelligence collection and the use of personal information. Specifically, the Executive Branch should improve its policies and procedures in the realms of policy clearance and development, compliance, oversight and investigations, and technology assessment.

A fundamental theme of this Report is that the fact that the intelligence community is able to collect personal information does not mean that it should do so. Similarly, the fact that collection is legal does

¹⁶² Although DHS was created ten years ago, Congress has yet to readjust its committees of jurisdiction.

not mean that it is good policy. The Intelligence Community's ability to collect and use information has expanded exponentially with the increased use of electronic communications technologies. The priority placed on national security after the attacks of September 11, including large budget increases, has made possible an enormous range of new collection and sharing capabilities, both within and outside the United States, on scales greater than previously imagined.

With this expansion of capabilities, there should be an accompanying set of institutions, properly funded, to ensure that the overall national interest is achieved in connection with intelligence collection and use. We recommend institutional changes within the Executive Branch designed to strengthen (1) policy clearance and development; (2) compliance; (3) oversight; and (4) technology assessment.

Recommendation 26

We recommend the creation of a privacy and civil liberties policy official located both in the National Security Staff and the Office of Management and Budget.

In some recent periods, the NSS, reporting in the White House to the President's National Security Advisor, has had a civil servant tasked with privacy issues. During that time, the Office of Management and Budget (OMB), which in its management role oversees privacy and cyber security, has similarly had a civil servant with privacy responsibilities. We recommend that the President name a policy official, who would sit within

both the NSS and the OMB, to coordinate US Government policy on privacy, including issues within the Intelligence Community.

This position would resemble in some respects the position of Chief Counselor for Privacy in OMB under President Clinton, from 1999 until early 2001. There are several reasons for creating this position: First, the OMB-run clearance process is an efficient and effective way to ensure that privacy issues are considered by policymakers. Second, a political appointee is more likely to be effective than a civil servant. Third, identifying a single, publicly named official provides a focal point for outside experts, advocacy groups, industry, foreign governments, and others to inform the policy process. Fourth, this policy development role is distinct from that of ensuring compliance by the agencies.¹⁶³

Recommendation 27

We recommend that:

- (1) The charter of the Privacy and Civil Liberties Oversight Board should be modified to create a new and strengthened agency, the Civil Liberties and Privacy Protection Board , that can oversee Intelligence Community activities for foreign intelligence purposes, rather than only for counterterrorism purposes;**
- (2) The Civil Liberties and Privacy Protection Board should be an authorized recipient for whistle-blower complaints related to**

¹⁶³ See Peter Swire, "The Administration Response to the Challenges of Protecting Privacy," Jan. 8, 2000, available at www.peterswire.net/pubs. Peter Swire is one of the five members of the Review Group; the comments in text are made here on behalf of the entire Review Group.

privacy and civil liberties concerns from employees in the Intelligence Community;

(3) An Office of Technology Assessment should be created within the Civil Liberties and Privacy Protection Board to assess Intelligence Community technology initiatives and support privacy-enhancing technologies; and

(4) Some compliance functions, similar to outside auditor functions in corporations, should be shifted from the National Security Agency and perhaps other intelligence agencies to the Civil Liberties and Privacy Protection Board.

1. *Creating the CLPP Board.* The 9/11 Commission recommended creation of what is now the PCLOB, an independent agency in the Executive Branch designed to conduct oversight of Intelligence Community activities related to terrorism and to make recommendations to Congress and the Executive Branch about how to improve privacy and civil liberty protections. The statute that authorizes the PCLOB gives it jurisdiction only over information collected and used for anti-terrorism purposes. There are major privacy and civil liberties issues raised by Intelligence Community collections for other foreign intelligence purposes, including anti-proliferation, counter-intelligence, economic policy, and other foreign affairs purposes.

To match the scope of information collection and use, we recommend the creation of a new and strengthened Board that has authority to oversee the full range of foreign intelligence issues. We have considered whether

changes should be made to the existing PCLOB, or whether instead it would be better to create an entirely new agency with augmented powers. An advantage of keeping the PCLOB as the organizational base is that a Chair and four Board members have already been confirmed by the Senate and are in place. On the other hand, the scope of responsibility that we contemplate for the agency is considerably broader than the existing PCLOB statute permits. There are also flaws with the current PCLOB statute. For those reasons, we recommend creation of a new independent agency in the Executive Branch. We refer to this new agency as the Civil Liberties and Privacy Protection Board, or CLPP Board.

Oversight should match the scope of the activity being reviewed. Having the new CLPP Board oversee “foreign intelligence” rather than “anti-terrorism” would match the scope of FISA. This broader scope would reduce any temptation Intelligence Community agencies might have to mischaracterize their activities as something other than anti-terrorism in order to avoid review by the current PCLOB.

We anticipate that this expanded scope would call for substantially increased funding and staff. With its current small staff, the PCLOB is limited in its ability to oversee intelligence agencies operating on the scale of tens of billions of dollars. This must be addressed. As with the PCLOB, the CLPP Board leadership and staff should have the clearances required to oversee this broader range of Intelligence Community activities. As under current statutes, the CLPP Board would make regular reports to Congress and the public, in a suitable mix of classified and unclassified forms.

2. *The CLPP Board and Whistle-blowers.* We recommend enactment of a statute that creates a path for whistle-blowers to report their concerns directly to the CLPP Board. Various criticisms have been published about the effectiveness of current whistle-blower provisions in the Intelligence Community. Although we have not evaluated all of these criticisms, the oversight and investigations role of the CLPP Board is well matched to examining whistle-blower allegations.

3. *A CLPP Board Office of Technology Assessment.* Public policy is shaped in part by what is technically possible, and technology experts are essential to analyzing the range of the possible. An improved technology assessment function is essential to informing policymakers about the range of options, both for collection and use of personal information, and also about the cost and effectiveness of privacy-enhancing technologies.

Prior to 1995, Congress had an Office of Technology Assessment that did significant studies on privacy and related issues. The OTA was then abolished, and no similar federal agency has existed since. Because the effectiveness of privacy and civil liberties protections depend heavily on the information technology used, a steady stream of new privacy and technology issues faces the Intelligence Community. For instance, the last few years have seen explosive growth in social networking, cloud computing, and Big Data analytics. Because the Intelligence Community pushes the state of the art to achieve military and other foreign policy objectives, assessment of the technological changes must be up-to-date.

We therefore recommend that the government should have an Office of Technology Assessment that does not report directly to the Intelligence Community but that has access to Intelligence Community activities. Congress is vital to oversight of the Intelligence Community, but it does not have an office to enable it to assess technological developments. The CLPP Board, with classified personnel and agency independence, is the logical place for this sort of independent assessment.

4. *Compliance Activities.* Although the Compliance program at NSA is independent and professional, there may be a public impression that any internal oversight function, at any agency, is vulnerable to pressure from the agency's leadership. To increase public trust and overcome even the perception of agency bias in NSA Compliance program, some of the compliance function and the relevant staff should be transferred to the CLPP Board. This structure would be analogous to the complementary roles of internal and external auditors familiar in public corporations. Under this approach, NSA would retain the internal compliance function, with the external function shifting to the CLPP Board. Consideration should also be given to transferring elements of other agencies' compliance functions to the CLPP Board.

5. *Technical Amendments to PCLOB Statute.* The current PCLOB statute has a number of limitations that reduce its ability to operate effectively. If a new CLPP Board is not created, we recommend that several changes be made to the PCLOB statute. First, the four members of the Board other than the Chair are unpaid government employees who are

permitted to work only a limited number of days per year on PCLOB matters. We recommend that these Board members should be paid for their service, and that they should not be restricted in the amount of service they provide in a year. Second, the current statute suggests that only the Chair can hire staff; any vacancy in the Chair position thus creates uncertainty about the legal basis for staff hiring. The statute should be amended to ensure smooth functioning of the Board even if the Chair position is vacant. Third, the Board should have the ability, held by other federal agencies, to subpoena records held in the private sector, without the current prior review of subpoena requests by the Attorney General. Fourth, the PCLOB needs better institutional assistance from the Intelligence Community to ensure administrative support for the Board's efforts. For instance, Board members sometimes need access to a classified facility outside of the Washington, DC headquarters, and ODNI or other support would make it easier to gain that access.

D. Reforming the FISA Court

Recommendation 28

We recommend that:

- (1) Congress should create the position of Public Interest Advocate to represent privacy and civil liberties interests before the Foreign Intelligence Surveillance Court;**
- (2) the Foreign Intelligence Surveillance Court should have greater technological expertise available to the judges;**

- (3) the transparency of the Foreign Intelligence Surveillance Court's decisions should be increased, including by instituting declassification reviews that comply with existing standards; and**
- (4) Congress should change the process by which judges are appointed to the Foreign Intelligence Surveillance Court, with the appointment power divided among the Supreme Court Justices.**

As we have seen, the FISC was established by the Foreign Intelligence Surveillance Act of 1978. The FISC, which today consists of eleven federal district court judges serving staggered seven-year terms, was created as a result of recommendations of the Church Committee to enable judicial oversight of classified foreign intelligence investigations. Most often, the judges of the FISC rule on government applications for the issuance of (a) FISA warrants authorizing electronic surveillance, (b) orders for section 215 business records, and (c) orders for section 702 interceptions targeting non-United States persons who are outside the United States.

The FISC has a staff of five full-time legal assistants with expertise in foreign intelligence issues. When preparing to rule on applications for such orders, the FISC's legal assistants often deal directly with the government's attorneys. Sometimes the judge approves the application without a hearing, and sometimes the judge concludes that a hearing with the government's attorneys is appropriate. FISA does not provide a mechanism for the FISC to invite the views of nongovernmental parties.

Rather, the FISC's proceedings are *ex parte*, as required by statute, and consistent with the procedures followed by other federal courts in ruling on applications for search warrants and wiretap orders.¹⁶⁴

Critics of the FISC have noted that the court grants more than 99 percent of all requested applications. In a recent letter to the Chairman of the Senate Judiciary Committee, FISC Presiding Judge Reggie Walton explained that this statistic is misleading, because that figure does "not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them."¹⁶⁵ Judge Walton's explanation seems quite credible. Moreover, this understanding of the FISC's approach is reinforced by the FISC's strong record in dealing with non-compliance issues when they are brought to its attention. As illustrated by the section 215 and section 702 non-compliance incidents discussed in chapters III and IV of this Report, the FISC takes seriously its responsibility to hold the government accountable for its errors.

We believe that reform of the FISC in the following areas will strengthen its ability to serve the national security interests of the United

¹⁶⁴ In one instance, the FISC heard arguments from a non-governmental party that sought to contest a directive from the government. In 2007, Yahoo declined to comply with a directive from the government. The government then filed a motion with the FISC to compel compliance. The FISC received briefings from both Yahoo and the government, and then rendered its decision in 2008 in favor of the government. Yahoo then appealed unsuccessfully to the FISA Court of Review. See *In re Directives [Redacted Version] Pursuant to Section 105b of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008). In several other instances, private parties, including the American Civil Liberties Union and the Electronic Frontier Foundation, Google, Inc., Microsoft Corporation, and the Media Freedom and Information Access Clinic, filed motions with the FISC seeking the release or disclosure of certain records. See Letter from Chief Judge Reggie Walton to Honorable Patrick Leahy (July 29, 2013); *In re Motion for Release of Court Records*, 526 F. Supp. 484 (FISA Ct. 2007).

¹⁶⁵ Letter from Chief Judge Reggie Walton to Honorable Patrick Leahy (July 29, 2013).

States while protecting privacy and civil liberties and promoting greater transparency.

(a) *Establishing a Public Interest Advocate.* Our legal tradition is committed to the adversary system. When the government initiates a proceeding against a person, that person is usually entitled to representation by an advocate who is committed to protecting her interests. If it is functioning well, the adversary system is an engine of truth. It is built on the assumption that judges are in a better position to find the right answer on questions of law and fact when they hear competing views.

When the FISC was created, it was assumed that it would resolve routine and individualized questions of fact, akin to those involved when the government seeks a search warrant. It was not anticipated that the FISC would address the kinds of questions that benefit from, or require, an adversary presentation. When the government applies for a warrant, it must establish “probable cause,” but an adversary proceeding is not involved. As both technology and the law have evolved over time, however, the FISC is sometimes presented with novel and complex issues of law. The resolution of such issues would benefit from an adversary proceeding.

A good example is the question whether section 215 authorized the bulk telephony meta-data program. That question posed serious and difficult questions of statutory and constitutional interpretation about which reasonable lawyers and judges could certainly differ. On such a question, an adversary presentation of the competing arguments is likely to

result in a better decision. Hearing only the government's side of the question leaves the judge without a researched and informed presentation of an opposing view.

We recommend that Congress should create a Public Interest Advocate, who would have the authority to intervene in matters that raise such issues. The central task of the Public Interest Advocate would be to represent the interests of those whose rights of privacy or civil liberties might be at stake. The Advocate might be invited to participate by a FISC judge. In addition, and because a judge might not always appreciate the importance of an adversary proceeding in advance, we recommend that the Advocate should receive docketing information about applications to the FISC, enabling her to intervene on her own initiative (that is, without an invitation from a FISC judge).

One difficult issue is where the Advocate should be housed. Because the number of FISA applications that raise novel or contentious issues is probably small, the Advocate might find herself with relatively little to do. It might therefore be sensible for the Advocate to have other responsibilities. One possibility would be for the Public Advocate to be on the staff of the CLPP Board, thus giving her other responsibilities and providing knowledge about the workings of the intelligence agencies. A drawback of this approach is that the Board has multiple roles, and it is possible that the presence of the Public Advocate in that setting might create conflicts of interest. Another possibility is to outsource the Public Advocate responsibility either to a law firm or a public interest group for a

sufficiently long period that its lawyers could obtain the necessary clearances and have continuity of knowledge about the intelligence agencies.¹⁶⁶ Under the former approach, the Advocate would be designated by the CLPP Board from among its employees; under the latter, the CLPP Board could oversee a procurement process to appoint the outside group of lawyers.

(b) *Bolster Technological Capacity.* The recently published opinions of the FISC make evident the technological complexity of many of the issues that now come before it. The compliance issues involving section 215 and 702 illustrate this reality and the extent to which it is important for the FISC to have the expertise available to it to oversee such issues.

Rather than relying predominantly on staff lawyers in its efforts to address these matters, the FISC should be able to call on independent technologists, with appropriate clearances, who do not report to NSA or Department of Justice. One approach would be for the FISC to use the court-appointed experts; another would be for the FISC to draw upon technologists who work with the CLPP Board.

(c) *Transparency.* The US Government should re-examine the process by which decisions issued by the FISC and its appellate body, the Foreign Intelligence Surveillance Court of Review (FISC-R) are reviewed for declassification and determine whether it ought to implement a more

¹⁶⁶ Other possible institutional homes for the Advocate appear to have serious shortcomings. Housing the Public Advocate with the FISC would run the risk of the Advocate often having little or nothing to do. Housing the Advocate within the Department of Justice would undermine the independence of the Advocate from the opposing brief writers in the case, who would also be in the same Department. Using a rotating panel of outside lawyers would risk a loss of continuity and knowledge about classified programs.

robust and regimented process of declassification of decisions to improve transparency.

The majority of the FISC's orders and filings are classified "Secret" or "Top Secret" using the standards set forth in Section 1 of Executive Order 13526 issued by President Obama on December 29, 2009. Under this Executive Order, classified national security information is subject to automatic declassification review upon passage of 25 years.

Pursuant to the Department of Justice's Automatic Classification Guide dated November 2012, "FISA Files"¹⁶⁷ are exempted from automatic declassification review at 25 years under a "File Series Exemption" granted by the Assistant to the President for National Security Affairs on October 5, 2006. These records are not subject to automatic declassification review until they reach 50 years in age from the date they were created. Consequently, the public is left uninformed as to decisions that may have far-reaching implications in terms of how the FISC interpreted the law.

The very idea of the rule of law requires a high degree of transparency. Transparency promotes accountability. As Justice Louis Brandeis once observed, sunlight can be "the best of disinfectants."¹⁶⁸ A lack of transparency can also breed confusion, suspicion, and distrust. In our system, judicial proceedings are generally open to the public, and

¹⁶⁷ "FISA Files" are files relating to the Foreign Intelligence Surveillance Act (FISA). These "FISA Files" may include the following: a request to initiate collection activity; an application; court order or authorization by the Attorney General; draft documents; related memoranda; motions, affidavits, filings, correspondence, and electronic communications; and other related documents or records. See p. 8 of United States Department of Justice "Automatic Declassification Guide – FOR USE AND REVIEW AND DECLASSIFICATION OF RECORDS UNDER EXECUTIVE ORDER 13526, "CLASSIFIED NATIONAL SECURITY INFORMATION."

¹⁶⁸ Louis Brandeis, *Other People's Money – And How Bankers Use It*, Chapter 5 (1914).

judicial opinions are made available for public scrutiny and inspection. Indeed, the ODNI has declassified a considerable number of FISC opinions in 2013, making the determination that the gains from transparency outweighed the risk to national security.

There can, of course, be a genuine need for confidentiality, especially when classified material is involved. When the FISC is dealing with such material, there are legitimate limits on disclosure. But in order to further the rule of law, FISC opinions or, when appropriate, redacted versions of FISC opinions, should be made public in a timely manner, unless secrecy of the opinion is essential to the effectiveness of a properly classified program.

(d) *Selection and Composition of the FISC.* Under FISA, the judges on the FISC are selected by the Chief Justice of the United States. In theory, this method of selection has significant advantages. Concentration of the power of appointment in one person can make the process more orderly and organized. But that approach has drawn two legitimate criticisms.

The first involves the potential risks associated with giving a single person, even the Chief Justice, the authority to select *all* of the members of an important court. The second involves the fact that ten of the eleven current FISC judges, all of whom were appointed by the current Chief Justice, were appointed to the federal bench by Republican presidents. Although the role of a judge is to follow the law and not to make political judgments, Republican-appointed and Democratic-appointed judges sometimes have divergent views, including on issues involving privacy,

civil liberties, and claims of national security. There is therefore a legitimate reason for concern if, as is now the case, the judges on the FISC turn out to come disproportionately from either Republican or Democratic appointees.

There are several ways to respond to this concern. We recommend allocating the appointment authority to the Circuit Justices. Under this approach, each member of the Supreme Court would have the authority to select one or two members of the FISC from within the Circuit(s) over which she or he has jurisdiction. This approach would have the advantage of dividing appointment authority among the Court's nine members and reducing the risks associated with concentrating the appointment power in a single person.

Chapter VII

Global Communications Technology: Promoting Prosperity, Security, and Openness in a Networked World

A. Introduction

An important goal of US policy is to promote prosperity, security, and openness in the predominant method of modern communication, the Internet. This chapter examines how to achieve that goal, consistent with other goals of US policy.

In 2011, the Obama Administration released a major report: “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.” In the letter introducing the report, President Obama wrote: “This strategy outlines not only a vision for the future of cyberspace, but an agenda for realizing it. It provides the context for our partners at home and abroad to understand our priorities, and how we can come together to preserve the character of cyberspace and reduce the threats we face.” The Strategy defined the overall goal: “The United States will work internationally to promote an **open, interoperable, secure, and reliable** information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation” (emphasis added).

We believe that this is an exceedingly important goal, and that it bears directly on efforts to engage in sensible risk management. In this chapter, we offer a series of recommendations designed to promote that

goal, and in the process to protect the central values associated with a free Internet.

B. Background: Trade, Internet Freedom, and Other Goals

The United States has a strong interest in promoting an open, interoperable, secure, and reliable information and communication structure. We focus our discussion on international trade, economic growth, and Internet freedom.

Throughout this report, we have stressed the need for a risk-management approach, balancing the imperatives for intelligence collection with the potential downsides. In the areas discussed in this chapter, prominent US policy goals run the risk of being undermined by the reports about US surveillance. We consider what measures will best achieve those goals for our global communications structure.

1. International Trade and Economic Growth

The US is committed to international economic competitiveness, to improvements in the international trade system, and to achievement of economic growth. The rules for international trade are crucial for the pervasively international conduct of commerce on the Internet, as well as for other sectors involved in international trade. Free trade agreements can contribute to economic growth. Unfortunately, foreign concerns about US surveillance threaten achievement of these various goals.

For example, the Transatlantic Trade and Investment Partnership (T-TIP) is a large and visible trade negotiation potentially affected by the

recent surveillance leaks. The T-TIP talks were launched in 2013 as “an ambitious, comprehensive, and high-standard trade and investment agreement” designed to eliminate all tariffs on trade, improve market access on trade in services, and address a wide range of other impediments to trade.¹⁶⁹ But strong concerns have been expressed about surveillance by European officials, as reflected in this statement by the EU Parliament Committee on Foreign Affairs: “With the damage to trust in the transatlantic relationship caused by NSA massive surveillance and lack of data privacy remedies for Europeans, the transatlantic economic relationship is at risk.”¹⁷⁰

European officials have similarly expressed doubt about whether to continue the existing Safe Harbor agreement for transfer of personal information to the US, under which companies are able to comply with the stricter EU privacy laws.¹⁷¹ Although the precise impact on such future negotiations is unclear, such statements show the linkage between intelligence collection decisions and international trade negotiations.

The effects of concern with US surveillance on US trade in cloud computing and other online activities have drawn particular attention. The public cloud computing market for enterprises is growing rapidly. By 2016, it is estimated to reach \$207 billion annually, more than double the

¹⁶⁹ White House Fact Sheet: *Transatlantic Trade and Investment Partnership (T-TIP)*, June, 2013, available at <http://www.ustr.gov/about-us/press-office/fact-sheets/2013/june/wh-ttip>.

¹⁷⁰ “Draft Working Document on Foreign Policy Aspect of the Inquiry on Electronic Mass Surveillance of EU Citizens,” European Parliament Committee on Foreign Affairs, Nov. 4, 2013, available at <http://www.statewatch.org/news/2013/nov/ep-nsa-surv-inq-working-document-fa-committee.pdf>.

¹⁷¹ “Bhatt Jaheen, “In Wake of PRISM, German DPAs Threaten to Halt Data Transfers to Non-EU Countries,” Bloomberg BNA, July 29, 2013, available at <http://www.bna.com/wake-prism-germann1717987502>.

2012 level.¹⁷² As a result, cloud computing vendors not only have to retain existing customers but also must recruit new customers to maintain market share. In the wake of press reports on US surveillance, two studies estimated large losses in sales for US cloud computing providers, due to concerns overseas about the security of US providers and possible legal measures to limit use of US-based cloud providers by other countries.¹⁷³ US-based information technology companies and trade associations have expressed strong concerns, fearing that Chinese, European, and other competitors will use the disclosures to promote their products over American exports.

Negative effects stemming from concern with US surveillance on trade and economic competitiveness may, in turn, have adverse effects on overall US economic growth. In recent years, the information technology sector has been a major source of innovation and growth. Foreign concerns about US surveillance can directly reduce the market share of US-based technology companies, and can in addition have an indirect effect of justifying protectionist measures. Addressing concerns about US Government surveillance would increase confidence in the US information technology sector, thus contributing to US economic growth.

¹⁷² "Garner Predict Cloud Computing Spending to Increase by 100% in 2016, says AppsCare," PRWEb.com, 2012, available at <http://prweb.com/releases/2012/7/prweb9711167.htm>.

¹⁷³ Daniel Castro, "How Much Will PRISM Cost the US Cloud Computing Industry," August, 2013 (estimating monetary impact on US cloud providers of \$21.5 billion by 2016, based on 10% loss in foreign market share), available at www2.itif.org/2013-cloud-computing-costs.pdf; Cloud Security Alliance, "CSA Survey Results: Government Access to Information", July 2013, available at https://downloads.cloudsecurityalliance.org/initiatives/surveys/nsa_prism/CSA-govt-access-survey-July-2013.pdf (losses up to \$180 billion by 2016).

2. Internet Freedom

US Internet freedom policy seeks to preserve and expand the Internet as an open, global space for free expression, for organizing and interaction, and for commerce. In recent years, the United States has highlighted Internet freedom as an important goal of US policy, including by pushing successfully in 2012 for the first United Nations resolution that confirms that human rights in the Internet realm must be protected with the same commitment as in the real world. The US has worked with the Dutch Foreign Ministry to establish the Freedom Online Coalition, currently a group of 21 governments from five regions committed to coordinating diplomatic efforts to advance Internet freedom. This Coalition has sought to broaden support for an approach based on universal human rights and the inclusive, multi-stakeholder model of Internet governance.

A central theme of US Internet freedom policy has been protection against intrusive surveillance and repression. The US Government has consistently spoken out against the arrest and persecution of bloggers and online activists in countries such as Azerbaijan, China, Cuba, Egypt, Ethiopia, Iran, Russia, Saudi Arabia, Thailand, Venezuela, and Vietnam. President Obama and Secretaries of State have publicly criticized restrictive Internet legislation designed to force companies to collaborate in censorship and pervasive surveillance of their users in order to chill expression and facilitate persecution. Since 2008, the Department of State and the United States Agency for International Development have invested over \$100 million in programs to enable human rights activists and

bloggers to exercise their human rights freely and safely online, including by distribution of strong encryption and other anti-censorship tools.

Revelations about US surveillance have threatened to undermine the US Internet freedom agenda. Countries that were previously criticized by the United States for excessive surveillance have accused the US of hypocrisy. In our view, these allegations lack force. US surveillance is subject to oversight by the multiple authorities shown in Appendix C, and the First Amendment protections under the US Constitution are an effective bulwark against censorship and political repression. Nonetheless, the reports about US surveillance have clearly made it more difficult to explain the key differences in international fora. As we have emphasized at several points in this Report, public trust is exceedingly important.

3. Internet Governance and Localization Requirements

The United States has strongly supported an inclusive multi-stakeholder model of Internet governance in order to maintain and expand a globally interoperable, open, and secure Internet architecture to which all people have access. This multi-stakeholder approach incorporates input from industry, governments, civil society, academic institutions, technical experts, and others. This approach has emphasized the primacy of interoperable and secure technical standards, selected with the help of technical experts.

A competing model, favored by Russia and a number of other countries, would place Internet governance under the auspices of the United Nations and the International Telecommunications Union (ITU).

This model would enhance the influence of governments at the expense of other stakeholders in Internet governance decisions, and it could legitimize greater state control over Internet content and communications. In particular, this model could support greater use of “localization” requirements, such as national laws requiring servers to be physically located within a country or limits on transferring data across borders.

The press revelations about US surveillance have emboldened supporters of localization requirements for Internet communications. Brazil, Indonesia, and Vietnam have proposed requiring e-mails and other Internet communications to be stored locally, in the particular country. Although generally favoring the multi-stakeholder approach to many Internet governance issues, the EU has also shifted in the direction of localization requirements. In the second half of 2013, the EU Parliament voted in favor of a proposal to limit international data flows; this provision would prohibit responding to lawful government requests, including from the US courts and government, until release of such records were approved by a European data protection authority.

Public debate has suggested a possible mix of motives supporting such localization requirements, including (1) concern about how records about their citizens will be treated in the US; (2) support for local cloud providers and other information technology companies with the effect of reducing the market share of US providers; and (3) use of the localization proposals as a way to highlight concerns about US intelligence practices and create leverage for possible changes in US policy. Whatever the mix of

motives, press reports about US surveillance have posed new challenges for the longstanding US policy favoring the multi-stakeholder approach to Internet governance as well as US opposition to localization requirements.

C. Technical Measures to Increase Security and User Confidence

Recommendation 29

We recommend that, regarding encryption, the US Government should:

- (1) fully support and not undermine efforts to create encryption standards;**
- (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and**
- (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage.**

Encryption is an essential basis for trust on the Internet; without such trust, valuable communications would not be possible. For the entire system to work, encryption software itself must be trustworthy. Users of encryption must be confident, and justifiably confident, that only those people they designate can decrypt their data.

The use of reliable encryption software to safeguard data is critical to many sectors and organizations, including financial services, medicine and health care, research and development, and other critical infrastructures in the United States and around the world. Encryption allows users of

information technology systems to trust that their data, including their financial transactions, will not be altered or stolen. Encryption-related software, including pervasive examples such as Secure Sockets Layer (SSL) and Public Key Infrastructure (PKI), is essential to online commerce and user authentication. It is part of the underpinning of current communications networks. Indeed, in light of the massive increase in cyber-crime and intellectual property theft on-line, the use of encryption should be greatly expanded to protect not only data in transit, but also data at rest on networks, in storage, and in the cloud.

We are aware of recent allegations that the United States Government has intentionally introduced “backdoors” into commercially available software, enabling decryption of apparently secure software. We are also aware that some people have expressed concern that such “backdoors” could be discovered and used by criminal cartels and other governments, and hence that some commercially available software is not trustworthy today.

Upon review, however, we are unaware of any vulnerability created by the US Government in generally available commercial software that puts users at risk of criminal hackers or foreign governments decrypting their data. Moreover, it appears that in the vast majority of generally used, commercially available encryption software, there is no vulnerability, or “backdoor,” that makes it possible for the US Government or anyone else to achieve unauthorized access.¹⁷⁴

¹⁷⁴ Any cryptographic algorithm can become exploitable if implemented incorrectly or used improperly.

Nonetheless, it is important to take strong steps to enhance trust in this basic underpinning of information technology. Recommendation 32 is designed to describe those steps. The central point is that trust in encryption standards, and in the resulting software, must be maintained. Although NSA has made clear that it has not and is not now doing the activities listed below, the US Government should make it clear that:

- NSA will not engineer vulnerabilities into the encryption algorithms that guard global commerce;
- The United States will not provide competitive advantage to US firms by the provision to those corporations of industrial espionage;
- NSA will not demand changes in any product by any vendor for the purpose of undermining the security or integrity of the product, or to ease NSA's clandestine collection of information by users of the product; and
- NSA will not hold encrypted communication as a way to avoid retention limits.

Although NSA is authorized to retain encrypted data indefinitely for cryptanalysis purposes, such as for encryption systems of nation-states or terrorist groups, NSA should not store generic commercial encrypted data, such as Virtual Private Network (VPN) or SSL data. If NSA is able to decrypt data years after it is collected, that data, once decrypted, should be sent to an analytic storage facility, where standard retention, minimization, and reporting rules would apply. Those rules should include minimization

of US person data and a prohibition on using data that is beyond authorized retention limits.

Recommendation 30

We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are often called "Zero Day" attacks because developers have had zero days to address and patch the vulnerability. US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.

NSA and other US Government agencies, such as DHS, have important missions to assist US corporations in the protection of privately owned and operated critical infrastructure information networks. To do so, NSA, DHS, and other agencies should identify vulnerabilities in software widely employed in critical infrastructure and then work to eliminate those vulnerabilities as quickly as possible. That duty to defend, however, may sometimes come into conflict with the intelligence collection mission, particularly when it comes to what are known as "Zero Days."

A Zero Day or "0 Day" exploit is a previously unknown vulnerability in software in a computer application or system – the developers or system

owners have had zero days to address or patch the vulnerability. Because the software attack technique has not been used or seen before, it enables a cyber attacker to penetrate a system or to achieve other malicious goals. In almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities—“patching” them—strengthens the security of US Government, critical infrastructure, and other computer systems.

We recommend that, when an urgent and significant national security priority can be addressed by the use of a Zero Day, an agency of the US Government may be authorized to use temporarily a Zero Day instead of immediately fixing the underlying vulnerability. Before approving use of the Zero Day rather than patching a vulnerability, there should be a senior-level, interagency approval process that employs a risk management approach. The NSS should chair the process, with regular reviews. All offices and departments with relevant concerns, generally including the National Economic Council, State, Commerce, Energy, and Homeland Security, should be involved in that process.

D. Institutional Measures for Cyberspace

Recommendation 31

We recommend that the United States should support international norms or international agreements for specific measures that will increase confidence in the security of online communications. Among those measures to be considered are:

- (1) Governments should not use surveillance to steal industry secrets to advantage their domestic industry;**
- (2) Governments should not use their offensive cyber capabilities to change the amounts held in financial accounts or otherwise manipulate the financial systems;**
- (3) Governments should promote transparency about the number and type of law enforcement and other requests made to communications providers;**
- (4) Absent a specific and compelling reason, governments should avoid localization requirements that (a) mandate location of servers and other information technology facilities or (b) prevent trans-border data flows.**

The US Government should encourage other countries to take specific measures to limit the possible negative consequences of their own intelligence activities, and increase public trust and user confidence in the security of online communications. Norms or agreements might be valuable for that purpose.

We suggest consideration of a series of specific steps. First, governments should not use their surveillance capabilities to steal industry secrets to advantage their domestic industries. Surveillance may take place against both foreign and domestic companies for a variety of reasons, such as to promote compliance with anti-money laundering, anti-corruption, and other laws, as well as international agreements such as economic sanctions against certain countries. The purpose of such surveillance,

however, should not be to enable a government to favor its domestic industry. Bolstering an international norm against this sort of economic espionage and competition would support economic growth, protect investment and innovation in intellectual property, and reduce costs to those innovators of protecting against nation-state cyber attacks.

Second, governments should abstain from penetrating the systems of financial institutions and changing the amounts held in accounts there. The policy of avoiding tampering with account balances in financial institutions is part of a broader US policy of abstaining from manipulation of the financial system. These policies support economic growth by allowing all actors to rely on the accuracy of financial statements without the need for costly re-verification of account balances. This sort of attack could cause damaging uncertainty in financial markets, as well as create a risk of escalating counter-attacks against a nation that began such an effort. The US Government should affirm this policy as an international norm, and incorporate the policy into free trade or other international agreements.

Third, governments should increase transparency about requests in other countries from communications providers. Elsewhere in this Report, we discuss the importance of such transparency, and recommend increasing reporting by both providers and the US Government. Transparency about the number and nature of such requests serves as a check against abuse of the lawful access process. Greater transparency can also encourage increased trust in the security of Internet communications

and reduce the risk that governments are obtaining widespread access to private communication records without the knowledge of users. Putting this sort of provision into free trade agreements or other international instruments can broaden the positive effects of greater transparency within the US.

Fourth, we support international efforts to limit localization requirements except where there is a specific and compelling reason for such actions. Global inter-operability has been a fundamental technical feature of the Internet; bits flow from one user to the next based on technical considerations rather than national boundaries. National efforts to tamper with this architecture would require pervasive technical changes and be costly in economic terms. A balkanized Internet, sometimes referred to as a “splinternet,” would greatly reduce the economic, political, cultural, and other benefits of modern communications technologies. The US Government should work with allies to reduce harmful efforts to impose localization rules onto the Internet.

Recommendation 32

We recommend that there be an Assistant Secretary of State to lead diplomacy of international information technology issues.

In the wake of recent disclosures, distortions, and controversies involving US Government intelligence collection, there is an increased need for vigorous, coordinated, senior-level US diplomacy across a broad range of inter-related information technology issues. We believe that the US should take the lead in proposing an agreement among multiple nations to

some set of Internet Norms for Cyberspace, such as a prohibition on industrial espionage, a protection of financial services and markets data standard, and others. To this end, we recommend a US diplomatic agenda to promote confidence-building measures for international cyber security, building on the Budapest Convention on Cyber Crime. The promotion of the Internet Freedom Agenda, the protection of intellectual property rights in cyber space, changes in Internet governance and the implementation of the President's International Cyber Strategy—all will necessitate agile diplomatic activity by the United States.

Currently, there is no single, senior US diplomat and no single Department of State Bureau, with lead responsibility across this broad set of issues. Just as other international, non-regional functional issues have in the past benefited from the creation of an Assistant Secretary of State position and of a State Department bureau (International Narcotics, Environmental Affairs, Counterterrorism, Human Rights), the interests of the United States would be served by the creation of a Department of State Bureau of Internet and Cyberspace Affairs, led by an experienced senior diplomat confirmed by the Senate as an Assistant Secretary of State. The Assistant Secretary would coordinate activity of the regional and functional bureaus on these issues and should, with NSS support, coordinate interagency activities with other governments.

Recommendation 33

We recommend that as part of its diplomatic agenda on international information technology issues, the United States should advocate for, and explain its rationale for, a model of Internet governance that is inclusive of all appropriate stakeholders, not just governments.

The United States Government should continue and strengthen its international advocacy for an Internet governance model that is inclusive of all appropriate stakeholders, not just governments. This recommendation builds on the administration's 2011 International Strategy for Cyberspace, which outlines multiple US Government goals with respect to global communications technologies. It articulates the need to protect national security, while also highlighting the importance of economic growth, openness, privacy protection, and a secure communications infrastructure. Other administration initiatives similarly emphasize the importance of multiple policy goals for online communications, such as the efforts led by the Department of State on the Internet Freedom agenda and the efforts led by the Department of Commerce on the Consumer Privacy Bill of Rights.

As part of the overall discussion of US policy concerning communications technology, we believe that the US Government should reaffirm that Internet governance must not be limited to governments, but should include all appropriate stakeholders. Inclusion of such stakeholders—including civil society, industry, and technical experts—is

important to ensure that the process benefits from a wide range of information and to reduce the risk of bias or partiality.

We are aware that some changes in governance approaches may well be desirable to reflect changing communications practices. For instance, the time may well be approaching for a hard look at the unique US relationship to the organization that governs the domain name system, the Internet Corporation for Assigned Names and Numbers (ICANN). The current US role is an artifact of the early history of the Internet, and may not be well suited to the broader set of stakeholders engaged in Internet governance today. The US Government and its allies, however, should continue to oppose shifting governance of the Internet to a forum, such as the International Telecommunications Union, where nation-states dominate the process, often to the exclusion of others. We believe that such a governance shift would threaten the prosperity, security, and openness of online communications.

Recommendation 34

We recommend that the US Government should streamline the process for lawful international requests to obtain electronic communications through the Mutual Legal Assistance Treaty process.

US efforts to obtain improved international cooperation on information technology issues of importance to us are undermined by the inability of the Department of Justice to provide adequate support to other nations when they request our assistance in dealing with cyber crime originating in the United States. The Justice Department has severely

under-resourced the so-called Mutual Legal Assistance Treaty (MLAT) support process.

The MLAT process essentially permits one country to seek electronic communication and other records held in other countries. For instance, non-US countries may seek e-mails held in the United States by web e-mail providers. Under the Electronic Communications Privacy Act, providers in the US can turn over the content of e-mails only through the required legal process, typically requiring probable cause that a crime has been committed.

The MLAT process creates a legal mechanism for non-US countries to obtain e-mail records, but the process today is too slow and cumbersome. Requests appear to average approximately 10 months to fulfill, with some requests taking considerably longer. Non-US governments seeking such records can face a frustrating delay in conducting legitimate investigations. These delays provide a rationale for new laws that require e-mail and other records to be held in the other country, thus contributing to the harmful trend of localization laws discussed above.

We believe that the MLAT process in the US should be streamlined, both in order to respond more promptly to legitimate foreign requests and to demonstrate the US commitment to a well-functioning Internet that meets the goals of the international community. Promising reform measures could include:

1. Increase resources to the office in the Department of Justice that handles MLAT requests. The Office of International Affairs (OIA) in the

Department of Justice has had flat or reduced funding over time, despite the large increase in the international electronic communications that are the subject of most MLAT requests.

2. Create an online submission form for MLATs. Today, there is no online form for foreign governments that seek to use the MLAT process. An online submission process, accompanied by clear information to foreign governments about the MLAT requirements, would make it easier for distant and diverse foreign governments to understand what is required under the US probable cause standard or other laws.

3. Streamline the number of steps in the process. Under the current system, the OIA first examines a request, and then forwards it to the US Attorney in the district where the records are held. That US Attorney's office then reviews the application a second time, and handles the request subject to the other priorities of that office. The Department of Justice should explore whether a single point of contact would be able to expedite the MLAT request.

4. Streamline provision of the records back to the foreign country. Under the current system, the provider sends the records to the Department of Justice, which then forwards the records to the requesting country. It may be possible to streamline this process by permitting the provider to send the records directly to the requesting country, with notice to the Justice Department of what has been sent.

5. Promote the use of MLATs globally and demonstrate the US Government's commitment to an effective process. Changing technology

has sharply increased the importance for non-US governments of gaining lawful access to records held in the United States. Web e-mail providers are largely headquartered in the United States, and today's use of secure encryption for e-mail means that other governments frequently cannot intercept and read the e-mail between the user and the server. It is in the interest of the United States to support the continued use of efficient and innovative technologies on the Internet, including through leading web e-mail providers. The US Government can promote this interest by publicizing and supporting the existence of a well-functioning MLAT process, thereby reducing the likelihood of harmful localization measures.

E. Addressing Future Technological Challenges

This chapter has thus far addressed issues that are currently known to implicate US intelligence and communications technology policy. Communications technology will continue to change rapidly, however, so institutional mechanisms should be in place to address such changes.

Recommendation 35

We recommend that for big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are statistically reliable, cost-effective, and protective of privacy and civil liberties.

We believe that the Intelligence Community should develop Privacy and Civil Liberties Impact Assessments for new programs or substantial modifications of existing programs that contain substantial amounts of

personally identifiable information. Under the E-Government Act of 2002, federal agencies are required to prepare Privacy Impact Assessments (PIAs) in connection with the procurement of new, or substantially modified, information technology systems. These PIAs are designed to encourage building privacy considerations early into the procurement cycle for such systems.

Our focus here is on the broader programs that may constitute multiple systems. The goal in the program assessment should be broader and more policy-based than has usually been the case for PIAs. For instance, policy officials should explicitly consider the costs and benefits of a program if it unexpectedly becomes public. In some cases, that consideration may result in modifications of the program, or perhaps even in a decision not to go forward with a program.¹⁷⁵

¹⁷⁵ We should emphasize here that data-mining and big data have been the subject of previous federally-funded reports, notably including "Safeguarding Privacy in the Fight Against Terrorism," from the Technology and Privacy Advisory Committee of the Department of Defense (2004), and "Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment," by the National Research Council (2008). These studies, have examined issues of data-mining in considerable detail, and we have found them useful and illuminating. Related academic work includes Fred H. Cate, "Government Data Mining: the Need for a Legal Framework," *Harvard Civil Rights-Civil Liberties Law Review* 43, 2008; Peter Swire, "Privacy and Information Sharing in the War Against Terrorism," 51 *Villanova Law Review* 260, 2006. We encourage agencies to study this literature, and adopt risk management approaches where feasible.

Recommendation 36

We recommend that for future developments in communications technology, the US should create program-by-program reviews informed by expert technologists, to assess and respond to emerging privacy and civil liberties issues, through the Civil Liberties and Privacy Protection Board or other agencies.

Technical collection and communications technologies continue to evolve rapidly. The US Government should adopt mechanisms that can assess and respond to emerging issues. To do this effectively, expert technologists, with clearances as needed, must be deeply involved in the process.¹⁷⁶

We recommended in Chapter VI that the CLPP Board should have an Office of Technology Assessment, capable of assessing the privacy and civil liberties implications of Intelligence Community programs. Sufficient funding for this office should be part of the generally enhanced budget for policy and oversight concerning the expensive and technically sophisticated programs of the Intelligence Community.¹⁷⁷

¹⁷⁶ The Federal Trade Commission (FTC) often plays this role for evolving privacy-related issues, such as through its recent workshops on the Internet of Things or Big Data. The FTC's jurisdiction, however, is limited to the commercial sector. It has no jurisdiction over technology issues facing government agencies, including the Intelligence Community.

¹⁷⁷ If an OTA is not created within the PCLOB or a new CLPP Board, then the intelligence community should find other mechanisms to institutionalize the effects of new programs on privacy, civil liberties, and the other important values implicated by cutting-edge intelligence technologies. These new mechanisms must include effective participation by expert technologists beyond those involved in development of the program.

This page has been intentionally left blank.

Chapter VIII

Protecting What We Do Collect

What intelligence and sensitive information the United States does choose to collect or store should be carefully protected from both the Insider Threat and the External Hack. Such protection requires new risk-management approaches to personnel vetting, a change in philosophy about classified networks, and adoption of best commercial practices for highly secure private sector networks.

Our comments in this chapter deal with personnel with security clearances and classified networks throughout the US Government and not just those in the Intelligence Community. We believe that this broad scope is necessary, and we note that previous reviews have been limited to the Intelligence Community. In general, we believe that the same standards applied to government employees with security clearances and IT networks with classified information should apply to private sector contractor personnel and networks dealing with Secret and Top Secret data.

A. Personnel Vetting and Security Clearances

Recommendation 37

We recommend that the US Government should move toward a system in which background investigations relating to the vetting of personnel for security clearance are performed solely by US Government employees or by a non-profit, private sector corporation.

Recommendation 38

We recommend that the vetting of personnel for access to classified information should be ongoing, rather than periodic. A standard of Personnel Continuous Monitoring should be adopted, incorporating data from Insider Threat programs and from commercially available sources, to note such things as changes in credit ratings or any arrests or court proceedings.

Recommendation 39

We recommend that security clearances should be more highly differentiated, including the creation of "administrative access" clearances that allow for support and information technology personnel to have the access they need without granting them unnecessary access to substantive policy or intelligence material.

Recommendation 40

We recommend that the US Government should institute a demonstration project in which personnel with security clearances would be given an Access Score, based upon the sensitivity of the information to which they have access and the number and sensitivity of Special Access Programs and Compartmented Material clearances they have. Such an Access Score should be periodically updated.

In the government as in other enterprises, vast stores of information are growing in data bases. Even one unreliable individual with access to parts of a data base may be capable of causing incalculable damage by compromising sensitive information. Unfortunately, almost every agency

with sensitive information has experienced a major incident in which a disloyal employee caused significant damage by revealing sensitive data directly or indirectly to another government or to others who would do us harm. All of the individuals involved in these cases have committed criminal acts after having been vetted by the current security clearance process and, in several well-known cases, after having been polygraphed. Although parts of the Intelligence Community have improved their personnel vetting systems and they may perform well, the general picture throughout the US Government is of an inadequate personnel vetting system.

We believe that the current security clearance personnel vetting practices of most federal departments and agencies are expensive and time-consuming, and that they may not reliably detect the potential for abuse in a timely manner.

The security clearance system should be designed to have an extremely low false-positive rate (granting or continuing a clearance when one should have been denied). Access to sensitive information should be recorded in more detail (e.g. who has access to what and when). The nature and degree of vetting procedures should be adjusted periodically and more closely tied to the sensitivity of the information to which access is granted.

1. How the System Works Now

There are essentially three levels of security clearance (Secret, Top Secret, and Top Secret/SCI). For those obtaining any level of security clearance, the fundamentals of the personnel vetting system are similar.

The applicant is asked to provide the names of a score or more of contacts. An investigator attempts to meet with those people whose names have been provided by the applicant. In many agencies, the investigator is often an employee of a private sector company that is paid by the number of investigations it completes.

If the investigators are unable to meet with the contacts in person, they may in some cases accept a telephone interview. In many agencies, the investigator begins the discussion with all contacts by informing them that anything they say about the applicant can be seen by the applicant because of the requirements of privacy laws. Not surprisingly, very few contacts suggested by the applicant provide derogatory information, especially because they know that their remarks may be disclosed to their friend or acquaintance.

Investigators are required to develop interviewees in addition to those suggested by the applicant. Often the investigator will attempt to inquire of neighbors, those living in the next apartment or house. Increasingly, however, neighbors may not know each other well. Online "friends" sometimes have a better idea about someone than the people living in physical proximity.

As part of an initial security review, investigators may also access some publicly available and commercially available data bases. Such data base reviews are used largely to corroborate information supplied by the applicant on a lengthy questionnaire. Agencies may require a financial disclosure form to be completed, revealing the financial health and

holdings of an applicant (although often those declarations are not verified). Some agencies require a polygraph for Top Secret/SCI clearances. Once a clearance has been granted, SECRET- level clearances are often updated only once a decade. Top Secret/SCI clearances may be updated every five years. Random testing for drug use and random polygraphing may occur in between clearance updates.

In many agencies, the current personnel vetting system does not do well in detecting changes in a vetted individual's status after a security clearance has been granted. In most agencies, the security clearance program office might not know if an employee between vettings had just become involved in a bankruptcy, a Driving Under the Influence arrest, a trip to a potentially hostile country, or a conversion to a radical cause such as al-Qa'ida.

Once granted a certain level of clearance because of a need to do part of their jobs, employees are often in a position to read other material at that classification, regardless of its relevance to their job. However, some sensitive projects or sensitive intelligence collection programs ("compartments") have dissemination controls ("bigot lists"). Sometimes access to these programs may be granted based solely on job-related needs and may not trigger an updated or closer review of personnel background material.

As the system works today, the use of special compartmented access programs, limiting access to data, is occasioned often by the means that were employed to collect the information, not by the content of the

information, or the target of the collection, or the damage that could be done by unauthorized disclosure of content or target.

2. How the System Might Be Improved

A series of broad changes could improve the efficacy of the personnel vetting system.

First, and consistent with practical constraints, agencies and department should move in the direction of reducing or terminating the use of “for-profit” corporations to conduct personnel investigations. When a company is paid upon completion of a case, there is a perverse incentive to complete investigations quickly. For those agencies that cannot do vetting with their own government employee staff, consideration should be given to the creation of a not-for-profit entity modeled on the Federally Funded Research and Development Centers (FFRDC), such as RAND and MITRE, to conduct background investigations and to improve the methodology for doing so. We recommend that a feasibility study be launched in the very near future.

Second, security clearance levels should be further differentiated so that administrative and technical staff who do not require access to the substance of data on a network are given a restricted level of access and security clearance that allows them to do their job, but that does not expose them to sensitive material.

Third, information should be given more restricted handling based not only on how it is collected, but also on the damage that could be created by its compromise.

Fourth, departments and agencies should institute a Work-Related Access approach to the dissemination of sensitive, classified information. While not diminishing the sharing of information between and among agencies, the government should seek to restrict distribution of data to personnel whose jobs actually require access to the information. Typically, analysts working on Africa do not need to read sensitive information about Latin America. Yet in today's system of information-sharing, such "interesting but not essential" data is widely distributed to people who do not really need it.

Implementing this sort of Work-Related Access will necessitate a greater use of Information Rights Management (IRM) software. Greater use of the software means actually widely employing it, not just procuring it. It may also require a significant improvement on the state of the art of such software, as discussed later in this chapter.

Fifth, we believe that after being granted their initial clearances, all personnel with access to classified information should be included in a Personnel Continuous Monitoring Program (PCMP). The PCMP would access both internally available and commercially available information, such as credit scores, court judgments, traffic violations, and other arrests. The PCMP would include the use of anomaly information from Insider Threat software. When any of these sources of information raised a level of concern, the individual involved would be re-interviewed or subject to further review, within existing employee rights and guidelines.

Sixth, ongoing security clearance vetting of individuals should use a risk-management approach and depend upon the sensitivity and quantity of the programs and information to which they are given access.

We recommend a pilot program of Access Scoring and additional screening for individuals with high scores. Everyone with a security clearance might, for example, be given a regularly updated Access Score, which would vary depending upon the number of special access programs or compartments they are cleared to be in, the sensitivity of the content of those compartments, and the damage that would be done by the compromise of that information.

It would be important that the Access Score be derived not only from the accesses granted by the individual's parent agency, and not only from the list of intelligence programs for which the individual was accredited, but also from all of the restricted programs to which that individual has access from any department, including the Departments of Defense, Energy, Homeland Security, and others.

The greater an individual's Access Score, the more background vetting he or she would be given. Higher scores should require vetting more frequent than the standard interval of five (Top Secret) or 10 (Secret) years. At a certain Access Score level, personnel should be entered into an Additional Monitoring Program. We recognize that such a program could be seen by some as an infringement on the privacy of federal employees and contractors who choose on a voluntary basis to work with highly sensitive information in order to defend our nation. But, employment in

government jobs with access to special intelligence or special classified programs is not a right. Permission to occupy positions of great trust and responsibility is already granted with conditions, including degrees of loss of privacy. In our view, there should be a sliding scale of such conditions depending on the number and sensitivity of the security accesses provided.

We believe that those with the greatest amount of access to sensitive programs and information should be subject to Additional Monitoring, in addition to the PCMP discussed earlier. The routine PCMP review would draw in data on an ongoing basis from commercially available data sources, such as on finances, court proceedings, and driving activity of the sort that is now available to credit scoring and auto insurance companies. Government-provided information might also be added to the data base, such as publicly available information about arrests and data about foreign travel now collected by Customs and Border Patrol.

Those with extremely high Access Scores might be asked to grant permission to the government for their review by a more intrusive Additional Monitoring Program, including random observation of the meta-data related to their personal, home telephone calls, e-mails, use of online social media, and web surfing. Auditing and verification of their Financial Disclosure Forms might also occur.

A data analytics program would be used to sift through the information provided by the Additional Monitoring Program on an ongoing basis to determine if there are correlations that indicate the advisability of some additional review. Usually, any one piece of

information obtained by an Additional Monitoring Program would not be determinative of an individual's suitability for special access. Such a review could involve interviewing the individual involved to obtain an explanation, or contacting her supervisor, or initiating more intrusive vetting. For example, a bankruptcy and a DUI arrest might indicate that the individual is under stress that might necessitate a review of his suitability for sensitive program access. A failure to report a foreign trip as required might trigger a further investigation. Employees whose "outside of work" activities show up in a big data analytics scan as possibly being of concern might have their use of government computers and data bases placed under additional scrutiny. We emphasize that employees with special access must not be stripped of their rights or subjected to Kafkaesque proceedings. For employees to be willing to participate in a Continuous Monitoring Program, they must know that they will have an opportunity to explain actions that may be flagged by data review.

We have noted that in the wake of recent security violations, some agencies are considering the more extensive use of polygraphy. There are widely varying views about the efficacy of polygraphing, but there can be no disputing that it cannot be a continuous process. It is unable to reveal events which occur after its use. The Personnel Continuous Monitoring Program, with its ongoing ingesting of information from commercial and government data bases, augmented by data analytics, is more likely to reveal any change in the status of an employee between programmed security clearance reviews.

Finally, the security clearance vetting process should also protect the rights of those with access to special programs and information. The President should also ensure that security clearance status not be affected by use of Whistle-Blower, Inspector General, or Congressional Oversight programs (see Appendix D).

About five million people now have active security clearances granted by some arm of the US Government, of which almost 1.5 million have Top Secret clearance. Although we do not have the capability to determine if those numbers are excessive, they certainly seem high. We believe that an interagency committee, representing not just the Intelligence Community, should review in detail why so many personnel require clearances and examine whether there are ways to reduce the total. Such a study may find that many of those with Secret-level clearances could do with a more limited form of access.

Personnel with Security Clearances (10/12)¹⁷⁸	Confidential/Secret	Top Secret
Government Employees	2,757,333	791,200
Contractors	582,524	483,263
Other	167,925	135,506
Subtotal	3,507,782	1,409,969
Total	4,917,751	

Once granted a clearance, only a very few have had it revoked for cause. Personnel lose clearances mainly because they retire or otherwise leave government service or change jobs. Indeed, many who leave government service manage to maintain their clearances as part-time advisors or by working with contractors. The strikingly small number of people who have their clearances revoked may be because the initial vetting process in all agencies does such a good job and because very few people become security risks after they are initially cleared. But, the numbers suggest to us that the re-vetting process, which usually occurs every five years, may in some agencies not be as rigorous as it should be. Sometimes the initial vetting is assumed to be correct and the only thing that is checked are the “new facts” that have occurred in the preceding five years. Sometimes the reviews that are supposed to take place every five

¹⁷⁸ Office of Director of National Intelligence, *2012 Report on Security Clearance Determinations*, p. 3, Table 1, (January 2013) available at www.fas.org/sgp/othergov/intel/clear-2012.pdf.

years are delayed. Many agencies do not have a program to obtain some kinds of important information in between security updates.

	Percent of Personnel Whose Security Clearances Were Revoked (FY 12) ¹⁷⁹
CIA	0.4
FBI	0.1
NGA	0.3
NRO	0.5
NSA	0.3
State	0.1

3. Information Sharing

Recommendation 41

We recommend that the “need-to-share” or “need-to-know” models should be replaced with a Work-Related Access model, which would ensure that all personnel whose role requires access to specific information have such access, without making the data more generally available to cleared personnel who are merely interested.

¹⁷⁹ Office of Director of National Intelligence, *2012 Report on Security Clearance Determinations*, p. 7, Table 5, (January 2013) available at www.fas.org/sgp/othergov/intel/clear-2012.pdf.

Classified information should be shared only with those who genuinely need to know. Beyond the use of compartments, however, the vast bulk of classified information is broadly available to people with security clearances. Analyses of the failure to prevent the September 11th, 2001 attacks concluded that information about those individuals involved in the plot had not been shared appropriately between and among agencies. Although some of that lack of sharing reflected intentional, high-level decisions, other data was not made broadly available because of a system that made it difficult to disseminate some kinds of information across agencies. Thus, after the attacks, the mantra "Need to Share" replaced the previous concept of "Need to Know."

In some contexts, that new approach may have gone too far or been too widely misunderstood. The "Need to Share" called for the distribution of relevant information to personnel with a job/task defined requirement for such information. It did not call for the profligate distribution of classified information to anyone with a security clearance and an interest in reading the information.

The problem with the "need-to-share" principle is that it gives rise to a multitude of other risks. Consistent with the goal of risk management, the appropriate guideline is that *information should be shared only with those who need to know*. There is no good reason to proliferate the number of people with whom information is shared if some or many of those people do not need or use that information in their work. The principle of "need to share"

can endanger privacy, heighten the risk of abuse, endanger public trust, and increase insider threats.

To be sure, the matching of one agency's records against another agency's records—for example, comparing fingerprints collected off of bomb fragments in Afghanistan to fingerprints culled at US border crossings—is one of the most important information tools we have in combating terrorism. Such sharing must continue, but can (and often does) take place on a machine-to-machine basis with strict control on which human beings can obtain access to the data.

To its credit, the Intelligence Community has been taking steps to restrict the number of people who have access to confidential or classified information. We applaud these steps. We recommend that seemingly compelling arguments about the importance of information-sharing should be qualified by a recognition that information should not be shared with those who do not have a genuine need to know.

B. Network Security¹⁸⁰

Recommendation 42

We recommend that the Government networks carrying Secret and higher classification information should use the best available cyber security hardware, software, and procedural protections against both external and internal threats. The National Security Advisor and the Director of the Office of Management and Budget should annually

¹⁸⁰ Michael Morell affirmatively recused himself from Review Group discussions of network security to mitigate the insider threat due to ongoing business interests.

report to the President on the implementation of this standard. All networks carrying classified data, including those in contractor corporations, should be subject to a Network Continuous Monitoring Program, similar to the EINSTEIN 3 and TUTELAGE programs, to record network traffic for real time and subsequent review to detect anomalous activity, malicious actions, and data breaches.

Recommendation 43

We recommend that the President's prior directions to improve the security of classified networks, Executive Order 13587, should be fully implemented as soon as possible.

Recommendation 44

We recommend that the National Security Council Principals Committee should annually meet to review the state of security of US Government networks carrying classified information, programs to improve such security, and evolving threats to such networks. An interagency "Red Team" should report annually to the Principals with an independent, "second opinion" on the state of security of the classified information networks.

Recommendation 45

We recommend that all US agencies and departments with classified information should expand their use of software, hardware, and procedures that limit access to documents and data to those specifically authorized to have access to them. The US Government should fund the development of, procure, and widely use on classified

networks improved Information Rights Management software to control the dissemination of classified data in a way that provides greater restrictions on access and use, as well as an audit trail of such use.

Information technology (IT) has become so central to the functioning of the government in general and national security in particular that policy officials need to be conversant with the technology. No longer can senior officials relegate concerns about IT networks to management or administrative staff. Policy officials are ultimately responsible for the IT networks of their organizations. They need to understand the systems and issues raised by technologists. Toward that end, technologists should be part of more policy, decision-making, and oversight processes. Similarly, national security policy officials need to take the time to understand in detail how the various components of the Intelligence Community work, and especially how their collection programs operate.

The security of classified networks is, in the age of cyber war, one of the highest priorities in national security. Nonetheless, the status of security improvement and the state of the cyber defenses of our sensitive networks have not been a topic for regular review by senior interagency policy officials. Department and agency leaders have also had little way to verify if the reports of their subordinates concerning the security of their classified networks are entirely accurate or complete. We recommend that there be an annual review by NSC Principals of the security of classified networks and the implementation of programmed upgrades. To inform the principals' discussion, we also recommend that the staffs of OMB and NSC

lead a process to identify issues and potential deficiencies. We also suggest that a "Red Team" be created to provide a second opinion to Principals on the security vulnerabilities of all classified networks.

The security of government networks carrying classified information has traditionally been outward looking. It was assumed that anyone who had access to the network had been subjected to extensive vetting and was therefore trustworthy and reliable.

There are two flaws in that thinking. First, as has been demonstrated, some people who have been given Top Secret/SCI clearances are not trustworthy. Second, it may be possible for unauthorized individuals to gain access to the classified networks and to assume the identity of an authorized user. The government's classified networks require immediate internal hardening.

Beyond measures designed to control access to data on networks, there is a need to increase the security of the classified networks in general. Many of the US Government's networks would benefit from a major technological refresh, to use newer and less vulnerable versions of operating systems, to adopt newer security software proven in the private sector, and to re-architect network designs to employ such improvements as Thin Client and air-gapped approaches.

Despite what some believe is the inherent security of classified networks, as the so-called Buckshot Yankee incident demonstrated, it is possible for foreign powers to penetrate US networks carrying classified information. Just as some foreign powers regularly attempt to penetrate

private sector networks in the US to steal intellectual property and research, others are engaged in frequent attempts to penetrate US networks with secret data.

To improve the security of classified networks, we believe that such networks should be given at least as much internal and external security as the most secure, unclassified networks in the private sector. Although many US corporations have inadequate network security, some in financial services have achieved a high level of assurance through the use of a risk management approach. State-of-the-art cyber security products used in private sector companies are not as often used on classified US Government networks as we would have believed likely.

We believe that inadequacy can be explained by two factors: 1) classified network administrators have traditionally focused on perimeter network defenses and 2) the procurement process in the government is too lengthy and too focused on large-scale system integrator contracts that do not easily allow for the agile adoption of new security products that keep up with the ever-changing threat. In our view, every department and agency's IT security budget and procurement processes ought to include funding set aside and procedures for the rapid acquisition and installation of newly developed security products related to recently appearing threats. These systems should be reviewed and procurement measures made through a decision making process that considers cost-benefit analysis, cost-effectiveness, and risk management.

1. Executive Order 13578

In recognition of the need to improve security on government networks with classified data, President Obama issued Executive Order 13587 to improve the security of classified networks against the Insider Threat. We have found that the implementation of that directive has been at best uneven and far too slow. Every day that it remains unimplemented, sensitive data, and therefore potentially lives, are at risk. Interagency implementation monitoring was not performed at a sufficiently high level in OMB or the NSS. The Administration did not direct the re-programming of adequate funds. Officials who were tardy in compliance were not held accountable. No central staff was created to enforce implementation or share best practices and lessons learned.

The implementation of Executive Order 13587 is in marked contrast to the enforcement of compliance with a somewhat similar effort, the conversion of government networks for Y2K. The Y2K software upgrades were carried out under the aegis of Executive Order 13073, issued only 22 months before the implementation deadline. That order established an Interagency Council co-chaired by an Assistant to the President and by the Director of OMB. It required quarterly reports to the President.

We believe that the implementation of Executive Order 13578 should be greatly accelerated, that deadlines should be moved up and enforced, and the adequate funding should be made available within agency budget ceilings and a Deputy Assistant to the President might be directed to

enforce implementation. The interagency process might be co-led by the Deputy Director of OMB.

In addition to the Insider Threat measures discussed above, we believe that government classified networks could have their overall security improved by, among other steps, priority implementation of the following:

- Network Continuous Monitoring techniques on all classified networks similar to the EINSTEIN-TUTELAGE Program now being implemented on US Government unclassified networks and the systems of certain private sector, critical infrastructure companies.
- A Security Operations Center (SOC) with real-time visibility on all classified US Government networks. There are now many SOCs, but no one place where fusion and total visibility takes place; and
- More severe limits on the movement of data from unclassified to classified networks. Although such data being uploaded is scanned today, the inspection is unlikely to detect a Zero Day threat (i.e. malicious software that has not been seen before).

2. Physical and Logical Separation

We believe that the most cost-effective efforts to enhance the security of IT networks carrying classified data are likely to be those that create greater physical and logical separation of data, through network segmentation, encryption, identity access management, access control to

data, limitation of data storage on clients, and “air-gapping.” Among the measures we suggest be more carefully considered are :

- The creation of Project Enclaves on networks, with firewalls, access control lists, and multi-factor (including biometric) authentication required for entry.
- Project-based encryption for data at rest and in use. Today, most data at rest on classified networks is not encrypted (although the networks and the data in transit are). Encrypting data whether at rest or in transit and linking that encryption with Identity Access Management (IAM) or IRM software would prevent reading by those not authorized even if they do access the data.
- IRM. To determine and limit who has access to data in a Project Based Encryption file, agencies should be encouraged to consider the use of IRM software that specifies what groups or individuals may read, or forward, or edit, or copy, or print, or download a document. IRM is known by other terms, such as Digital Rights Management, in some agencies. The IRM software should be linked to a multi-factor Identity Access Management system so that administrative and technical staff, such as System Administrators, and others cannot access the content of the data.
- Separation of Networks. Networks can be physically separated to varying degrees, from using separate colors on a fiber to using different fibers, to using different physical paths. In true “air-gapping,” a network shares no physical devices whatsoever with

other networks. In logical separation, networks may be maintained separate by firewalls, access controls, identity access management systems, and encryption. We believe that every relevant agency should conduct a review using cost-benefit analysis, and risk-management principles to determine if it would make sense to achieve greater security by further physical and logical separation of networks carrying data of highly sensitive programs.

We have found that there are few choices and perhaps insufficiently robust products today among Identity Rights Management software and among Insider Threat Anomaly Detection software. We believe that the government should fast track the development of Next-Generation IRM and Next-Generation Insider Threat software, waiving the normal research and procurement rules and timetables. The development of NextGen software in these areas should not, however, be an excuse for failure to deploy the software that is now available.

Fortunately, the government itself may have developed the basis for a more robust IRM software. The National Institute for Standards and Technology (NIST) of the Department of Commerce has created an Open Source platform for Next-Generation IRM software. Private sector developers should be granted access to that platform quickly, as well as encouraged to develop their own systems.

The NIST open source software, like other software now being used in some agencies, prevents the downloading of sensitive data from central servers. Analysts may access the data and employ it, but may not transfer

it. With the NIST software, the user sees an image of the data, but is unable to download it to a client and then to a thumb drive, CD, or other media. In general, we believe that sensitive data should reside only on servers and not on clients.

IRM systems and “data-on-server only” policies allow for auditing of data access, but they also generally presume the use of a data-tagging system when data is initially ingested into a network or system. We believe that additional work needs to be done to make that phase of data control less onerous, complex, and time-consuming. Government-sponsored development or procurement would promote the more rapid solution of those problems with data tagging.

NSA, among others, is returning to the Thin Client architecture, which many agencies abandoned 15-20 years ago in favor of cheaper, Commercial Off The Shelf (COTS) models. In the Thin Client architecture, the user may employ any screen on the network after properly authenticating. The screens, however, are “dumb terminals” with little software loaded on the devices. All applications and data are stored on servers, which are easier to secure and monitor than are large numbers of distributed clients. The use of a Thin Client architecture is, we believe, a more secure approach for classified networks and should be more widely used.

C. Cost-Benefit Analysis and Risk Management

Recommendation 46

We recommend the use of cost-benefit analysis and risk-management approaches, both prospective and retrospective, to orient judgments about personnel security and network security measures.

In our statement of principles, we have emphasized that in many domains, public officials rely on a careful analysis of both costs and benefits. In our view, both prospective and retrospective analysis have important roles to play in the domain under discussion, though they also present distinctive challenges, above all because of limits in available knowledge and challenges in quantifying certain variables. In particular, personnel security and network security measures should be subject to careful analysis of both benefits and costs (to the extent feasible).

Monetary costs certainly matter; public and private resources are limited. When new security procedures are put in place—for example, to reduce insider threats—the cost may well be ascertainable. It may be possible to identify a range, with upper and lower bounds. But the benefits of security procedures are likely to be more challenging to specify. It remains difficult, even today, to quantify the damage done by the recent leaks of NSA material. In principle, the question is the magnitude of the harm that is averted by new security procedures. Because those procedures may discourage insider threats from materializing, it will not be feasible to identify some averted harms.

Even if so, some analysis should be possible. For example, officials should be able to see to what extent new security procedures are helpful in detecting behavior with warning signs. Retrospective analysis can improve judgments by showing what is working and what is not. Risk-management approaches generally suggest hedging strategies on investment in preventative measures when detailed actuarial data are not available. That approach, along with breakeven analysis,¹⁸¹ may be necessary when considering risk contingencies that have never come to fruition in the past.

¹⁸¹ See OMB Circular A-4.

Conclusion

In this Report, we have explored both continuity and change. The continuity involves enduring values, which we have traced to the founding of the American republic. When the Constitution was ratified, We the People—in whom sovereignty resides—made commitments, at once, to the protection of the common defense, securing the blessings of liberty, and ensuring that people are “secure in their persons, houses, papers, and effects.” In the American tradition, liberty and security need not be in conflict. They can be mutually supportive. This understanding lies at the foundation of our culture and our rights, and it is shared by many of our close friends and allies.

At the same time, we live in a period of astonishingly rapid change. We face new threats to the common defense, including those that come from terrorism. For those who seek to do us harm, new technologies provide unprecedented opportunities for coordination across space and time, and also for identifying potential vulnerabilities. For the United States, our allies, and others whom we seek to protect, those very technologies provide opportunities to identify threats and to eliminate them. And in light of the pace of change, there is no question that today’s technologies, extraordinary though they are, will seem hopelessly primitive in the relatively near future—and that both the threats and the opportunities will expand accordingly. We have emphasized the importance of careful assessment of the real-world consequences of our

choices, and of a willingness to reassess those choices as new information is obtained.

Our goal in this Report has been to promote enduring values in a period of rapid change, and to assert that those values are essentially timeless. We have identified a series of reforms that are designed to safeguard the privacy and dignity of American citizens, and to promote public trust, while also allowing the Intelligence Community to do what must be done to respond to genuine threats.

No nation treats citizens of other nations the same way that it treats its own people, but we have emphasized that numerous steps can and should be taken to protect the privacy and dignity of citizens of other nations, including those who are outside the United States. We have also emphasized that surveillance should never be undertaken to promote illegitimate goals, such as the theft of trade secrets or the suppression of freedom of speech or religion.

We have also called for institutional reforms designed to ensure that NSA remains a foreign intelligence collection agency and that other institutions, both independent and inside the Executive Branch, work to protect privacy and civil liberty. We have stressed that it is exceedingly important to maintain a secure and open Internet, and several of our recommendations are designed to promote that goal. Protection of what we collect is indispensable to safeguarding national security, privacy, and public trust; the recommendations made here would significantly strengthen existing protections.

We have emphasized throughout that the central task is one of managing a wide assortment of risks. We are hopeful that the recommendations made here might prove helpful in striking the right balance. Free nations must protect themselves, and nations that protect themselves must remain free.

This page has been intentionally left blank.

Appendix A: The Legal Standards for Government Access to Communications

There is considerable complexity in the legal standards for government access to communications-related information. This Appendix seeks to make the legal requirements and possible reforms easier to understand. This is achieved by setting forth an outline consisting of four components. This short appendix can only set forth certain key elements of the law and is not aimed at representing a comprehensive picture of all relevant statutory provisions and jurisprudence.

The first component sets forth the burden of proof that the government must meet in order to obtain the information. From less strict to stricter, the burden of proof used in this area of law includes: (1) relevant; (2) reasonable grounds to believe, or reasonable and articulable suspicion; and (3) probable cause.

The second component sets forth the scope of the activity to which the burden of proof applies, such as a criminal investigation or foreign intelligence investigation. Both a law enforcement and FISA warrant require "probable cause." The probable cause is of a different thing, however. For a criminal warrant there must be probable cause that a crime has been, is, or will be committed. For a FISA warrant, there must be probable cause that the target is an agent of a foreign power.

The third component sets forth the level of authorization required to undertake the activity. The decision is sometimes made by the analyst, or

subject to approval within the executive branch, or subject to approval by a judge.

The fourth component is the nature of the information that can be obtained pursuant to the relevant legal authority.

If policymakers wish to raise the standards for government access, one or more of the first three components can be amended. For instance, a standard could be raised to probable cause, the scope of investigation could be narrowed, or higher-level approval could be required. Similarly, easing the standards could occur along one or more of these three dimensions. For instance, relevance might be required rather than a stricter standard, or the scope of the investigation could broaden, or no sign-off by higher authority would be needed.

This appendix sets forth the standards for law enforcement's undertaking of criminal investigations and the intelligence community's foreign intelligence investigations. The standards presented below are in some instances simplified, so the applicable statutes and case law should be consulted for further details.

LAW ENFORCEMENT PURPOSES

Traditional Warrant: (1) Probable cause. (2) Crime has been, is, or will be committed. (3) Order from a judge or, in the language of the Fourth Amendment, a "neutral magistrate." (4) Can obtain documents, records, or things.

Wiretap (18 U.S.C. § 2518): (1) Probable cause, plus additional requirements such as other investigatory methods are unlikely to succeed. (2) Crime has been, is, or will be committed, only for crimes listed in 18 U.S.C. § 2516. (3) Order issued by judge. (4) Conversations that are evidence of criminal activity.

Pen/Trap (18 U.S.C. § 3122): (1) Relevant. (2) Ongoing criminal investigation. (3) Order issued by Judge. (4) Communications meta-data (dialing, routing, addressing, and signaling information but not content).

Required Disclosure of Customer Communications Records (18 U.S.C. § 2703(d)): (1) Specific and articulable facts that there are reasonable grounds to believe relevant and material. (2) Ongoing criminal investigation. (3) Order issued by Judge. (4) Various classes of records, including opened e-mails if there is notice to the subscriber and non-content records with no notice requirement.

INTELLIGENCE PURPOSES

Title I FISA (50 U.S.C. § 1801): (1) Probable cause. (2) Target is an agent of a foreign power or a foreign power and each of the facilities or places is used or about to be used by a foreign power or an agent of a foreign power. (3) Order issued by FISC pursuant to AG certification. (4) Contents of communications.

Pen/Trap FISA (50 U.S.C. § 1842): (1) Relevant to an ongoing investigation. (2) To protect against international terrorism or clandestine intelligence

activities, or to obtain foreign intelligence information not concerning a US person. (3) Order issued by FISC pursuant to AG certification. (4) Communications meta-data (but not content).

FISA Section 702 (50 U.S.C. § 1881): (1) Reasonable belief person is non-US Person located outside the US and subject to one of the FISC-approved certifications. (2) To acquire foreign intelligence. (3) Targeting requested by analyst subject to review by adjudicators. (4) Content of communications.

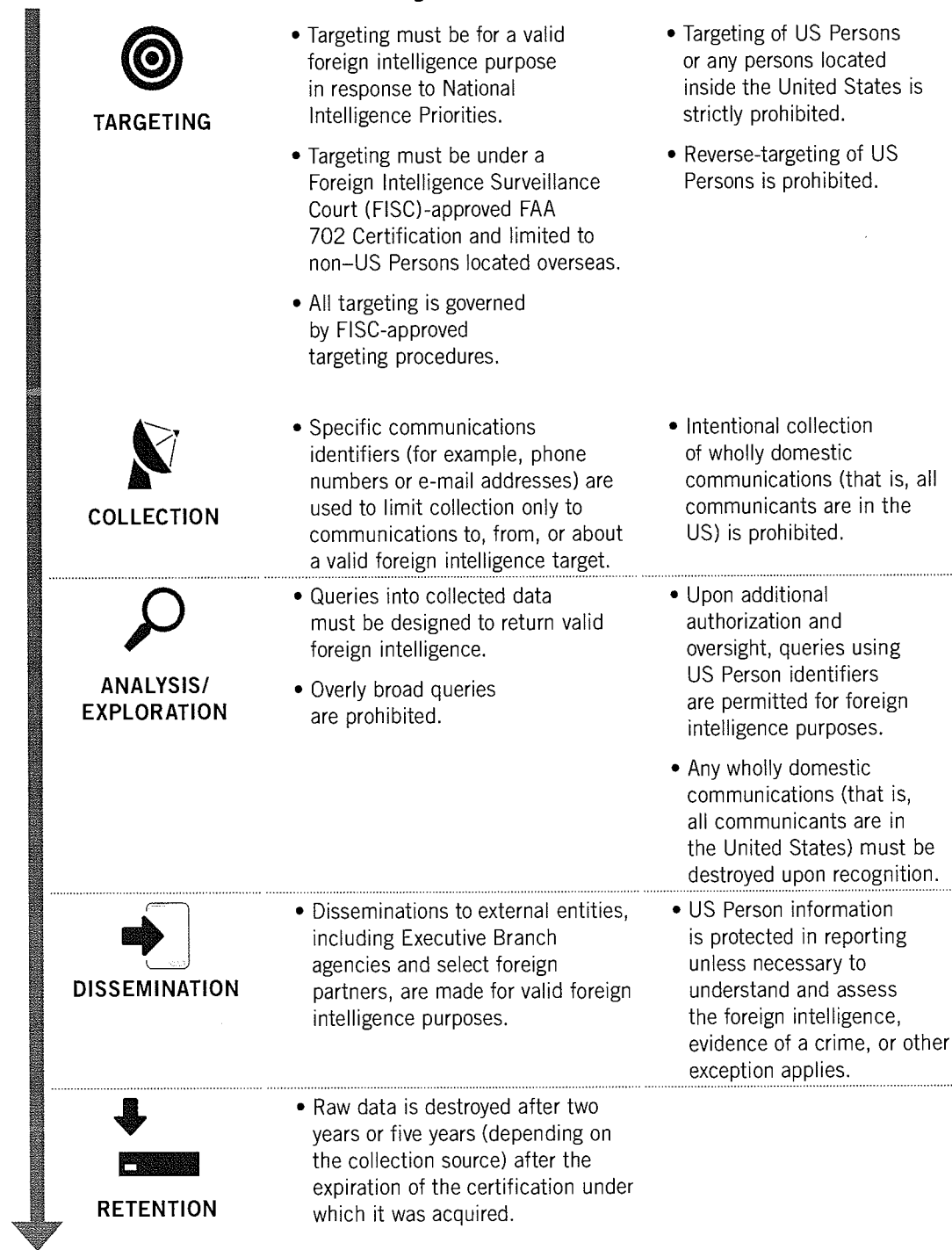
Section 215 (50 U.S.C. § 1861): (1) Reasonable grounds to believe that the tangible things sought are relevant. (2) To obtain foreign intelligence information about a non-US person or to protect against international terrorism or clandestine intelligence activities relevant to an authorized investigation. (3) Order issued by FISC pursuant to AG certification. (4) Documents, records, or other tangible things.

National Security Letters (50 U.S.C. § 436): (1) Relevant or pursuant to an open national security investigation. (2) For counterintelligence and counterterrorism, including cyber investigations. (3) FBI Special Agent in Charge or more senior FBI official. (4) Communications meta-data. Note: Other NSL statutes exists for other categories of records.

Executive Order 12333: (1) No requirement. (2) For foreign intelligence or counterintelligence purposes. (3) Decided by analyst with supervisory approval pursuant to internal guidelines. (4) Foreign intelligence information.

Appendix B:

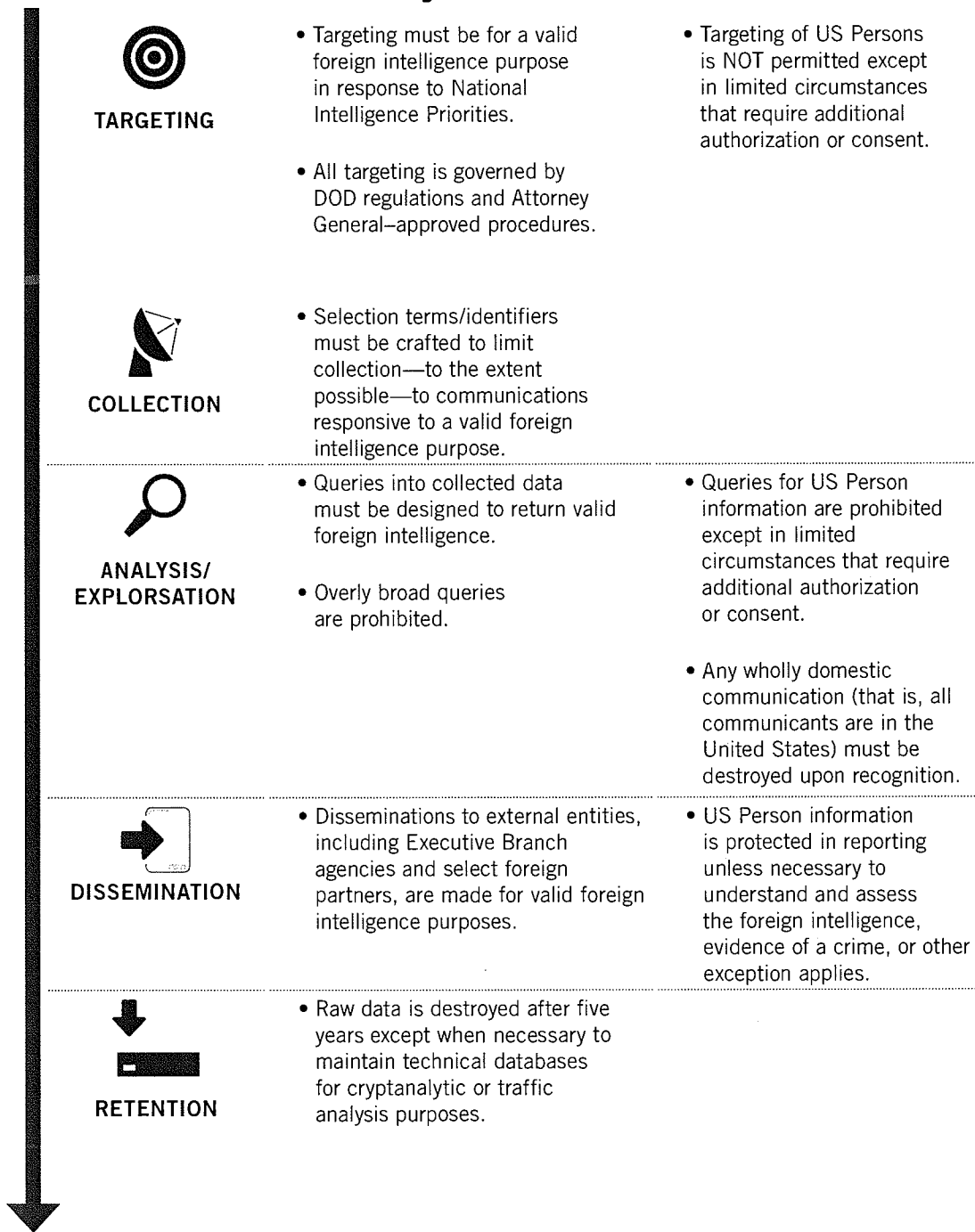
Overview of NSA Privacy Protections Under FAA 702



DISCLAIMER: This overview is a quick reference guide and is not intended as a substitute for the minimization procedures and their implementation.

Appendix B:

Overview of NSA Privacy Protections Under EO 12333



DISCLAIMER: This overview is a quick reference guide and is not intended as a substitute for the minimization procedures and their implementation.

Appendix C:

US Intelligence: Multiple Layers of Rules and Oversight

The graphic below illustrates the role played by each of the three branches of the US Government in governance of a query run by an intelligence analyst. On the left are the laws and guidelines that apply to actions of the analyst, setting forth the parameters within which the search may be conducted. The right side of the graphic highlights the review, oversight, and auditing functions of each of the three branches, once the search has been conducted.

Guidance to the IC**LEGISLATIVE BRANCH**

- Constitution
- Statutes

JUDICIAL BRANCH

- Court orders and standard minimization procedures

EXECUTIVE BRANCH

- Executive Orders and Presidential Directives
- Attorney General Guidelines
- IC Directives
- Agency regulations, instructions, and policies
- Agency training and guidance

*Analyst***Oversight and Enforcement****LEGISLATIVE BRANCH**

- Congress^a

JUDICIAL BRANCH

- Foreign Intelligence^b

EXECUTIVE BRANCH

- Privacy and Civil Liberties Oversight Board^c
- President's Intelligence Oversight Board^d
- Department of Justice^e
- ODNI-level officials^f
- Department-level officials^g
- Agency-level officials^h

^aDetermines whether and how to authorize/fund intelligence activities and conducts oversight via intelligence and other committees.

^bRules on matters under Foreign Intelligence Surveillance Act.

^cProvides privacy/civil liberties advice and oversight for USG efforts to protect the nation from terrorism.

^dReviews reports of potential violations of law and executive order on behalf of President.

^eIncludes DOJ's National Security Division and DOJ's Privacy and Civil Liberties Office.

^fIncludes ODNI's Civil Liberties and Privacy Office, ODNI/OGC, and the IC Inspector General.

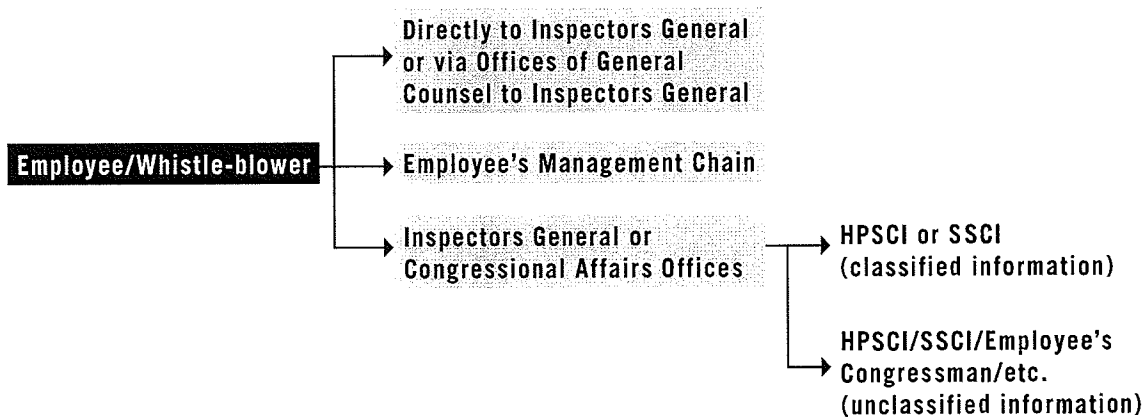
^gAt the department level, these can include departmental counterparts to the agency-level organizations, and may also include other offices (for example, DOD's Assistant to the Secretary of Defense for Intelligence oversight).

^hAt the agency level, these can include the following organizations: Offices of General Counsel, Offices of Inspector General, Civil Liberties and Privacy Offices, Intelligence Oversight Offices, Compliance Offices (for example, NSA's new Civil Liberties and Privacy Officer position, and NSA's Office of the Director of Compliance).

This page has been intentionally left blank.

Appendix D:

Avenues for Whistle-blowers in the Intelligence Community



EMPLOYEE PROTECTIONS FOR DISCLOSURES:

- National Security Act of 1947, CIA Act of 1949, Inspector General Act of 1978
 - Presidential Policy Directive No. 19
 - Agencies' Internal Policies
-

This page has been intentionally left blank.

Appendix E: US Government Role in Current Encryption Standards

NSA provided the Review Group the following information, outlining the reliability of certain encryption systems. Our recommendation 31 would give the force of law to prohibitions on undercutting these and other standards.

Most of the standards described below are approved by NIST for protecting unclassified US Government information and by NSA for protecting classified US Government information. AES, SHA-2, EC-DSA, and EC-DH make up the core of "Suite B," NSA's mandated set of public standard algorithms, approved in 2006, for protecting classified information.¹⁸² Each algorithm discussed below is currently in use in National Security Systems, although NSA is pursuing the transition from SHA-1 to SHA-2. For further information on all but SHA-1 see <https://www.cnss.gov/policies.html> and references contained there.

In general, NSA applies the deep cryptanalytic tradecraft and mathematical expertise developed over decades of making and breaking codes, to ensure that cryptography standardized by the US Government is strong enough to protect its own sensitive communications.

¹⁸² This paper addresses the strength of standard cryptographic algorithms. Any cryptographic algorithm can become exploitable if implemented incorrectly or used improperly. NSA works with NIST to ensure that NIST standards incorporate guidance on correct implementation and usage. NSA will exploit vulnerable implementations and uses to support the lawful conduct of signals intelligence.

AES - The Advanced Encryption Standard - FIPS 197

NSA did not contribute to nor modify the design of the Advanced Encryption Standard (AES). It was designed by two European cryptographers: Joan Daemen and Vincent Rijmen. It was published and submitted in 1998 for NIST's AES competition and selected in 2001 as the Advanced Encryption Standard. NSA extensively examined the algorithms in the competition and provided technical guidance to NIST during the competition to make sure that NIST's final selection was a secure algorithm. NIST made the final algorithm choice under its own authority, independent of NSA. Both NSA and the academic cryptography community have thoroughly analyzed the AES.

RSA - The Rivest, Shamir, Adelman Public Key Algorithm - FIPS 186, NIST SP 800-56B

NSA did not contribute to, nor modify, the design of RSA, but it did provide input on RSA usage in standards. It was designed in 1977 by three cryptographers working at MIT: Americans Ron Rivest, and Leonard Adelman, and Israeli Adi Shamir. The algorithm was independently designed earlier by Cliff Cocks of UK GCHQ in 1973 but was not published, and was only declassified in 1997. Both NSA and the academic cryptography community have thoroughly analyzed the RSA algorithm both as a digital signature (FIPS-186) and as an encryption algorithm for keys (SP 800-56B).

Diffie-Hellman/Elliptic Curve Diffie-Hellman - The Diffie-Hellman Key Exchange Algorithm - NIST SP 800-56A

NSA did not contribute to, nor modify, the design of Diffie-Hellman. The Diffie-Hellman Key Exchange Algorithm was designed by American cryptographer Whitfield Diffie and Martin Hellman at Stanford University in 1976. It was invented by Malcolm Williamson of GCHQ a few years earlier, but never published. The elliptic curve variant of the Diffie-Hellman key exchange was invented independently by American cryptographers Victor Miller and Neal Koblitz in 1985. NSA ensured that a class of potentially weak elliptic curve parameters was not included in the NIST standard. Both NSA and the academic cryptography community have thoroughly analyzed both the Diffie-Hellman Key Exchange algorithm and its elliptic curve variant (both found in NIST SP 800-56A).

DSA/ECDSA – The Digital Signature Algorithm/Elliptic Curve DSA – FIPS 186

NSA designed the algorithm known as DSA as the original signature algorithm in FIPS 186 initially in 1991-1993, then contributed advice on later versions of the standard. NSA also designed a variant of DSA that uses the mathematics of elliptic curves and is known as the “Elliptic Curve DSA” or ECDSA. Both NSA and the academic cryptography community have thoroughly analyzed the DSA (FIPS 186).

SHA-1 - The Secure Hash Algorithm Variant 1 - FIPS 180-1

NSA designed the SHA-1 algorithm as a correction to the SHA-0 algorithm, a longer (160-bit) variant of the MD5 algorithm designed by Ron Rivest.

SHA-0 was an NSA design standardized in 1993. In 1994, NSA acted quickly to replace SHA-0 with SHA-1 as a NIST standard when NSA cryptanalysts discovered a problem with the SHA-0 design that reduced its security. Both NSA and the academic cryptography community have thoroughly analyzed the SHA-1 (FIPS 180). For many years NIST and NSA have recommended that people stop using SHA-1 and start using the SHA-2 hash algorithms.

SHA-2 - The Secure Hash Algorithm Variant 2 - FIPS 180-2

NSA designed the four different-length hash algorithms contained in FIPS-180-2 and collectively known as SHA-2. Because of their longer hash lengths (224, 256, 384, and 512 bits), the SHA-2 hash lengths provide greater security than SHA-1. SHA-2 also blocks some algorithm weaknesses in the SHA-1 design. These algorithms were standardized in 2002. Both NSA and the academic cryptography community have thoroughly analyzed the SHA-2 hash algorithms (FIPS 180).

Appendix F: Review Group Briefings and Meetings

GOVERNMENT

Executive Branch

Assistant to the President for Homeland Security & Counterterrorism

Bureau of Alcohol, Tobacco, Firearms and Explosives

Central Intelligence Agency

Defense Intelligence Agency

Department of Commerce

Department of Defense

Department of Homeland Security

Department of Justice

Department of State

Drug Enforcement Agency

Federal Bureau of Investigations

National Archives and Records Administration

National Counterterrorism Center

National Institute for Standards and Technology

National Reconnaissance Office

National Security Advisor

National Security Agency

Office of the Director of National Intelligence

President's Intelligence Advisory Board

Privacy and Civil Liberties Oversight Board

Program Manager for the Information Sharing Environment (PM-ISE)

Special Assistant to the President for Cyber Security

Treasury Department

Legislative Branch

House Judiciary Committee

House Permanent Select Committee on Intelligence

Senate Judiciary Committee

Senate Select Committee on Intelligence

Judicial Branch

Judge John D. Bates, United States District Court Judge (former Foreign Intelligence Surveillance Court Judge)

PRIVATE ENTITIES

Organizations

American Civil Liberties Union

Apple

AT&T

Brennan Center for Justice

CATO Institute

Center for Democracy & Technology

Center for National Security Studies

Electronic Frontier Foundation

Electronic Privacy Information Center

Enterprise Risk Management/Root Cause Analysis

Facebook

Google

Human Rights Watch

IBM Center for Excellence

Information Technology and Innovation Foundation

Information Technology Industry Council

Microsoft

New America Foundation

Open Technology Institute

Palantir

Rackspace

Reporters Committee for Freedom of the Press

Software & Information Industry Association

the TOR Project

Verizon

Yahoo

Individuals

Baker, Stewart; Steptoe & Johnson

Berman, Jerry

Blaze, Matt; University of Pennsylvania

Bowden, Caspar

Cate, Fred; Indiana University

Donohue, Laura; Georgetown Law School

Farber, David; Carnegie Mellon University

Felten, Ed; Princeton University

Klein, Hans; Georgia Institute of Technology

Kris, David; Intellectual Ventures (Former DoJ NSD Chief)

Malinowski, Tom; Human Rights Watch former director

Soltani, Ashkan

Wittes, Ben; Brookings Institution

Wolf, Christopher; Hogan, Lovells

FOREIGN ORGANIZATIONS

(LIBE) European Parliament Committee on Civil Liberties, Justice, and
Home Affairs

European Union Privacy & Civil Liberties delegation

This page has been intentionally left blank.

Appendix G: Glossary

A (AES) Advanced Encryption Standard An encryption algorithm for securing sensitive but unclassified material by US Government agencies and, as a consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector.

Source:

<http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>

AG Attorney General

B Backdoor A means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes.

Source:

<http://searchsecurity.techtarget.com/definition/back-door>

Big Data Analytics The process of examining large amounts of data of a variety of types (big data) to uncover hidden patterns, unknown

correlations, and other useful information.

Source:

<http://searchbusinessanalytics.techtarget.com/definition/big-data-analytics>

Bulk Data An electronic collection of data composed of information from multiple records, whose primary relationship to each other is their shared origin from a single or multiple databases.

Source:

<http://www.maine.gov/legis/opla/RTKINFORMEcomments.pdf>

- C Church Committee An 11-member investigating body of the Senate (a Senate Select Committee) that studied governmental operations with respect to Intelligence Activities. It published 14 reports that contain a wealth of information on the formation, operation, and abuses of US intelligence agencies. The reports were published in 1975 and 1976, after which recommendations for reform were debated in Congress and in some cases enacted.

Source:

http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm

CIA Central Intelligence Agency

Cloud Computing A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Source:

<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>

CLPP Board Civil Liberties and Privacy Protection Board

(CMP) Continuous Monitoring Program Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Source:

<http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>

Counter-intelligence Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on

behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities.

Source: (Executive Order 12333, as amended 30 July 2008 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

<http://www.fas.org/irp/eprint/ci-glossary.pdf>

Counter-proliferation Those actions (e.g., detect and monitor, prepare to conduct counter-proliferation operations, offensive operations, weapons of mass destruction, active defense, and passive defense) taken to defeat the threat and/or use of weapons of mass destruction against the United States, our military forces, friends, and allies.

Source: (JP 1-02 & JP 3-40)

<http://www.fas.org/irp/eprint/ci-glossary.pdf>

D Data Mining The process of collecting, searching through, and analyzing a large amount of data within a database, to discover patterns of relationships.

Source:

<http://dictionary.reference.com/browse/data+mining?s=t>

Decryption The process of converting encrypted data back to its original form, so it can be understood.

Source:

<http://searchsecurity.techtarget.com/definition/encryption>

DHS Department of Homeland Security

DIAA Defense Information Assurance Agency

Diffie-Hellman Key Exchange Algorithm Cryptographic algorithm used for secure key exchange. The algorithm allows two users to exchange a symmetric secret key through an insecure wired or wireless channel and without any prior secrets.

Source: (2005 International Conference on Wireless Networks, Communications and Mobile Computing)

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1549408&tag=1

(DRM) Digital Rights Management/ (IRM) Information Rights Management A collection of systems and software applications used to protect the copyrights of documents and electronic media. These include digital music and movies, as well as other data that is stored and transferred digitally. DRM is important to publisher of electronic media because it helps to control the trading, protection, monitoring, and tracking of digital media, limiting the illegal propagation of

copyrighted works.

Source:

<http://www.techterms.com/definitions/drm>

DISA Defense Information Systems Agency

DNI Director of National Intelligence

DOD Department of Defense

DOJ Department of Justice

DTRA Defense Threat Reduction Agency

- E Einstein 3 An advanced, network-layer intrusion detection system (IDS) which analyzes Internet traffic as it moves in and out of United States Federal Government networks. EINSTEIN filters packets at the gateway and reports anomalies to the United States Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security.

Source:

<http://searchsecurity.techtargget.com/definition/Einstein>

Encryption The conversion of data into a form, called a ciphertext (encrypted text), that cannot be easily understood by unauthorized people.

Source:

<http://searchsecurity.techtargget.com/definition/encryption>

Executive Order Official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

Source:

<http://www.archives.gov/federal-register/executive-orders/about.html>

Executive Order 12333 Under section 2.3, intelligence agencies can only collect, retain, and disseminate information about a “US person” (US citizens and lawful permanent residents) if permitted by applicable law, if the information fits within one of the enumerated categories under Executive Order 12333, and if it is permitted under that agency’s implementing guidelines approved by the Attorney General. The EO has been amended to reflect the changing security and intelligence

environment and structure within the US Government.

Source:

<https://it.ojp.gov/default.aspx?area=privacy&page=1261#12333>

F FBI Federal Bureau of Investigation

(FISA) Foreign Intelligence Surveillance Act As amended, establishes procedures for the authorization of electronic surveillance, use of pen registers and trap-and-trace devices, physical searches, and business records for the purpose of gathering foreign intelligence.

Source:

<https://it.ojp.gov/default.aspx?area=privacy&page=1286>

(FISC) Foreign Intelligence Surveillance Court A special court for which the Chief Justice of the United States designates 11 federal district court judges to review applications for warrants related to national security investigations.

Source:

https://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html

FTC Federal Trade Commission

- I Identifier/Selector Communication accounts associated with a target (e.g., e-mails address, phone number)

IAD Information Assurance Directorate of the National Security Agency

Intelligence Community Seventeen-member group of Executive Branch agencies and organizations that work separately and together to engage in intelligence activities, either in an oversight, managerial, support, or participatory role necessary for the conduct of foreign relations and the protection of the national security of the United States.

Source:

<http://www.fas.org/irp/eprint/ci-glossary.pdf>

- M Meta-data A characterization or description documenting the identification, management, nature, use, or location of information resources (data).

Source: A Glossary of Archival and Records Terminology Copyright,

2012, Society of American Archivists,
(<http://www2.archivists.org/glossary>).

(MLAT) Mutual Legal Assistance Treaty An understanding and agreement between two countries that wish to mutually cooperate regarding investigation, prosecution, and enforcement of the provisions of the laws of the agreeing countries. The MLAT also specifies the grounds on which a request by either nation may be rejected or denied by the other nation.

Source:

http://perry4law.org/clic/?page_id=39

N NAS National Academy of Sciences

(NIPF) National Intelligence Priorities Framework DNI's guidance to the Intelligence Community on the national intelligence priorities approved by the President. The NIPF guides prioritization for the operation, planning, and programming of US intelligence analysis and collection.

Source:

<http://www.fbi.gov/about-us/nsb/faqs>

(NSC/DC) National Security Council Deputies Committee The senior sub-Cabinet interagency forum for consideration of policy issues affecting national security. The NSC/DC prescribes and review work for the NSC interagency groups discussed in a directive. The NSC/DC helps to ensure issues brought before the NSC/PC or the NSC have been properly analyzed and prepared for decision. The regular members of the NSC/DC consist of the Deputy Secretary of State or Under Secretary of the Treasury or Under Secretary of the Treasury for International Affairs, the Deputy Secretary of Defense or Under Secretary of Defense for Policy, the Deputy Attorney General, the Deputy Director of the Office of Management and Budget, the Deputy Director of Central Intelligence, the Vice Chairman of the Joint Chiefs of Staff, the Deputy Chiefs of Staff to the President for Policy, the Chief of Staff and National Security Advisor to the Vice President, the Deputy Assistant to the President for International Economic Affairs, and the Assistant to the President and Deputy National Security Advisor (who shall serve as chair).

Source:

<http://www.fas.org/irp/offdocs/nspd/nspd-1.htm>

(NSC/PC) National Security Council Principals Committee The senior interagency forum for consideration of policy affecting national security. The regular members of the NSC/PC consist of the Secretary

of State, the Secretary of the Treasury, the Secretary of Defense, the Chief of Staff to the President, and the Assistant to the President for National Security Affairs, who serves and chair.

Source:

<http://www.fas.org/irp/offdocs/nspd/nspd-1.htm>

(NSL) National Security Letter A letter from a United States government agency demanding information related to national security. It is independent of legal courts and therefore is different from a subpoena. It is used mainly by FBI when investigating matters related to national security. It is issued to a particular entity or organization to turn over records and data pertaining to individuals. By law, NSLs can request only non-content information, such as transactional records, phone numbers dialed, or sender or recipient of the letter from disclosing that the letter was ever issued.

Source:

http://en.wikipedia.org/wiki/National_security_letter

Source: USA PATRIOT Improvement and Reauthorization Act of 2005: A legal Analysis Congressional Research Service's report for Congress, Brian T. Yeh, Charles Doyle, December 21, 2006.

NSS National Security Staff

NIST National Institute of Standards and Technology

Non-Disclosure Agreement (commonly referred to as "Gag Orders")
Contracts intended to protect information considered to be proprietary or confidential. Parties involved in executing a NDA promise not to divulge secret or protected information.

Source:

<http://inventors.about.com/od/nondisclosure/a/Nondisclosure.htm>

NRC National Research Council

NRO National Reconnaissance Office

NSA National Security Agency

NSD/DoJ National Security Division of the Department of Justice

O ODNI Office of the Director of National Intelligence

ODOC NSA's Office of the Director of Compliance

OIA/DoJ Office of International Affairs of the Department of Justice

OMB Office of Management and Budget

OSD Office of the Secretary of Defense

OTA Office of Technology Assessment

P PATRIOT Act An Act of Congress that was signed into law by President George W. Bush on October 26, 2001. The title of the act is a ten-letter acronym (USA PATRIOT) that stands for Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001.

Source:

<http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm>

PCLOB Privacy and Civil Liberties Oversight Board

Pen Register A device that decodes or records electronic impulses, allowing outgoing numbers from a telephone to be identified.

Source:

<http://legal-dictionary.thefreedictionary.com/Pen+Register>

PII Personally identifiable information

PIBD Public Interest Declassification Board

R (RAS) Reasonable Articulate Suspicion/Reasonable Grounds to Believe (as applied to Section 215) A legal standard of proof in United States law that is less than probable cause, the legal standard for arrests and warrants, but more than an “inchoate and unparticularized suspicion or ‘hunch’”; it must be based on “specific and articulable facts”, “taken together with rational inferences from those facts.”

Source:

<http://supreme.justia.com/cases/federal/us/392/1/case.html#27>

Source:

http://en.wikipedia.org/wik/Reasonable_Articulable_Suspicion#cite_note-1

Rockefeller Commission Headed by Vice-President Nelson Rockefeller, the commission issued a single report in 1975, which delineated CIA abuses including mail openings and surveillance of domestic dissident groups.

Source:

http://historymatters.com/archive/contents/church/contents_church_reports_rockcomm.htm

RSA Algorithm (Rivest-Shamir-Adleman) An Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape and many other products.

Source: <http://searchsecurity.techtarget.com/definition/RSA>

S Section 215 Statutory provision of FISA that permits the government access to business records for foreign intelligence and international terrorism investigations. The governing federal officials are permitted the ability to acquire business and other 'tangible records' which include: business records, phone provider records, apartment rental

records, driver's license, library records, book sales records, gun sales records, tax return records, educational records, and medical records. Under this provision, federal investigators can compel third-party record holders, such as telecom firms, banks or others, to disclose these documents. In order to use this provision, the US government must show that there are reasonable grounds to believe that the records are relevant to an international terrorism or counterintelligence investigation.

Source:

<http://www.law.cornell.edu/uscode/text/50/1861>

Source:

http://belfercenter.ksg.harvard.edu/publication/19163/usapatriot_act.html

Section 702 Statutory provision for the targeting of individuals reasonably believed to be non-U.S persons located outside the United States.

Source:

<http://www.fas.org/irp/news/2013/06/nsa-sect702.pdf>

(SSL) Secure Sockets Layer A commonly used protocol for managing the security of a message transmission on the internet.

Source:

<http://searchsecurity.techtargt.com/definition/Secure-Sockets-Layer-SSL>

(SIGINT) Signals Intelligence Intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, and radar communications system.

Source:

<http://www.nsa.gov/sigint>

Social Networking A dedicated website or other application that enables users to communicate with each other by posting information, comments, messages, images, etc...

Source:

http://www.oxforddictionaries.com/us/definition/american_english/social-network

Splinternet Also referred to as “cyberbalkanization” or “Internet Balkanization”, it is the segregation of the Internet into smaller groups with similar interests, to a degree that they show a narrow-minded approach to outsiders or those with contradictory views.

Source:

<http://www.techopedia.com/definition/28087/cyberbalkanization>

T Third Party Doctrine Provides that information “knowingly exposed” to a third party is not subject to Fourth Amendment protection because one “assumes the risk” that the third party will disclose that information. The doctrine holds that the information that individual disclosed to businesses credit card transactions, phone records, etc. doesn’t carry with it a “reasonable expectation of privacy” under the Fourth Amendment, as one has “assumed the risk” that this information might at some point be disclosed.

Source:

http://www.lawtechjournal.com/articles/2007/02_070426_lawless.pdf

Source:

<http://www.nationalreview.com/agenda/350896/third-party-doctrine-reihan-salam>

T-TIP Transatlantic Trade and Investment Partnership

Trap-and-Trace A device or process 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, provided, however, that such information shall not include the contents of any communication.

Source: 18 USC. § 3127(3)

Tutelage The codename of a classified NSA technology used to monitor communications used on military networks.

Source: <http://www.wired.com/threatlevel/2009/07/einstein/>

W Warfighter Military personnel with a combat or combat related mission.

Whistle-Blower A person who tells someone in authority about something they believe to be illegal that is happening, especially in a government department or a company.

Source:

<http://dictionary.cambridge.org/dictionary/british/whistle-blower>

Wiretap To place a device on (someone's phone) in order to secretly listen to telephone calls.

Source:

<http://www.merriam-webster.com/dictionary/wiretap>

Z Zero Day Exploitation Taking advantage of security vulnerability on the same day that the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack. It is an exploit of vulnerability in software, which is being utilized for the first time and which, therefore, is unknown to defensive software.

Source:

<http://searchsecurity.techtarget.com/definition/zero-day-exploit>

This page has been intentionally left blank.

This page has been intentionally left blank.

Exhibit C

Exhibit C



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

***Report on the Telephone Records Program
Conducted under Section 215
of the USA PATRIOT Act and on the
Operations of the Foreign Intelligence Surveillance Court***

JANUARY 23, 2014

Privacy and Civil Liberties Oversight Board

David Medine, Chairman

Rachel Brand

Elisebeth Collins Cook

James Dempsey

Patricia Wald



PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

**Report on the Telephone Records Program Conducted under Section 215 of the USA
PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court**

Part 1 INTRODUCTION	1
Part 2 EXECUTIVE SUMMARY	8
Part 3 DESCRIPTION OF THE NSA SECTION 215 PROGRAM	21
Part 4 HISTORY OF THE NSA SECTION 215 PROGRAM	37
Part 5 STATUTORY ANALYSIS	57
Part 6 CONSTITUTIONAL ANALYSIS	103
Part 7 POLICY ANALYSIS AND RECOMMENDATIONS REGARDING THE NSA SECTION 215 PROGRAM	137
Part 8 DISCUSSION AND RECOMMENDATIONS REGARDING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT	173
Part 9 DISCUSSION AND RECOMMENDATIONS REGARDING TRANSPARENCY	190
Part 10 CONCLUSION	207
ANNEXES.....	208
A. Separate Statement by Board Member Rachel Brand	208
B. Separate Statement by Board Member Elisebeth Collins Cook	214
C. July 9, 2013 Workshop Agenda and Link to Workshop Transcript	219

D. November 4, 2013 Hearing Agenda and Link to Hearing Transcript 222

E. Request for Public Comments on Board Study 225

F. Index to Public Comments on www.regulations.gov 227

Part 1: INTRODUCTION

On June 5, 2013, the British newspaper *The Guardian* published the first of a series of articles based on unauthorized disclosures of classified documents by Edward Snowden, a contractor for the National Security Agency (“NSA”).¹ The article described an NSA program to collect millions of telephone records, including records about purely domestic calls. Over the course of the next several days, there were additional articles regarding this program as well as another NSA program referred to in leaked documents as “PRISM.”

These disclosures caused a great deal of concern both over the extent to which they damaged national security and over the nature and scope of the surveillance programs they purported to reveal. Subsequently, authorized disclosures from the government confirmed both programs. Under one, the NSA collects telephone call records or metadata — but not the content of phone conversations — covering the calls of most Americans on an ongoing basis, subject to renewed approvals by the Foreign Intelligence Surveillance Court (“FISC” or “FISA court”). This program was approved by the FISC pursuant to Section 215 of the USA PATRIOT Act (“Patriot Act”). Under the second program, the government collects the content of electronic communications, including phone calls and emails, where the targets are reasonably believed to be non-U.S. persons located outside the United States.² Section 702 of the FISA Amendments Act is the basis for this program.³

Immediately following the press revelations, the public and many policymakers began asking questions about the scope and nature of these NSA programs. Central among the issues raised was the degree to which the programs included appropriate safeguards for privacy and civil liberties. One week after the first news article appeared, a bipartisan group of thirteen U.S. Senators asked the recently reconstituted Privacy and Civil Liberties Oversight Board (“PCLOB”) to investigate the two NSA programs and to provide an unclassified report “so that the public and the Congress can have a long overdue debate” about the privacy issues raised.⁴ A July 11, 2013, letter from House Minority Leader Nancy Pelosi requested that the Board also consider the operations of the FISC, which approved

¹ See Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013).

² Even when the target is a non-U.S. person, collections of communications involving U.S. persons may still occur, either where those individuals are in communication with non-U.S. persons or where they are mistakenly believed to be non-U.S. persons.

³ This is the program inaccurately referred to in early reports as the PRISM program. PRISM is actually the database in which such communications are compiled.

⁴ Letter from Senator Tom Udall *et al.* to the Privacy and Civil Liberties Oversight Board (June 12, 2013), available at <http://www.pclob.gov/>.

the two programs. On June 21, 2013, the Board met with President Obama and his senior staff at the White House, and the President asked the Board to review “where our counterterrorism efforts and our values come into tension.”⁵

In response to the congressional and presidential requests, the Board immediately initiated a study of the 215 and 702 programs and the operation of the FISA court. This Report contains the results of the Board’s 215 program study as well as our analysis and recommendations regarding the FISC’s operation.

I. Background

The PCLOB is an independent bipartisan agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act of 2007.⁶ The Board is comprised of four part-time members and a full-time chairman, all appointed by the President and confirmed by the Senate. The Board’s authorizing statute gives it two primary responsibilities:

- 1) To analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and
- 2) To ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.⁷

This Report arises out of the Board’s responsibility to provide oversight by analyzing and reviewing executive branch actions, in this case the operation of the Section 215 telephone records program.

The Board today is in its third iteration. In July 2004, the National Commission on Terrorist Attacks on the United States (known as the 9/11 Commission) recommended that “there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil

⁵ See Letter from Democratic Leader Nancy Pelosi to Chairman David Medine (July 11, 2013), available at <http://www.pclob.gov/>; Remarks by the President in a Press Conference at the White House (Aug. 9, 2013), available at <http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference>.

⁶ Pub. L. No. 110-53, § 801(a), 121 Stat. 266, 352-58 (2007).

⁷ See Pub. L. No. 110-53, § 801(a) (codified at 42 U.S.C. § 2000ee).

liberties.”⁸ In August 2004, President George W. Bush created the President’s Board on Safeguarding Americans’ Civil Liberties by executive order.⁹ The President’s Board ceased to meet upon the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004, which created a Privacy and Civil Liberties Oversight Board within the Executive Office of the President.¹⁰

In 2007, the Implementing Recommendations of the 9/11 Commission Act reconstituted the Board in its current form as an independent agency within the executive branch.¹¹ The Act requires that all five Board members be appointed by the President, by and with the advice and consent of the Senate, for staggered six-year terms. The Act further requires that the Board be bipartisan in composition. No more than three of the five members may be from the same political party, and before appointing members who are not from the President’s political party, the President must consult with the leadership of the opposing party.

With the reconstitution of the Board, the 9/11 Commission Act terminated, effective January 30, 2008, the terms of the individuals then serving as Board members within the Executive Office of the President. From that time until August 2012, the Board did not function, as none of the positions on the Board were filled. Then, in August 2012, the Board’s current four part-time members were confirmed by the Senate, providing the reconstituted Board with its first confirmed members and a quorum to begin operations.¹²

⁸ THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, at 395 (2004). The 9/11 Commission was a bipartisan panel established to “make a full and complete accounting of the circumstances surrounding” the September 11, 2001, terrorist attacks, and to provide “recommendations for corrective measures that can be taken to prevent acts of terrorism.” Intelligence Authorization Act for Fiscal Year 2003, Pub. L. No. 107-306, § 602(4), (5), 116 Stat. 2383, 2408 (2002).

⁹ See Exec. Order No. 13353, 69 Fed. Reg. 53,585 (Aug. 27, 2004). The President’s Board was chaired by the Deputy Attorney General and consisted of twenty-two representatives from the Departments of State, Defense, Justice, Treasury, Health and Human Services, and Homeland Security; the Office of Management and Budget; and the Intelligence Community. During its tenure, the President’s Board met six times.

¹⁰ See Pub. L. No. 108-458, § 1061(b), 118 Stat. 3638, 3684 (2004). As chartered under IRTPA, the Board was comprised of two Board members appointed by the President, by and with the advice and consent of the Senate, and three additional Board members appointed by the President. *Id.* § 1061(e)(1).

¹¹ See Pub. L. No. 110-53, § 801(a), 121 Stat. 266, 352-58 (2007).

¹² The Board’s four part-time members were confirmed by the Senate on August 2, 2012, and were appointed by the President and sworn into office later that month for the following terms:

- Rachel L. Brand, for a term ending January 29, 2017;
- Elisebeth Collins Cook, for a term ending January 29, 2014. On January 6, 2014, Ms. Cook was nominated for a second term ending January 29, 2020. Under the Board’s authorizing statute, as a result of this nomination, Ms. Cook can continue to serve through the end of the Senate’s current session and, if confirmed before then, through January 29, 2020.
- James X. Dempsey, for a term ending January 29, 2016; and

The Board's chairman, its only full-time member, was confirmed on May 7, 2013, and sworn in on May 29, five days before news stories based upon the NSA leaks began to appear.

Since the PCLOB began operations as an independent agency in August 2012, it has released two semi-annual reports to Congress and the President summarizing the agency's start up activities.¹³ This Report represents the Board's first comprehensive study of a government program.

II. Study Methodology

In response to the congressional and presidential requests, the PCLOB undertook an in-depth study of the Section 215 and 702 programs as well as the operations of the FISA court.¹⁴ This study included classified briefings with officials from the Office of the Director for National Intelligence ("ODNI"), NSA, Department of Justice, Federal Bureau of Investigation ("FBI"), and Central Intelligence Agency ("CIA"). Board members also met with White House staff, a former presiding judge of the FISA court, academics, privacy and civil liberties advocates, technology and communications companies, and trade associations. The Board also received a demonstration of the Section 215 program's operation and capabilities at the NSA. The Board has been provided access to classified opinions by the FISC, various inspector general reports, and additional classified documents relating to the operation and effectiveness of the programs. At every step of the way, the Board has received the full cooperation of the intelligence agencies. Board staff have conducted a detailed analysis of applicable statutory authorities, the First and Fourth Amendments to the Constitution, and privacy and civil liberties policy issues.

As part of its study, and consistent with our statutory mandate to operate publicly where possible, the Board held two public forums. The first was a day-long public workshop held in Washington, D.C., on July 9, 2013, comprised of three panels addressing

-
- Patricia M. Wald, for a term ending January 29, 2013. On December 12, 2013, the Senate confirmed Ms. Wald for a second term ending January 29, 2019.

The Board's chairman and only full-time member, David Medine, was originally nominated by the President on December 15, 2011, and was re-nominated on January 22, 2013. The Senate confirmed Mr. Medine on May 7, 2013, and he was sworn in on May 29, 2013, for a term ending January 29, 2018.

¹³ See Privacy and Civil Liberties Oversight Board, Semi-Annual Report, September 2012 to March 2013 (June 27, 2013); Privacy and Civil Liberties Oversight Board, Semi-Annual Report, March 2013 to September 2013 (Nov. 3, 2013), available at <http://www.pclob.gov/>.

¹⁴ Prior to the confirmation of the chairman, the four part-time members had identified implementation of the FISA Amendments Act as a priority for oversight; in other words, the Section 702 Program already was familiar to the majority of the Board in June 2013.

different aspects of the Section 215 and 702 programs.¹⁵ The panelists provided input on the legal, constitutional, technology, and policy issues implicated by the two programs. The first panel addressed the legality of the programs, and included comments from a former FISC judge regarding the operation of that court. Because technological issues are central to the operations of both programs, the second panel was comprised of technology experts. The third panel included academics and members of the advocacy community; panelists were invited to provide views on the policy implications of the NSA programs and what changes, if any, would be appropriate.

As the Board's study of the NSA surveillance programs moved forward, the Board began to consider possible recommendations for program changes. At the same time, the Board wanted to try to identify any unanticipated consequences of reforms it was considering. Accordingly, on November 4, 2013, the Board held a public hearing in Washington, D.C.¹⁶ The hearing began with a panel of current government officials who addressed the value of the programs and the potential impact of proposed changes. The second panel, designed to explore the operation of the FISA court, consisted of another former FISC judge, along with a former government official and a private attorney who both had appeared before the FISC. Finally, the Board heard from a diverse panel of experts on potential Section 215 and 702 reforms.

The Board provided its draft description of the operations of the FISA court (but not our recommendations) to court's staff to ensure that this description accurately portrayed the court's operations. The Board also provided draft portions of its analysis regarding the effectiveness of the Section 215 program (but not our conclusions and recommendations) to the U.S. Intelligence Community to ensure that our factual statements were correct and complete. While the Board's Report was subject to classification review, none of the changes resulting from that process affected our analysis or recommendations. There was no outside review of the substance of the Board's analysis and recommendations.

During the time the PCLOB has been conducting this study, members of Congress have introduced a variety of legislative proposals to address the Section 215 and 702 programs, the government has engaged in several internal reviews of the programs, and several lawsuits have been filed challenging the programs' legitimacy. To ensure that the PCLOB's recommendations may be considered as part of this ongoing debate, the Board divided this study into two parts. The first part, this Report, covers the PCLOB's analysis and recommendations regarding operation of the 215 program and the FISA court. The second part will be a subsequent unclassified report containing PCLOB's analysis and recommendations concerning the 702 program.

¹⁵ See Annex C.

¹⁶ See Annex D.

In addition, proposals for modifications to the Section 215 program and the operation of the FISC were under active consideration by the White House while we were conducting our study. Pursuant to the Board's statutory duty to advise the President and elements of the executive branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation of legislation and policies and to provide advice on proposals to retain or enhance a particular power, the PCLOB briefed senior White House staff on the Board's tentative conclusions on December 5, 2013. The PCLOB provided a near final draft of the Board's conclusions and recommendations on Section 215 and the operations of the FISA court (Parts 5, 7 and 8 of this Report) to the White House on January 3, the transparency section (Part 9) on January 8, 2014, and additional statutory analysis on January 14, 2014 (Part 5). On January 8, the full Board met with the President, the Vice President and senior officials to present the Board's conclusions and the views of individual Board members.

III. Report Organization

The body of this Report consists of seven sections, five of which address the Section 215 telephone records program. After this introduction and the executive summary, Part 3 describes in detail how the telephone records program works. To put the present-day operation of the program in context, Part 4 reviews its history, including its evolution from predecessor intelligence activities. An analysis of whether the telephone records program meets applicable statutory requirements follows in Part 5. Part 6 addresses the constitutional issues raised by the telephone records program under both the First and Fourth Amendments. The final section discussing the Section 215 program, Part 7, examines the potential benefits of the program, its efficacy in achieving its purposes, the impact of the program on privacy and civil liberties, and the Board's conclusions that reforms are needed.

After considering the 215 program, the Report addresses the operations of the Foreign Intelligence Surveillance Court. That section, Part 8, concludes by proposing an approach that, in appropriate cases, would allow the FISC judges to hear from a Special Advocate. Part 9, the final section of the Report, addresses the issue of transparency, which has been a priority of this Board since it began operations.¹⁷

¹⁷ See Privacy and Civil Liberties Oversight Board, Minutes of Open Meeting of March 5, 2013, at 6-7, available at <http://www.pclob.gov/>.

IV. What's Next?

While this Report includes a number of detailed conclusions and recommendations, it does not purport to answer all questions. The Board welcomes the opportunity for further dialogue within the executive branch and with Congress about the issues raised in this Report and how best to implement the Board's recommendations.

The Board's next report will consider the Section 702 program, addressing whether, in the Board's view, the program is consistent with statutory authority, complies with the Constitution, and strikes the appropriate balance between national security and privacy and civil liberties. That report will also be made available to the public.

Part 2:
EXECUTIVE SUMMARY

The statute creating the Privacy and Civil Liberties Oversight Board (“PCLOB” or “Board”) directs the Board to analyze and review actions taken by the executive branch to protect the nation from terrorism, “ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties.”¹⁸ In pursuit of this mission, the PCLOB has conducted an in-depth analysis of the bulk telephone records program operated by the National Security Agency (“NSA”) under Section 215 of the USA PATRIOT Act (“Patriot Act”). The Board’s examination has also included a review of the operation of the Foreign Intelligence Surveillance Court (“FISC” or “FISA court”). This Executive Summary outlines the Board’s conclusions and recommendations.

I. Overview of the Report

A. Background: Description and History of the Section 215 Program

The NSA’s telephone records program is operated under an order issued by the FISA court pursuant to Section 215 of the Patriot Act, an order that is renewed approximately every ninety days. The program is intended to enable the government to identify communications among known and unknown terrorism suspects, particularly those located inside the United States. When the NSA identifies communications that may be associated with terrorism, it issues intelligence reports to other federal agencies, such as the FBI, that work to prevent terrorist attacks. The FISC order authorizes the NSA to collect nearly all call detail records generated by certain telephone companies in the United States, and specifies detailed rules for the use and retention of these records. Call detail records typically include much of the information that appears on a customer’s telephone bill: the date and time of a call, its duration, and the participating telephone numbers. Such information is commonly referred to as a type of “metadata.” The records collected by the NSA under this program do not, however, include the content of any telephone conversation.

After collecting these telephone records, the NSA stores them in a centralized database. Initially, NSA analysts are permitted to access the Section 215 calling records only through “queries” of the database. A query is a search for a specific number or other selection term within the database. Before any specific number is used as the search target or “seed” for a query, one of twenty-two designated NSA officials must first determine that

¹⁸ 42 U.S.C. § 2000ee(c)(1).

there is a reasonable, articulable suspicion (“RAS”) that the number is associated with terrorism. Once the seed has been RAS-approved, NSA analysts may run queries that will return the calling records for that seed, and permit “contact chaining” to develop a fuller picture of the seed’s contacts. Contact chaining enables analysts to retrieve not only the numbers directly in contact with the seed number (the “first hop”), but also numbers in contact with all first hop numbers (the “second hop”), as well as all numbers in contact with all second hop numbers (the “third hop”).

The Section 215 telephone records program has its roots in counterterrorism efforts that originated in the immediate aftermath of the September 11 attacks. The NSA began collecting telephone metadata in bulk as one part of what became known as the President’s Surveillance Program. From late 2001 through early 2006, the NSA collected bulk telephony metadata based upon presidential authorizations issued every thirty to forty-five days. In May 2006, the FISC first granted an application by the government to conduct the telephone records program under Section 215.¹⁹ The government’s application relied heavily on the reasoning of a 2004 FISA court opinion and order approving the bulk collection of Internet metadata under a different provision of FISA.²⁰

On June 5, 2013, the British newspaper *The Guardian* published an article based on unauthorized disclosures of classified documents by Edward Snowden, a contractor for the NSA, which revealed the telephone records program to the public. On August 29, 2013, FISC Judge Claire Eagan issued an opinion explaining the court’s rationale for approving the Section 215 telephone records program.²¹ Although prior authorizations of the program had been accompanied by detailed orders outlining applicable rules and minimization procedures, this was the first judicial opinion explaining the FISA court’s legal reasoning in authorizing the bulk records collection. The Section 215 program was reauthorized most recently by the FISC on January 3, 2014.

Over the years, a series of compliance issues were brought to the attention of the FISA court by the government. However, none of these compliance issues involved significant intentional misuse of the system. Nor has the Board seen any evidence of bad faith or misconduct on the part of any government officials or agents involved with the program.²² Rather, the compliance issues were recognized by the FISC — and are

¹⁹ See Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 06-05 (FISA Ct. May 24, 2006).

²⁰ See Opinion and Order, No. PR/TT [redacted] (FISA Ct.).

²¹ See Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

²² Neither has the Board seen any evidence that would suggest any telephone providers did not rely in good faith on orders of the FISC when producing metadata to the government.

recognized by the Board — as a product of the program’s technological complexity and vast scope, illustrating the risks inherent in such a program.

B. Legal Analysis: Statutory and Constitutional Issues

Section 215 is designed to enable the FBI to acquire records that a business has in its possession, as part of an FBI investigation, when those records are relevant to the investigation. Yet the operation of the NSA’s bulk telephone records program bears almost no resemblance to that description. While the Board believes that this program has been conducted in good faith to vigorously pursue the government’s counterterrorism mission and appreciates the government’s efforts to bring the program under the oversight of the FISA court, the Board concludes that Section 215 does not provide an adequate legal basis to support the program.

There are four grounds upon which we find that the telephone records program fails to comply with Section 215. First, the telephone records acquired under the program have no connection to any specific FBI investigation at the time of their collection. Second, because the records are collected in bulk — potentially encompassing all telephone calling records across the nation — they cannot be regarded as “relevant” to any FBI investigation as required by the statute without redefining the word relevant in a manner that is circular, unlimited in scope, and out of step with the case law from analogous legal contexts involving the production of records. Third, the program operates by putting telephone companies under an obligation to furnish new calling records on a daily basis as they are generated (instead of turning over records already in their possession) — an approach lacking foundation in the statute and one that is inconsistent with FISA as a whole. Fourth, the statute permits only the FBI to obtain items for use in its investigations; it does not authorize the NSA to collect anything.

In addition, we conclude that the program violates the Electronic Communications Privacy Act. That statute prohibits telephone companies from sharing customer records with the government except in response to specific enumerated circumstances, which do not include Section 215 orders.

Finally, we do not agree that the program can be considered statutorily authorized because Congress twice delayed the expiration of Section 215 during the operation of the program without amending the statute. The “reenactment doctrine,” under which Congress is presumed to have adopted settled administrative or judicial interpretations of a statute, does not trump the plain meaning of a law, and cannot save an administrative or judicial interpretation that contradicts the statute itself. Moreover, the circumstances presented here differ in pivotal ways from any in which the reenactment doctrine has ever been applied, and applying the doctrine would undermine the public’s ability to know what the law is and hold their elected representatives accountable for their legislative choices.

The NSA's telephone records program also raises concerns under both the First and Fourth Amendments to the United States Constitution. We explore these concerns and explain that while government officials are entitled to rely on existing Supreme Court doctrine in formulating policy, the existing doctrine does not fully answer whether the Section 215 telephone records program is constitutionally sound. In particular, the scope and duration of the program are beyond anything ever before confronted by the courts, and as a result of technological developments, the government possesses capabilities to collect, store, and analyze data not available when existing Supreme Court doctrine was developed. Without seeking to predict the direction of changes in Supreme Court doctrine, the Board urges as a policy matter that the government consider how to preserve underlying constitutional guarantees in the face of modern communications technology and surveillance capabilities.

C. Policy Implications of the Section 215 Program

The threat of terrorism faced today by the United States is real. The Section 215 telephone records program was intended as one tool to combat this threat — a tool that would help investigators piece together the networks of terrorist groups and the patterns of their communications with a speed and comprehensiveness not otherwise available. However, we conclude that the Section 215 program has shown minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. Even in that case, the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program.

The Board's review suggests that where the telephone records collected by the NSA under its Section 215 program have provided value, they have done so primarily in two ways: by offering additional leads regarding the contacts of terrorism suspects already known to investigators, and by demonstrating that foreign terrorist plots do *not* have a U.S. nexus. The former can help investigators confirm suspicions about the target of an inquiry or about persons in contact with that target. The latter can help the intelligence community focus its limited investigatory resources by avoiding false leads and channeling efforts where they are needed most. But with respect to the former, our review suggests that the Section 215 program offers little unique value but largely duplicates the FBI's own information gathering efforts. And with respect to the latter, while the value of proper

resource allocation in time-sensitive situations is not to be discounted, we question whether the American public should accept the government's routine collection of all of its telephone records because it helps in cases where there is no threat to the United States.

The Board also has analyzed the Section 215 program's implications for privacy and civil liberties and has concluded that they are serious. Because telephone calling records can reveal intimate details about a person's life, particularly when aggregated with other information and subjected to sophisticated computer analysis, the government's collection of a person's entire telephone calling history has a significant and detrimental effect on individual privacy. The circumstances of a particular call can be highly suggestive of its content, such that the mere record of a call potentially offers a window into the caller's private affairs. Moreover, when the government collects *all* of a person's telephone records, storing them for five years in a government database that is subject to high-speed digital searching and analysis, the privacy implications go far beyond what can be revealed by the metadata of a single telephone call.

Beyond such individual privacy intrusions, permitting the government to routinely collect the calling records of the entire nation fundamentally shifts the balance of power between the state and its citizens. With its powers of compulsion and criminal prosecution, the government poses unique threats to privacy when it collects data on its own citizens. Government collection of personal information on such a massive scale also courts the ever-present danger of "mission creep." An even more compelling danger is that personal information collected by the government will be misused to harass, blackmail, or intimidate, or to single out for scrutiny particular individuals or groups. To be clear, the Board has seen no evidence suggesting that anything of the sort is occurring at the NSA and the agency's incidents of non-compliance with the rules approved by the FISC have generally involved unintentional misuse. Yet, while the danger of abuse may seem remote, given historical abuse of personal information by the government during the twentieth century, the risk is more than merely theoretical.

Moreover, the bulk collection of telephone records can be expected to have a chilling effect on the free exercise of speech and association, because individuals and groups engaged in sensitive or controversial work have less reason to trust in the confidentiality of their relationships as revealed by their calling patterns. Inability to expect privacy vis-à-vis the government in one's telephone communications means that people engaged in wholly lawful activities — but who for various reasons justifiably do not wish the government to know about their communications — must either forgo such activities, reduce their frequency, or take costly measures to hide them from government surveillance. The telephone records program thus hinders the ability of advocacy organizations to communicate confidentially with members, donors, legislators, whistleblowers, members of the public, and others. For similar reasons, awareness that a record of all telephone calls

is stored in a government database may have debilitating consequences for communication between journalists and sources.

To be sure, detailed rules currently in place limit the NSA's *use* of the telephone records it collects. These rules offer many valuable safeguards designed to curb the intrusiveness of the program. But in our view, they cannot fully ameliorate the implications for privacy, speech, and association that follow from the government's ongoing *collection* of virtually all telephone records of every American. Any governmental program that entails such costs requires a strong showing of efficacy. We do not believe the NSA's telephone records program conducted under Section 215 meets that standard.

D. Operation of the Foreign Intelligence Surveillance Court

Congress created the FISA court in 1978 in response to concerns about the abuse of electronic surveillance. This represented a major restructuring of the domestic conduct of foreign intelligence surveillance, with constitutional implications. Prior to then, successive Presidents had authorized national security wiretaps and other searches solely on the basis of their executive powers under Article II of the Constitution. The Foreign Intelligence Surveillance Act ("FISA") of 1978 provided a procedure under which the Attorney General could obtain a judicial warrant authorizing the use of electronic surveillance in the United States for foreign intelligence purposes.

Over time, the scope of FISA and the jurisdiction of the FISA court have evolved. Initially, the FISC's sole role was to approve individualized FISA warrants for electronic surveillance relating to a specific person, a specific place, or a specific communications account or device. Beginning in 2004, the role of the FISC changed when the government approached the court with its first request to approve a program involving what is now referred to as "bulk collection." In conducting this study, the Board was told by former FISA court judges that they were quite comfortable hearing only from government attorneys when evaluating individual surveillance requests but that the judges' decision making would be greatly enhanced if they could hear opposing views when ruling on requests to establish new surveillance programs.

Upon the FISC's receipt of a proposed application, a member of the court's legal staff will review the application and evaluate whether it meets the legal requirements under FISA. The FISC's legal staff are career employees who have developed substantial expertise in FISA, but they serve as staff to the judges rather than as advocates. While their role includes identifying any flaws in the government's statutory or constitutional analysis, it does not reach to contesting the government's arguments in the manner of an opposing party. The FISA court process for considering applications may include a hearing, and FISC judges have the authority to take testimony from government employees familiar with the technical details of an application. FISA does not provide a mechanism for the court to

invite non-governmental parties to provide views on pending government applications or otherwise participate in FISC proceedings prior to approval of an application.

FISA also established a Foreign Intelligence Court of Review (“FISCR”), comprised of three judges drawn from U.S. district courts or courts of appeals. Appeals to the FISCR have been rare: thus far there have been only two decisions issued by the court. Electronic communications service providers have some limited ability to appeal FISC orders, but FISA does not provide a way for the FISCR to receive the views of other non-governmental parties on appeals pending before it.²³

The FISC’s *ex parte*, classified proceedings have raised concerns that the court does not take adequate account of positions other than those of the government. It is critical to the integrity of the process that the public has confidence in its impartiality and rigor. Therefore, the Board believes that some reforms are appropriate and would help bolster public confidence in the operation of the court. The most important reforms proposed by the Board are: (1) creation of a panel of private attorneys, Special Advocates, who can be brought into cases involving novel and significant issues by FISA court judges; (2) development of a process facilitating appellate review of such decisions; and (3) providing increased opportunity for the FISC to receive technical assistance and legal input from outside parties.

E. Transparency Issues

In a representative democracy, the tension between openness and secrecy is inevitable and complex. The challenges are especially acute in the area of intelligence collection, where the powers exercised by the government implicate fundamental rights and our enemies are constantly trying to understand our capabilities in order to avoid detection. In this context, both openness and secrecy are vital to our survival, and we must strive to develop and implement intelligence programs in ways that serve both values.

Transparency is one of the foundations of democratic governance. Our constitutional system of government relies upon the participation of an informed electorate. This in turn requires public access to information about the activities of the government. Transparency supports accountability. It is especially important with regard to activities of the government that affect the rights of individuals, where it is closely interlinked with redress for violations of rights. In the intelligence context, although a certain amount of secrecy is necessary, transparency regarding collection authorities and

²³ However, the court has in one instance accepted amicus, or “friend of the court,” briefs on a significant legal question pending before it.

their exercise can increase public confidence in the intelligence process and in the monumental decisions that our leaders make based on intelligence products.

In the aftermath of the Snowden disclosures, the government has released a substantial amount of information on the leaked government surveillance programs. Although there remains a deep well of distrust, these official disclosures have helped foster greater public understanding of government surveillance programs. However, to date the official disclosures relate almost exclusively to specific programs that had already been the subject of leaks, and we must be careful in citing these disclosures as object lessons for what additional transparency might be appropriate in the future.

The Board believes that the government must take the initiative and formulate long-term solutions that promote greater transparency for government surveillance policies more generally, in order to inform public debate on technology, national security, and civil liberties going beyond the current controversy. In this effort, all three branches have a role. For the executive branch, disclosures about key national security programs that involve the collection, storage and dissemination of personal information — such as the operation of the National Counterterrorism Center — show that it is possible to describe practices and policies publicly, even those that have not been otherwise leaked, without damage to national security or operational effectiveness.

With regard to the legislative process, even where classified intelligence operations are involved, the purposes and framework of a program for domestic intelligence collection should be debated in public. During the process of developing legislation, some hearings and briefings may need to be conducted in secret to ensure that policymakers fully understand the intended use of a particular authority. But the government should not base an ongoing program affecting the rights of Americans on an interpretation of a statute that is not apparent from a natural reading of the text. In the case of Section 215, the government should have made it publicly clear in the reauthorization process that it intended for Section 215 to serve as legal authority to collect data in bulk on an ongoing basis.

There is also a need for greater transparency regarding operation of the FISA court. Prospectively, we encourage the FISC judges to continue the recent practice of writing opinions with an eye to declassification, separating specific sensitive facts peculiar to the case at hand from broader legal analyses. We also believe that there is significant value in producing declassified versions of earlier opinions, and recommend that the government undertake a classification review of all significant FISC opinions and orders involving novel interpretations of law. We realize that the process of redacting opinions not drafted for public disclosure will be more difficult and will burden individuals with other pressing duties, but we believe that it is appropriate to make the effort where those opinions and orders complete the historical picture of the development of legal doctrine regarding

matters within the jurisdiction of the FISA court. In addition, should the government adopt our recommendation for a Special Advocate in the FISC, the nature and extent of that advocate's role must be transparent to be effective.

It is also important to promote transparency through increased reporting to the public on the scope of surveillance programs. We urge the government to work with Internet service providers and other companies to reach agreement on standards allowing reasonable disclosures of aggregate statistics that would be meaningful without revealing sensitive government capabilities or tactics. We recommend that the government should also increase the level of detail in its unclassified reporting to Congress and the public regarding surveillance programs.

II. Overview of the PCLOB's Recommendations

A. Section 215 Program

Recommendation 1: *The government should end its Section 215 bulk telephone records program.*

The Section 215 bulk telephone records program lacks a viable legal foundation under Section 215, implicates constitutional concerns under the First and Fourth Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value. As a result, the Board recommends that the government end the program.

Without the current Section 215 program, the government would still be able to seek telephone calling records directly from communications providers through other existing legal authorities. The Board does not recommend that the government impose data retention requirements on providers in order to facilitate any system of seeking records directly from private databases.

Once the Section 215 bulk collection program has ended, the government should purge the database of telephone records that have been collected and stored during the program's operation, subject to limits on purging data that may arise under federal law or as a result of any pending litigation.

The Board also recommends against the enactment of legislation that would merely codify the existing program or any other program that collects bulk data on such a massive scale regarding individuals with no suspected ties to terrorism or criminal activity. Moreover, the Board's constitutional analysis should provide a message of caution, and as a policy matter, given the significant privacy and civil liberties interests at stake, if Congress

seeks to provide legal authority for any new program, it should seek the least intrusive alternative and should not legislate to the outer bounds of its authority.

The Board recognizes that the government may need a short period of time to explore and institutionalize alternative approaches, and believes it would be appropriate for the government to wind down the 215 program over a brief interim period. If the government does find the need for a short wind-down period, the Board urges that it should follow the procedures under Recommendation 2 below.

Recommendation 2: The government should immediately implement additional privacy safeguards in operating the Section 215 bulk collection program.

The Board recommends that the government immediately implement several additional privacy safeguards to mitigate the privacy impact of the present Section 215 program. The recommended changes can be implemented without any need for congressional or FISC authorization. Specifically, the government should:

- (a) reduce the retention period for the bulk telephone records program from five years to three years;
- (b) reduce the number of “hops” used in contact chaining from three to two;
- (c) submit the NSA’s “reasonable articulable suspicion” determinations to the FISC for review after they have been approved by NSA and used to query the database; and
- (d) require a “reasonable articulable suspicion” determination before analysts may submit queries to, or otherwise analyze, the “corporate store,” which contains the results of contact chaining queries to the full “collection store.”

B. FISA Court Operations

Recommendation 3: Congress should enact legislation enabling the FISC to hear independent views, in addition to the government’s views, on novel and significant applications and in other matters in which a FISC judge determines that consideration of the issues would merit such additional views.

Congress should authorize the establishment of a panel of outside lawyers to serve as Special Advocates before the FISC in appropriate cases. The Presiding Judge of the FISC should select attorneys drawn from the private sector to serve on the panel. The attorneys

should be capable of obtaining appropriate security clearances and would then be available to be called upon to participate in certain FISC proceedings.

The decision as to whether the Special Advocate would participate in any particular matter should be left to the discretion of the FISC. The Board expects that the court would invite the Special Advocate to participate in matters involving interpretation of the scope of surveillance authorities, other matters presenting novel legal or technical questions, or matters involving broad programs of collection. The role of the Special Advocate, when invited by the court to participate, would be to make legal arguments addressing privacy, civil rights, and civil liberties interests. The Special Advocate would review the government's application and exercise his or her judgment about whether the proposed surveillance or collection is consistent with law or unduly affects privacy and civil liberties interests.

Recommendation 4: *Congress should enact legislation to expand the opportunities for appellate review of FISC decisions by the FISCR and for review of FISCR decisions by the Supreme Court of the United States.*

Providing for greater appellate review of FISC and FISCR rulings will strengthen the integrity of judicial review under FISA. Providing a role for the Special Advocate in seeking that appellate review will further increase public confidence in the integrity of the process.

Recommendation 5: *The FISC should take full advantage of existing authorities to obtain technical assistance and expand opportunities for legal input from outside parties.*

FISC judges should take advantage of their ability to appoint Special Masters or other technical experts to assist them in reviewing voluminous or technical materials, either in connection with initial applications or in compliance reviews. In addition, the FISC and the FISCR should develop procedures to facilitate amicus participation by third parties in cases involving questions that are of broad public interest, where it is feasible to do so consistent with national security.

C. Promoting Transparency

Recommendation 6: *To the maximum extent consistent with national security, the government should create and release with minimal redactions declassified versions of new decisions, orders and opinions by the FISC and FISCR in cases involving novel interpretations of FISA or other significant questions of law, technology or compliance.*

FISC judges should continue their recent practice of drafting opinions in cases involving novel issues and other significant decisions in the expectation that declassified versions will be released to the public. The government should promptly create and release declassified versions of these FISC opinions.

Recommendation 7: Regarding previously written opinions, the government should perform a declassification review of decisions, orders and opinions by the FISC and FISCR that have not yet been released to the public and that involve novel interpretations of FISA or other significant questions of law, technology or compliance.

Although it may be more difficult to declassify older FISC opinions drafted without expectation of public release, the release of such older opinions is still important to facilitate public understanding of the development of the law under FISA. The government should create and release declassified versions of older opinions in novel or significant cases to the greatest extent possible consistent with protection of national security. This should cover programs that have been discontinued, where the legal interpretations justifying such programs have ongoing relevance.

Recommendation 8: The Attorney General should regularly and publicly report information regarding the operation of the Special Advocate program recommended by the Board. This should include statistics on the frequency and nature of Special Advocate participation in FISC and FISCR proceedings.

These reports should include statistics showing the number of cases in which a Special Advocate participated, as well as the number of cases identified by the government as raising a novel or significant issue, but in which the judge declined to invite Special Advocate participation. The reports should also indicate the extent to which FISC decisions have been subject to review in the FISCR and the frequency with which Special Advocate requests for FISCR review have been granted.

Recommendation 9: The government should work with Internet service providers and other companies that regularly receive FISA production orders to develop rules permitting the companies to voluntarily disclose certain statistical information. In addition, the government should publicly disclose more detailed statistics to provide a more complete picture of government surveillance operations.

The Board urges the government to pursue discussions with communications service providers to determine the maximum amount of information that companies could voluntarily publish to show the extent of government surveillance requests they receive per year in a way that is consistent with protection of national security. In addition, the

government should itself release annual reports showing in more detail the nature and scope of FISA surveillance for each year.

Recommendation 10: *The Attorney General should fully inform the PCLOB of the government's activities under FISA and provide the PCLOB with copies of the detailed reports submitted under FISA to the specified committees of Congress. This should include providing the PCLOB with copies of the FISC decisions required to be produced under Section 601(a)(5).*²⁴

Recommendation 11: *The Board urges the government to begin developing principles and criteria for transparency.*

The Board urges the Administration to commence the process of articulating principles and criteria for deciding what must be kept secret and what can be released as to existing and future programs that affect the American public.

Recommendation 12: *The scope of surveillance authorities affecting Americans should be public.*

In particular, the Administration should develop principles and criteria for the public articulation of the legal authorities under which it conducts surveillance affecting Americans. If the text of the statute itself is not sufficient to inform the public of the scope of asserted government authority, then the key elements of the legal opinion or other documents describing the government's legal analysis should be made public so there can be a free and open debate regarding the law's scope. This includes both original enactments such as 215's revisions and subsequent reauthorizations. While sensitive operational details regarding the conduct of government surveillance programs should remain classified, and while legal interpretations of the application of a statute in a particular case may also be secret so long as the use of that technique in a particular case is secret, the government's interpretations of statutes that provide the basis for ongoing surveillance programs affecting Americans can and should be made public.

²⁴ Section 601(a)(5), which is codified at 50 U.S.C. § 1871(a)(5), requires the congressional intelligence and judiciary committees to be provided with decisions, orders, and opinions from the FISC, and from its companion appellate court, that include significant construction or interpretation of FISA provisions.

Part 3:
DESCRIPTION OF THE NSA SECTION 215 PROGRAM

I. Telephone Calling Records

When a person completes a telephone call, telephone company equipment generates a record of certain details about that call. These “call detail records” typically include much of the information that appears on a customer’s telephone bill: the date and time of a call, its duration, and the participating telephone numbers. Such records also can include a range of technical information about how the call was routed from one participant to the other through the infrastructure of the telephone companies’ networks. Telephone companies create these records in order to bill customers for their calls, detect fraud, and for other business purposes.

While calling records provide information about particular telephone calls, they do not include the contents of any telephone conversations. Because these records provide information about a communication but not the communication itself, they often are referred to as a form of “metadata,” a word sometimes defined as “data about data.” Call detail records often are called “telephony metadata.”

After generating calling records in the normal course of business, telephone companies keep them on file for varying periods of time. Federal regulations presently require the companies to retain toll billing records for a minimum of eighteen months.²⁵

II. What the NSA Collects under Section 215 of the Patriot Act

The Foreign Intelligence Surveillance Act (“FISA”) includes a “business records” provision that allows the FBI to obtain books, records, papers, documents, and other items that may be relevant to a counterterrorism investigation. To obtain such records under this provision, the FBI must file an application with the Foreign Intelligence Surveillance Court (“FISC” or “FISA court”) requesting that the court issue an order directing a person or entity to turn over the items sought.²⁶ The business records provision of FISA was significantly expanded by Section 215 of the Patriot Act in 2001, and as a result it frequently is referred to as Section 215.²⁷ Under a program authorized by the FISA court pursuant to Section 215, the NSA is permitted to obtain all call detail records generated by

²⁵ See 47 C.F.R. § 42.6.

²⁶ See 50 U.S.C. § 1861(a)(1), (b)(2)(A). See also pages 40 to 42 of this Report for a more detailed discussion of FISA’s business records provision.

²⁷ See Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861).

certain telephone companies in the United States. The FISA court has determined that Section 215 provides a legal basis to order the telephone companies to facilitate this program by supplying the NSA with their calling records.²⁸

Under the FISA court's orders, certain telephone companies must provide the NSA with "all call detail records" generated by those companies.²⁹ Because the companies are directed to supply virtually all of their calling records to the NSA, the FISA court's orders result in the production of call detail records for a large volume of telephone communications; the NSA has described its program as enabling "comprehensive" analysis of telephone communications "that cross different providers and telecommunications networks."³⁰ The vast majority of the records obtained are for purely domestic calls, meaning those calls in which both participants are located within the United States, including local calls.

The calling records provided to the NSA do not identify which individual is associated with any particular telephone number: they do not include the name, address, or financial information of any telephone subscriber or customer. (Such information can be obtained by the government through other means, however, including reverse telephone directories and subpoenas issued to the telephone companies.) Nor do the records, as noted, include the spoken contents of any telephone conversation.³¹ In other words, the NSA is not able to listen to any telephone calls under the authority provided by these orders.

In addition, the calling records that the NSA collects under its Section 215 program do not currently include "cell site location information." That information, unique to mobile phones, is a component of a call detail record that shows which cell phone tower a mobile phone is connecting with. Thus it can be used to track the geographic location of a mobile phone user at that time the user places or receives a call. At the NSA's request, telephone companies remove that information from their calling records before transmitting the

²⁸ See Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013); Memorandum, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-158 (FISA Ct. Oct. 11, 2013). See pages 40 to 46 of this Report for a description of the FISA court's initial approval of the NSA's telephone records program under Section 215.

²⁹ Primary Order at 3, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-158 (FISA Ct. Oct. 11, 2013) ("Primary Order"). At least one telephone company presently is ordered to provide less than all of its call detail records. See *id.* at 3-4.

³⁰ See Declaration of Teresa H. Shea, Signals Intelligence Director, National Security Agency, ¶¶ 59-60, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Oct. 1, 2013) ("Shea Decl.").

³¹ See Primary Order at 3 n.1 (noting that "[t]elephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8)"). Section 2510(8) defines "content" as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

records to the NSA.³² In the past, the NSA has collected a limited amount of cell site location information to test the feasibility of incorporating such information into its Section 215 program, but that information has not been used for intelligence analysis, and the government has stated that the agency does not now collect it under this program.

Some information obtained by the NSA under Section 215 could nevertheless provide a general indication of a caller's geographic location. For instance, the area code and prefix of a landline telephone number can indicate the general area from which a call is sent. The same may be true of the "trunk identifier" associated with a telephone call, which pinpoints a segment of the communication line that connects two telephones during a conversation.³³

III. Delivery of Calling Records from Telephone Companies to the NSA

Approximately every ninety days, the government files an application with the FISA court requesting that the telephone companies be ordered to continue providing their calling records to the NSA for another ninety days. These applications are signed by officials from the FBI, as required by Section 215, but they typically note that the FBI is seeking the production of telephone records to the NSA. Accordingly, the FISA court's orders direct the telephone companies to "produce to NSA" their calling records.³⁴

When the FISA court approves the government's applications to renew the program, the court issues a "primary order" outlining the scope of what each telephone company must furnish to the NSA and the conditions under which the government can use, retain, and disseminate the data. At the same time, the court issues individual "secondary orders" separately addressed to each telephone company, directing it to comply with those terms and produce its records to the NSA.³⁵ After receiving a secondary order, a telephone company must continue the production of its records "on an ongoing daily basis" for the

³² Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, at 4 n.5, No. BR 13-109 (FISA Ct. Aug. 29, 2013); *see also* Declaration of Acting Assistant Director Robert J. Holley, Federal Bureau of Investigation, ¶ 5, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Oct. 1, 2013) ("Holley Decl.") (stating that metadata obtained under the orders does not include cell site location information). Agency personnel check this portion of incoming records to ensure that cell site location information has been removed.

³³ *See* Primary Order at 3 n.1 (noting that for purposes of the order, "telephony metadata" includes the "trunk identifier" for a call).

³⁴ Primary Order at 3.

³⁵ *See, e.g.*, Secondary Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-80 (FISA Ct. Apr. 25, 2013) ("Secondary Order").

ninety-day duration of the order.³⁶ The company may not disclose to anyone that it has received such an order.³⁷

Each telephone company must furnish the NSA with “an electronic copy” of its calling records.³⁸ Companies transmit those records to the NSA, which stores them “in repositories within secure networks.”³⁹

Telephone companies must provide their calling records to the NSA on a daily basis until the expiration date of each FISA court order. In other words, when the companies are served with an order from the FISC, they do not hand over to the NSA the calling records they have in their possession at that time. Instead, over the next ninety days, they must provide the NSA with the new calling records that they generate each day.

IV. How the NSA Stores and Handles the Telephone Records

When the records of particular telephone calls reach the NSA, the agency stores and processes those records in repositories within secure networks under its control.⁴⁰ Upon the arrival of new records at the NSA, agency technical personnel perform a number of steps to ensure that the records, which come from different telephone companies, are in a standard format compatible with the NSA’s databases. The agency is permitted to duplicate the data it receives for storage in recovery back-up systems.⁴¹

³⁶ Primary Order at 3-4; *id.* at 17 (indicating duration of the order).

³⁷ Every “secondary order” delivered to the telephone companies directing them to provide calling records to the NSA prohibits the companies from publicly disclosing the existence of the order and tightly limits the persons with whom that information may be shared. Specifically, the secondary orders direct that, with three exceptions, “no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order.” Secondary Order at 2. The personnel who receive a secondary order on behalf of the telephone companies are permitted to disclose its existence only to (1) “those persons to whom disclosure is necessary to comply with such Order,” (2) “an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order,” and (3) “other persons as permitted by the Director of the FBI or the Director’s designee.” *Id.* Any person to whom disclosure is made under one of these exceptions must be informed of the limitations set forth above. *Id.* at 3. Furthermore, any person who makes or intends to make a disclosure under the first or third exception above (*i.e.*, a disclosure to anyone except to an attorney for legal assistance) must, at the request of the FBI director or his designee, “identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.” *Id.* at 3.

³⁸ Primary Order at 3-4.

³⁹ Primary Order at 4.

⁴⁰ Primary Order at 4.

⁴¹ *See* Primary Order at 4-5 n.2. Should it ever be necessary to recover data that is stored in these back-up systems, “in the event of any natural disaster, man-made emergency, attack, or other unforeseen event,” the FISA court’s orders appear to require that any access or use of the back-up data be conducted in compliance with the same rules that ordinarily govern utilization of the records. *Id.*

Once the calling records are properly formatted, NSA houses them within its data repositories. At this point, technical personnel may take additional measures to make the calling records usable for intelligence analysis, including removing “high volume” telephone identifiers and other unwanted data.⁴²

The NSA is required to limit who has access to the calling records it obtains. The agency must restrict access to authorized personnel who have received training on the use of those records.⁴³ Such personnel can include both NSA employees and other individuals who are working under the NSA Director’s control on Signals Intelligence.⁴⁴ The calling records are routed to dedicated portions of NSA’s systems and are required to carry unique data markings enabling software and other controls to restrict access to the authorized personnel who have received the proper training and guidance.⁴⁵ Training is required both for intelligence analysts and for the technical personnel who access the data to make it usable for analysis.⁴⁶

Calling records must be deleted from the NSA’s repositories no later than five years after the agency receives them.⁴⁷ If a calling record shows up in a “query” performed by an analyst, however — a process described below — the information about that call need not be destroyed after five years.

V. How the NSA Analyzes the Telephone Records

The NSA uses the calling records it obtains under Section 215 to attempt to identify communications among known and unknown terrorism suspects, particularly those located inside the United States.⁴⁸ When the NSA identifies communications or telephone numbers of interest, it issues intelligence reports to other federal agencies, such as the FBI,

⁴² Primary Order at 6.

⁴³ Primary Order at 5.

⁴⁴ See Primary Order at 6 n.5 (requiring that all personnel engaged in signals intelligence operations be “under the direction, authority, or control” of the director of the NSA).

⁴⁵ Primary Order at 4-5.

⁴⁶ Primary Order at 5. The training requirements do not, however, extend to all technical personnel who might have access to the records, including those responsible for “NSA’s underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA.” *Id.* at 5 n.3.

⁴⁷ Primary Order at 14.

⁴⁸ See Shea Decl. ¶ 8 (stating that “by analyzing telephony metadata based on telephone numbers associated with terrorist activities, trained expert intelligence analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the U.S.”). The records of domestic and international calls — where one or both participants are inside the United States — are viewed as the most “analytically significant” by the agency, which sees them as “particularly likely” to identify suspects in the United States who are planning domestic attacks. Shea Decl. ¶ 9.

that work to prevent terrorist attacks. In carrying out this endeavor, the NSA is required by the FISA court to adhere to certain “minimization” requirements, described below, that govern the manner in which the calling records may be used within the agency and disseminated outside of it.⁴⁹

The NSA is prohibited from using the calling records it obtains under the FISA court’s orders except as specified in those orders.⁵⁰ The vast majority of the records the NSA collects are never seen by any person.⁵¹

The rules governing the NSA’s access to the calling records under the FISA court’s orders are set forth below.

A. Contact Chaining and the Query Process

Analysis of calling records under this program begins with telephone numbers that already are suspected of being associated with terrorism. The NSA then searches for other telephone numbers that have been in contact with a suspected number, or in contact with those who have been in contact with a suspected number.⁵²

Initially, NSA analysts are permitted to access the Section 215 calling records only through “queries” of the database. A query is a software-enabled search for a specific number or other selection term within the database.⁵³ When an analyst performs a query of a telephone number, for instance, the software interfaces with the database and provides results to the analyst that include a record of calls in which that number participated.

Analysts perform these queries to facilitate what is called “contact chaining” — the process of identifying the connections among individuals through their calls with each other.⁵⁴ The goals of contact chaining are to identify unknown terrorist operatives through

⁴⁹ See Primary Order at 4.

⁵⁰ See Primary Order at 4.

⁵¹ Shea Decl. ¶ 23.

⁵² Calling records may be searched or identified using numbers other than a “telephone number” as that term is normally used — *i.e.*, a number associated with a specific telephone that another caller can dial in order to reach that phone. The records may also include other unique numbers that are associated with a particular telephone user or a particular communications device. Among these are a telephone calling card number, which is used to pay for individual telephone calls, and an International Mobile station Equipment Identity (“IMEI”) number, which is uniquely associated with a particular mobile telephone. See Primary Order at 3 n.1 (explaining that telephony metadata includes IMEI numbers, IMSI numbers, and calling card numbers).

⁵³ Analysts can search the database using numbers, words, or symbols that uniquely identify a particular caller or device, like a telephone number or a calling card number. These types of selection terms are referred to as “identifiers.” But analysts also can search for selection terms that are not uniquely associated with any particular caller or device.

⁵⁴ Primary Order at 6.

their contacts with known suspects, discover links between known suspects, and monitor the pattern of communications among suspects.⁵⁵ Presently, the only purpose for which NSA analysts are permitted to search the Section 215 calling records housed in the agency's database is to conduct queries as described above, which are designed to build contact chains leading outward from a target to other telephone numbers.⁵⁶ The NSA has stated that it does not conduct pattern-based searches. Instead, every search begins with a specific telephone number or other specific selection term.⁵⁷

B. Standards for Approving Queries

A telephone number (or other selection term) used to search the calling records is referred to as a "seed."⁵⁸ Before analysts can search the records with that seed, one of twenty-two designated NSA officials must give approval.⁵⁹ Such approval can be granted only if the official determines that there is reasonable, articulable suspicion that the selection term is associated with terrorism: in the words of the FISA court orders, a term can be approved for use as a seed only after the designated official has determined that, "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 number "is associated with" a terrorist organization identified in the FISA court's orders.⁶⁰

The requirement that analysts have "reasonable articulable suspicion" before searching the database with a particular number is often referred to as the "RAS" standard. It is designed in part "to prevent any general browsing of data."⁶¹ Government lawyers have characterized this standard as "the cornerstone minimization procedure" that "ensures the overall reasonableness" of the program.⁶²

⁵⁵ See Shea Decl. ¶ 8.

⁵⁶ Primary Order at 6.

⁵⁷ As described below, however, different standards govern how NSA analysts may access and analyze the *results* of these searches.

⁵⁸ Primary Order at 6.

⁵⁹ Primary Order at 7.

⁶⁰ Primary Order at 7. NSA analysts may also perform queries of the calling records using numbers that are, at the time, the subject of electronic surveillance authorized by the FISA court, based on the court's finding of probable cause to believe that the number is used by an agent of a specified terrorist organization. Primary Order at 9. Analysts may query only those numbers that have received an individual probable cause determination by the FISA court, not numbers that are being monitored with FISA court approval pursuant to the broader authorities conferred by Sections 702, 703, or 704 of the FISA Amendments Act. *Id.* at 9-10.

⁶¹ Shea Decl. ¶ 20.

⁶² Report of the United States at 23, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 09-09 (FISA Ct. Aug. 17, 2009).

The FISA court orders approving the Section 215 program do not explain what it means for a selection term, like a telephone number, to be “associated with” a designated terrorist organization. The NSA has developed internal criteria to implement this standard, however. To take a simple example illustrating one of these criteria, intelligence reports might indicate that a particular person has communicated by email with a known terrorism suspect in furtherance of terrorist activity. Other intelligence reports might provide a telephone number believed to be used by that person. Together, these pieces of information would provide reasonable articulable suspicion that the telephone number is associated with terrorism.

If a telephone number or other selection term is “reasonably believed” to be used by a U.S. person, the FISA court’s orders specify that it may not be regarded as associated with a terrorist organization solely “on the basis of activities that are protected by the First Amendment to the Constitution.”⁶³ In implementing this requirement, the NSA presumes that, absent information to the contrary, any U.S. telephone number is used by a U.S. person. Because this restriction prohibits the NSA only from using First Amendment-protected activity as the *sole* basis for regarding a number as associated with terrorism, the agency may consider activities such as participating a public rally, attending a particular place of worship, expressing political views on the Internet, or buying a particular book — as long as those activities are not the *exclusive* basis for the agency’s assessment.

The information on which the NSA’s RAS determinations are based comes from several sources, including other federal agencies. In some instances, other agencies specifically request that the NSA conduct analysis of particular telephone numbers.⁶⁴

After a selection term has been approved for use as a “seed” — based on a determination that it is reasonably suspected of being associated with a specified terrorist organization — that approval is effective for one year, meaning that repeated queries using that seed can be made for the next year. Approval lasts only six months, however, if the term is reasonably believed to be used by a U.S. person.⁶⁵

C. How Queries Are Conducted and What They Produce

There are two methods through which the NSA is permitted to “query” the Section 215 calling records for analytic purposes with approved selection terms.

The first method is a manual process performed by individual analysts. In a “manual analyst query,” an individual analyst working at a computer terminal personally enters an approved seed term into the agency’s database software. The software searches the

⁶³ Primary Order at 9.

⁶⁴ See, e.g., Holley Decl. ¶ 16 (referring to information requests by the FBI).

⁶⁵ Primary Order at 10.

records obtained by the agency under Section 215 and returns those records that are within one “hop” of the seed (*i.e.*, all of the telephone numbers directly in contact with the seed). The analyst may then review the telephone numbers found to be in contact with a first-hop number (*i.e.*, within two hops of the seed) and the telephone numbers found to be in contact with a second-hop number (*i.e.*, within three hops of the seed).⁶⁶

If analysts try to look beyond the third hop of a query, or to perform a query of a selection term that has not been RAS approved, the NSA’s software is designed to prevent the action from being completed.⁶⁷

The results gathered by the NSA’s software show the web of telephone connections emanating outward from the seed, up to three links away from it. For every connection that is represented in these links, the software provides the associated information about the telephone calls involved, such as their date, time of day, and duration.

An analyst’s query, therefore, provides access to more than the calling records of a seed number that is reasonably suspected being associated with terrorism. The query also gives the analyst access to the complete calling records of every number that has been in direct contact with the seed number. It further gives the analyst access to the complete calling records of every number that has been in contact with one of those numbers. To put it another way, an analyst who performs a query of a suspected number is able to view the records of calls involving telephone numbers that had contact with a telephone number that had contact with another telephone number that had contact with the original target.

If a seed number has seventy-five direct contacts, for instance, and each of these first-hop contact has seventy-five new contacts of its own, then each query would provide the government with the complete calling records of 5,625 telephone numbers. And if each of those second-hop numbers has seventy-five new contacts of its own, a single query would result in a batch of calling records involving over 420,000 telephone numbers.

Calling records that fall within the results of a query are not deleted after five years. The results can be stored by the analyst who performed the query and may then be analyzed for intelligence purposes and shared with others, inside and outside the NSA, under rules described below. The results may be searched using terms that are not RAS-approved, subjected to other analytic methods or techniques besides querying, or integrated with records obtained by the NSA under other authorities.

⁶⁶ See Shea Decl. ¶ 22.

⁶⁷ The NSA is directed by the FISA court to “ensure, through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved.” Primary Order at 6-7. NSA’s technical controls are designed to preclude any query for intelligence analysis purposes using a seed that lacks RAS approval.

In 2012, the FISA court approved a new and automated method of performing queries, one that is associated with a new infrastructure implemented by the NSA to process its calling records.⁶⁸ The essence of this new process is that, instead of waiting for individual analysts to perform manual queries of particular selection terms that have been RAS approved, the NSA's database periodically performs queries on all RAS-approved seed terms, up to three hops away from the approved seeds. The database places the results of these queries together in a repository called the "corporate store."

The ultimate result of the automated query process is a repository, the corporate store, containing the records of all telephone calls that are within three "hops" of every currently approved selection term.⁶⁹ Authorized analysts looking to conduct intelligence analysis may then use the records in the corporate store, instead of searching the full repository of records.⁷⁰

According to the FISA court's orders, records that have been moved into the corporate store may be searched by authorized personnel "for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms."⁷¹ Analysts therefore can query the records in the corporate store with terms that are not reasonably suspected of association with terrorism. They also are permitted to analyze records in the corporate store through means other than individual contact-chaining queries that begin with a single selection term: because the records in the corporate store all stem from RAS-approved queries, the agency is allowed to apply other analytic methods and techniques to the query results.⁷² For instance, such calling records may be integrated with data acquired under other authorities for further analysis. The FISA court's orders expressly state that the NSA may apply "the full range" of signals intelligence analytic tradecraft to the calling records that are responsive to a query, which includes every record in the corporate store.⁷³

If the NSA queries around 300 seed numbers a year, as it did in 2012, then based on the estimates provided earlier about the number of records produced in response to a

⁶⁸ This "automated query process" was first approved for use by the FISA court in late 2012. Primary Order at 11 n.11.

⁶⁹ See Primary Order at 11.

⁷⁰ Under the manual query process, by contrast, analysts access the main collection repository, which contains all telephone records obtained under Section 215, but software controls are designed to prevent analysts from viewing records not linked to an RAS-approved number.

⁷¹ Primary Order at 11.

⁷² See Primary Order at 13 n.15.

⁷³ Primary Order at 13 n.15.

single query, the corporate store would contain records involving over 120 million telephone numbers.⁷⁴

The FISA court's orders call for audit capability with respect to all queries of the call detail records.⁷⁵ This requirement of an auditable record does not apply, however, "to the results of RAS-approved queries."⁷⁶ Therefore, when analysts access records that have turned up within three hops of a selection term — whether through a manual analyst query or by searching the corporate store — the court's orders do not impose a requirement that their actions be recorded or subject to audit, though other rules governing the NSA may impose this requirement.

VI. What the NSA Does with Information Obtained from the Telephone Records

By analyzing telephone calling records obtained under Section 215, the NSA seeks to identify counterterrorism information that is of investigative value to other intelligence and law enforcement agencies such as the FBI.⁷⁷ Such information could indicate that there have been communications between known or suspected terrorist operatives overseas and persons within the United States, or among suspects within the United States, which could assist in detecting people in the United States who may be acting in furtherance of a foreign terrorist organization.⁷⁸

Information obtained by NSA analysts through querying the calling records — the telephone connections, the associated details of each telephone call identified, and other intelligence gleaned derived from these sources — may be shared for intelligence purposes among NSA analysts who have received "appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information," according to the FISA court.⁷⁹

Once the NSA has identified information believed to have potential counterterrorism value, it passes that information on to other federal agencies, including the FBI. Before the NSA may share information it obtains from the calling records outside

⁷⁴ While fewer than 300 identifiers were used to query the call detail records in 2012, that number "has varied over the years." Shea Decl. ¶ 24.

⁷⁵ See Primary Order at 7 ("Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.").

⁷⁶ Primary Order at 7 n.6.

⁷⁷ Shea Decl. ¶ 26.

⁷⁸ Shea Decl. ¶¶ 16, 28.

⁷⁹ Primary Order at 12-13.

the agency, it must apply to that information the minimization procedures of Section 7 of United States Signals Intelligence Directive SP0018 (“USSID 18”), which prescribes rules for the dissemination of information about U.S. persons in order to ensure that the NSA’s activities are conducted consistent with law and the Fourth Amendment to the Constitution.⁸⁰

Additionally, before the NSA may disseminate any “U.S. person information” outside the agency, one of five designated high-level NSA officials must determine that the information “is in fact related to counterterrorism information” and that it “is necessary to understand the counterterrorism information or assess its importance.”⁸¹

The FBI can use the information it receives from the NSA to guide its investigations into terrorist operatives and threats inside the United States. When the FBI receives information that was obtained through Section 215, the Bureau is ordered by the FISA court to follow the minimization procedures set forth in the *Attorney General’s Guidelines for Domestic FBI Operations* (Sept. 29, 2008).⁸²

Other federal agencies also receive information from the NSA that was obtained through Section 215, but the FISA court’s orders do not establish rules for how those agencies must handle the information they receive.⁸³ In addition, the government has informed the FISA court that it may provide telephone numbers derived from the program to “appropriate . . . foreign government agencies.”⁸⁴

The NSA tracks the number of reports it provides to other agencies and the number of telephone numbers identified as investigative leads in those reports. During the first three years in which the telephone records program was authorized by the FISA court (between May 2006 and May 2009), the NSA “provided to the FBI and/or other intelligence

⁸⁰ Primary Order at 13; see United States Signals Intelligence Directive SP0018 (Jan. 25, 2011), available at <http://icontherecord.tumblr.com/>.

⁸¹ Primary Order at 13. The agency also may share such information with “Executive Branch personnel” for specific oversight purposes, namely in order to (1) permit those personnel “to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings,” or (2) permit those personnel “to facilitate their lawful oversight functions.” *Id.* at 13-14.

⁸² See Primary Order at 4.

⁸³ See Primary Order; see also Shea Decl. ¶ 26 (reporting that the agency analyzes the call detail records to find information that would be of investigative value to the FBI “or other intelligence agencies”). The text of Section 215 appears to require that all federal officers and employees who receive information acquired from the calling records adhere to the Attorney General’s guidelines, see 50 U.S.C. § 1861(h), but such a requirement is not explicit in the FISA court’s orders.

⁸⁴ See Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism, at 15, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 06-05 (FISA Ct. May 23, 2006).

agencies a total of 277 reports containing approximately 2,900 telephone identifiers that the NSA had identified.”⁸⁵

VII. Internal Oversight and Reporting to the FISA Court

Monitoring of the NSA’s compliance with the FISA court’s orders is undertaken by the NSA and the National Security Division of the Department of Justice, which periodically must report certain information to the court. The details of these oversight requirements are set forth below.

First, the NSA must enforce rules on which of its personnel have access to the calling records and information extracted from the calling records. Both groups of personnel must receive training tailored to their respective privileges. Specifically, the NSA’s Office of General Counsel and its Office of the Director of Compliance are ordered to “ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata.”⁸⁶ Those two offices “shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.”⁸⁷ The NSA is directed to maintain records of all such training and to provide the Justice Department (“DOJ”) with copies of “all formal briefing and/or training materials” used to “brief/train NSA personnel.”⁸⁸

Second, the NSA must take certain steps to ensure the effectiveness of the measures it has put in place to limit access to the calling records. Specifically, the agency’s Office of the Director of Compliance is tasked with monitoring the software and other technical controls that restrict the work of NSA personnel, as well as the agency’s logging, for auditing purposes, of instances in which personnel access the records.⁸⁹

Third, the NSA must cooperate with the DOJ regarding how it interprets and implements the FISA court’s orders authorizing the program. Specifically, the NSA’s Office

⁸⁵ Shea Decl. ¶ 26.

⁸⁶ Primary Order at 14. The government uses the term “BR metadata” to refer to the business records metadata acquired under the Section 215 program.

⁸⁷ Primary Order at 14.

⁸⁸ Primary Order at 14-15. The FISA court’s orders do not specify what this training must consist of, stating instead that “[t]he nature of the training that is appropriate and adequate for a particular person will depend on the person’s responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.” *Id.* at 14 n.17.

⁸⁹ Primary Order at 15.

of General Counsel is to consult with the Department of Justice on “all significant legal opinions that relate to the interpretation, scope, and/or implementation” of the program.⁹⁰ At least once during every ninety-day authorization period, NSA and DOJ representatives are required to meet “for the purpose of assessing compliance” with the FISA court’s orders, including “a review of NSA’s monitoring and assessment to ensure that only approved metadata is being acquired.” The results of this meeting must be put in writing and submitted to the FISA court as part of any request to renew or reinstate authority for the program.⁹¹ During every authorization period, DOJ personnel also must meet with the inspector general of the NSA “to discuss their respective oversight responsibilities and assess NSA’s compliance with the Court’s orders.”⁹² And at least once during each authorization period, officials from the DOJ and the NSA’s Office of General Counsel must review a sample of the justifications that were used by the NSA to approve the querying of particular telephone numbers within the database of calling records.⁹³

Fourth, during each ninety-day period for which the program is authorized by the FISA court, the government must file monthly reports with the court on its execution of the program. Approximately every thirty days, the NSA must submit a report that “includes a discussion” of the agency’s application of the RAS standard and its implementation of the new automated query process.⁹⁴ Each report also must state the number of instances since the last report “in which NSA has shared, in any form, results from queries of the BR metadata that contain U.S. person information, in any form, with anyone outside NSA.”⁹⁵ For every instance in which information about a U.S. person was shared in this manner, the report must include an attestation that one of the officials authorized to approve such disseminations determined, in advance, “that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.”⁹⁶ In practice, these monthly reports typically provide (1) a short description of some of the considerations that go into the agency’s RAS determinations, (2) the number of selection terms currently approved for querying the database, (3) a paragraph describing a single example of an RAS determination made during the previous month, and (4) a list of the instances during the prior month in which information extracted from the calling records was shared with other agencies (including

⁹⁰ Primary Order at 15.

⁹¹ Primary Order at 15.

⁹² Primary Order at 15.

⁹³ Primary Order at 16.

⁹⁴ Primary Order at 16.

⁹⁵ Primary Order at 16.

⁹⁶ Primary Order at 16-17.

the date and recipients of the dissemination and the required attestation about the need to share such information). NSA officials sign the reports under penalty of perjury.⁹⁷

The NSA has implemented an extensive array of internal procedures designed to ensure that its actions comply with the rules described above.

VIII. Congressional Reporting Requirements

In addition to the reporting obligations contained in the FISA court's orders, which require that designated information periodically be supplied to the court, the FISA statute requires the executive branch to report particular matters to the intelligence and judiciary committees in Congress. Certain developments in the NSA's Section 215 program, including changes proposed by the government or approved by the FISA court, would trigger these reporting requirements.

The executive branch must provide four congressional committees with significant orders and opinions of the FISA court and information about the ramifications of the FISA court's orders. Specifically, twice a year, the Attorney General is required to submit to the House and Senate intelligence and judiciary committees "a summary of significant legal interpretations" of FISA involving matters before the FISA court or its companion appellate court, the Foreign Intelligence Surveillance Court of Review, "including interpretations presented in applications or pleadings" filed with those courts.⁹⁸ This summary must be accompanied by "copies of all decisions, orders, or opinions" of the two courts "that include significant construction or interpretation" of the provisions of FISA.⁹⁹ For the preceding six-month period, the Attorney General's report also must set forth the aggregate number of persons targeted for orders issued under FISA, including a breakdown of those targeted for access to records under Section 215.¹⁰⁰

In addition, on an annual basis the Attorney General must "inform" the House and Senate intelligence committees and the Senate Judiciary Committee "concerning all requests" for the production of items under Section 215.¹⁰¹ The Attorney General must submit a report to the intelligence and judiciary committees setting forth, with respect to

⁹⁷ If the government seeks to renew its authority to collect calling records at the end of a ninety-day authorization period, it must include in its most recent thirty-day report "a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata." Primary Order at 16.

⁹⁸ 50 U.S.C. § 1871(a)(4).

⁹⁹ 50 U.S.C. § 1871(a)(5).

¹⁰⁰ 50 U.S.C. § 1871(a)(1)(D).

¹⁰¹ 50 U.S.C. § 1862(a).

the previous calendar year, statistical information about the applications filed with the FISA court under Section 215 and the orders issued by the court granting, modifying, or denying such applications.¹⁰² An unclassified report must also be provided to Congress containing a subset of this statistical information.¹⁰³

¹⁰² 50 U.S.C. § 1862(b).

¹⁰³ 50 U.S.C. § 1862(c).

Part 4:
HISTORY OF THE NSA SECTION 215 PROGRAM

I. The NSA's Initiation of Bulk Telephone Records Collection Under the President's Surveillance Program

The telephone records program that the NSA operates today under Section 215 of the Patriot Act evolved out of counterterrorism efforts that began shortly after the attacks of September 11, 2001. In October 2001, President George W. Bush issued a highly classified presidential authorization directing the NSA to collect certain foreign intelligence by electronic surveillance in order to prevent acts of terrorism within the United States, based upon a finding that an extraordinary emergency existed because of the September 11 attacks. Under this authorization, electronic surveillance was permitted within the United States for counterterrorism purposes without judicial warrants or court orders for a limited number of days.¹⁰⁴ President Bush authorized the NSA to: (1) collect the contents of certain international communications, a program that was later referred to as the Terrorist Surveillance Program ("TSP"), and (2) collect in bulk non-content information, or "metadata," about telephone and Internet communications.¹⁰⁵

The President renewed the authorization for the NSA's activities in early November 2001. Thereafter, the authorization was renewed continuously, with some modifications in the scope of the authorized collection, approximately every thirty to sixty days until 2007. Each presidential authorization included the finding that an extraordinary emergency continued to exist justifying ongoing warrantless surveillance. Key members of Congress and the presiding judge of the Foreign Intelligence Surveillance Court were briefed on the existence of the program. The collection of communications content and bulk metadata under these presidential authorizations became known as the President's Surveillance Program. According to a 2009 report by the inspectors general of several defense and intelligence agencies, over time, "the program became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool."¹⁰⁶

¹⁰⁴ See DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013), <http://icontherecord.tumblr.com/>.

¹⁰⁵ See *id.* With respect to telephone communications, metadata includes information about the participating telephone numbers and the date, time, and duration of a call. With respect to Internet communications, metadata includes, among other things, addressing information that helps route a message to the proper destination, such as the "to" and "from" lines attached to an email.

¹⁰⁶ See Unclassified Report on the President's Surveillance Program, prepared by the Office of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence, at 31 (July 10, 2009) ("OIGs Rpt.").

II. Reassessment of Legal Basis for President’s Surveillance Program

In 2003, the Office of Legal Counsel in the Department of Justice (“OLC”) began a comprehensive reassessment of the legal basis for the President’s Surveillance Program. The OLC conducted a new legal analysis that supported much of the program authorized by the President, but it became concerned that this revised analysis would not be sufficient to support the legality of certain aspects of the program.¹⁰⁷ After extensive debate within the Administration, in March 2004 the President decided to modify certain intelligence-gathering activities under the program, discontinuing the bulk collection of Internet metadata.¹⁰⁸

III. Transition of Internet Metadata Collection to FISA Court Authority

The Foreign Intelligence Surveillance Act of 1978 (“FISA”) created, for the first time, a legislative structure governing executive branch efforts to conduct surveillance within the United States to obtain foreign intelligence. The Act established a special court, comprised of sitting federal judges, to review and grant or deny applications made by the executive branch to conduct electronic surveillance for foreign intelligence purposes — the Foreign Intelligence Surveillance Court (“FISC” or “FISA court”).¹⁰⁹

One of FISA’s provisions allows the government to seek permission from the FISA court to monitor communications by installing a “pen register” or “trap and trace device” to capture information sent from a communications instrument or facility.¹¹⁰ A pen register records the “dialing, routing, addressing, or signaling information” transmitted through wire or electronic communication, but does not capture the contents of communications.¹¹¹ Early versions of pen registers simply recorded the numbers dialed from a telephone, but later developments allowed the devices to capture information such as the “to” line in an email. A “trap and trace device” records information about *incoming* telephone calls or other electronic communications.¹¹² Sometimes combined in a single instrument, pen registers and trap and trace devices are often referred to as pen/trap or PR/TT devices.

¹⁰⁷ OIGs Rpt. at 20.

¹⁰⁸ See OIGs Rpt. at 29; DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013), <http://icontherecord.tumblr.com/>.

¹⁰⁹ See Part 8 of this Report for a discussion of the FISA court and its operations.

¹¹⁰ See 50 U.S.C. § 1842.

¹¹¹ 18 U.S.C. § 3127(3).

¹¹² 18 U.S.C. § 3127(4).

In 2004, the Administration sought FISA court approval for NSA to collect large amounts of Internet metadata in bulk under FISA's pen/trap provisions. Judge Kollar-Kotelly granted the government's application in July 2004.¹¹³ Her order approved the government's request while requiring the government to comply with certain additional restrictions and procedures.¹¹⁴ As proposed by the government, Judge Kollar-Kotelly's order permitted Internet metadata to be acquired only if it travelled through certain designated communications channels that were relatively likely to contain messages of counterterrorism interest, "in order to build a meta data archive that will be, in relative terms, richly populated" with terrorism-related communications.¹¹⁵

Once in the possession of the NSA, the Internet metadata collected under the FISA court's order could be accessed by NSA personnel only through queries targeting particular Internet accounts or addresses, and only after the NSA concluded there was a "reasonable articulable suspicion" that the account or address was "associated with" a target.¹¹⁶ The NSA was permitted to employ only the specific analytical methods described in the court's opinion. Under these rules, it could engage in "contact chaining" to identify Internet users directly in contact with a target account or address, or directly in contact with a user who was directly in contact with the target. In other words, the agency could search for Internet users who were up to two steps removed from a target.¹¹⁷

Judge Kollar-Kotelly issued a lengthy opinion with her order approving the Internet metadata program, discussing the statutory and constitutional issues raised by the government's request and the "exceptionally broad form of collection" it entailed.¹¹⁸ The opinion concluded that the Internet metadata to be obtained by the government was "relevant to an ongoing investigation," as required by the statute, "even though only a very small percentage of the information obtained" would be "directly relevant to such an investigation." This was so, the opinion said, because large-scale collection was "necessary to identify the much smaller number" of terrorism-related communications.¹¹⁹ Emphasizing that "senior responsible officials, whose judgment on these matters is entitled to deference, have . . . also explained why they seek to collect the particular meta data . . .

¹¹³ See Opinion and Order, No. PR/TT [redacted] (FISA Ct.) ("PR/TT Op.").

¹¹⁴ See PR/TT Op. at 84-85.

¹¹⁵ PR/TT Op. at 47.

¹¹⁶ PR/TT Op. at 83.

¹¹⁷ PR/TT Op. at 42-45. See pages 26 to 31 of this Report for an explanation of contact chaining within the context of telephone metadata analysis.

¹¹⁸ PR/TT Op. at 23.

¹¹⁹ PR/TT Op. at 47-49.

identified in the application,” the opinion stated: “Based on these explanations, the proposed collection appears to be a reasonably effective means to this end.”¹²⁰

After several years of operation, which included significant incidents of noncompliance with the FISA court’s orders, the bulk collection of Internet metadata under FISA court approval was terminated. Upon concluding that the program’s value was limited, the NSA did not seek to renew it. The government’s successful transition of this collection authority from the President’s Surveillance Program to the FISA court, however, served as a model for a similar transition in the NSA’s bulk collection of telephone records.

IV. Transition of Telephone Records Collection to FISA Court Authority

In December 2005, the *New York Times* published articles revealing the portion of the President’s Surveillance Program that involved intercepting the contents of international emails and telephone calls. This article caused concern for the telephone companies that were providing records under the program. Although their concerns about the interception of communications content were somewhat assuaged by the issuance of a Department of Justice “white paper” outlining the legal argument in favor of those interceptions, the companies remained concerned about providing telephone metadata (calling records) to the government. The *New York Times* had not revealed that aspect of the program, but reporters at *USA Today* were investigating it in early 2006. As a result, the government began to explore options for obtaining an order issued by the FISA court compelling assistance with the collection of telephone metadata, similar to the orders compelling assistance with the Internet metadata program. Ultimately, in May 2006 the government moved to transition the telephone records program from the President’s Surveillance Program to a section of FISA known as the “business records” provision.

FISA’s business records provision was first enacted in 1998.¹²¹ Titled “Access to certain business records for foreign intelligence and international terrorism investigations,” the provision originally permitted the FBI to apply to the FISA court for an order requiring a business “to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism.”¹²² The FISA court could issue such orders to only four types of businesses: “a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility.”¹²³ Any application for such an order was required to attest that there were

¹²⁰ PR/TT Op. at 53-54.

¹²¹ See Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2410-12 (Oct. 20, 1998).

¹²² 50 U.S.C. § 1862(a) (2000).

¹²³ 50 U.S.C. § 1862(a) (2000).

“specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.”¹²⁴

The Patriot Act, passed in 2001, significantly extended the reach of FISA’s business records provision.¹²⁵ Section 215 of the Patriot Act made two fundamental changes to the law. First, the FBI was no longer limited to seeking records from common carriers, public accommodation facilities, physical storage facilities, or vehicle rental facilities. Instead, the FBI could apply to the FISA court for an order requiring the production of “any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism.”¹²⁶ Second, the FBI no longer needed to demonstrate “specific and articulable facts” showing that a person to whom the records pertained was a foreign power or an agent of a foreign power. Instead, the FBI only needed to specify that the records concerned were being sought “for an authorized investigation” conducted under guidelines approved by the Attorney General.¹²⁷

Section 215 became one of the most controversial features of the Patriot Act, criticized by some lawmakers and others for the potentially wide scope of the record-gathering it authorized, as well as for its nondisclosure provision, which prevented recipients of an order from telling anyone about the order. It was one of several Patriot Act provisions that were not made permanent by the Act but were set to expire in 2005 (later extended to 2006).

Beginning in 2005, numerous bills were introduced in Congress to reauthorize Section 215 and the other “sunsetting” provisions of the Patriot Act, while making certain changes to those provisions. Congressional debate over these competing proposals extended into the spring of 2006. Thus, legislative debate about the reauthorization of Section 215, including proposals to limit its scope and impose additional safeguards, was occurring at the same time that executive branch lawyers were formulating a strategy to use that statute as the legal basis for the NSA’s bulk telephone records collection. The collection of telephone records under the President’s Surveillance Program was classified, however, and the government’s plans to seek new legal authority for that collection were not made public. Thus, congressional debates about the terms on which Section 215 should be renewed included no public discussion of the fact that the executive branch was planning to place the NSA’s bulk calling records program under the auspices of the reauthorized statute.

¹²⁴ 50 U.S.C. § 1862(b)(2)(B) (2000).

¹²⁵ See Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001).

¹²⁶ 50 U.S.C. § 1861(a)(1) (2002).

¹²⁷ 50 U.S.C. § 1861(b)(2) (2002).

In March 2006, the President signed the USA PATRIOT Improvement and Reauthorization Act of 2005, which made a number of changes to the business records provision of FISA (by then commonly referred to as Section 215).¹²⁸ Among other changes, the new law required that before granting a business records application, FISA court judges had to determine that the records being sought were likely “relevant” to an FBI investigation. Specifically, the law now demanded that each application contain “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).”¹²⁹

The new law made other modifications to Section 215 as well. One such change explicitly limited the items that could be obtained under the statute to those that were obtainable through grand jury subpoenas, administrative subpoenas, or court orders.¹³⁰ Certain proposals to restrict the scope of Section 215 even further were rejected.

By May 2006, Congress had renewed Section 215, and government lawyers were finalizing their application to the FISA court seeking permission to conduct the NSA’s telephone records program under the auspices of the amended statute.

The government’s application, filed in May 2006, requested an order directing certain U.S. telephone companies to provide the NSA with call detail records created by those companies. It requested that the companies be ordered to produce these records “on an ongoing daily basis to the extent practicable for a period of ninety days.” In other words, the application sought to put the companies under a continuing obligation, for a period of ninety days, to provide the NSA with all of their newly created calling records on a daily basis, rather than direct the companies to turn over records already in their possession at the time an order was served on them. The government sought telephone records so that the NSA could analyze them and disseminate intelligence from those records to “the FBI, CIA, or other appropriate U.S. Government and foreign government agencies.”¹³¹

The government’s application included a proposed set of rules for NSA’s handling, analysis, and dissemination of the calling records it received.¹³² The application and its

¹²⁸ See Pub. L. No. 109-177, 120 Stat. 192 (2006).

¹²⁹ 50 U.S.C. § 1861(b)(2)(A); see *id.* § 1861(c)(1) (requiring FISA court judge to find that an application meets this requirement before entering an order).

¹³⁰ See 50 U.S.C. § 1861(c)(2)(D) (stating that an order issued under Section 215 “may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things”).

¹³¹ Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism, at 15, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 06-05 (FISA Ct. May 23, 2006) (“2006 Mem.”).

¹³² See 2006 Mem. at 21-22.

supporting memorandum of law explained that the telephone records were being sought “by the FBI on behalf of NSA” so that the NSA could use metadata analysis “to identify and find operatives” of terrorist organizations. The application was supported by two declarations: one from NSA Director Lieutenant General Keith Alexander, describing the requested calling records and how the NSA would treat them, and one from National Counterterrorism Center Director Vice Admiral John Scott Redd, describing the threat to the United States posed by Al Qaeda.

The government’s memorandum of law argued, among other things, that the application was “completely consistent with this Court’s ground breaking and innovative decision” that had approved the collection of “bulk e-mail metadata” under FISA’s pen register provision.¹³³ The memorandum extensively cited that 2004 decision in discussing one of the key statutory prerequisites of FISA’s business records section — the requirement that any records sought be “relevant” to an authorized FBI investigation.

As noted above, Section 215 requires any application to include “a statement of facts showing that there are reasonable grounds to believe” that the records sought “are relevant to an authorized investigation” conducted in accordance with certain criteria.¹³⁴ To show that this requirement was met, the government argued: “All of the business records to be collected here are relevant to FBI investigations . . . because the NSA can effectively conduct metadata analysis only if it has the data in bulk.”¹³⁵ Echoing the arguments made in its 2004 Internet metadata application, the government stated that “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.”¹³⁶

The government’s legal memorandum relied heavily on the FISA court’s 2004 decision approving the NSA’s bulk Internet metadata program, arguing that the interpretation of the word “relevant” in Section 215 should incorporate “deference . . . to the fully considered judgment of the executive branch in assessing and responding to national security threats and in determining the potential significance of intelligence-related information.”¹³⁷ It further argued that the statute “does not expressly impose any requirement to tailor a request for tangible things precisely to obtain solely records that

¹³³ 2006 Mem. at 3.

¹³⁴ 50 U.S.C. § 1861(b)(2)(A).

¹³⁵ 2006 Mem. at 2.

¹³⁶ 2006 Mem. at 8 (emphasis in original).

¹³⁷ 2006 Mem. at 16-17.

are strictly relevant to the investigation.”¹³⁸ Even if it did, the memorandum argued, to interpret the word “relevant” in the statute it was “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.”¹³⁹ In sum, the government argued: “Just as the bulk collection of e-mail metadata was relevant to FBI investigations . . . so is the bulk collection of telephony metadata described herein.”¹⁴⁰

While acknowledging that its request would result in the collection of a “substantial portion” of call detail records that “would not relate to [terrorist] operatives,” the government argued that the records as a whole were nevertheless relevant because “the intelligence tool that the Government hopes to use to find [terrorist] communications — metadata analysis — requires collection and storing large volumes of the metadata to enable later analysis.”¹⁴¹ “All of the metadata collected is thus relevant,” the government concluded, “because the success of this investigative tool depends on bulk collection.”¹⁴²

The government’s application requested that during the analysis of calling records, contact chaining should be permitted to extend up to three “hops” from a seed number — instead of the two hops permitted in the Internet metadata program. In explanation for this difference, the supporting legal memorandum stated: “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.”¹⁴³

Although the memorandum’s discussion of the “relevance” requirement in Section 215’s relied heavily on the FISC’s earlier opinion approving the bulk collection of Internet metadata, the memorandum did not discuss whether that comparison was affected by differences between the telephone and Internet metadata collection programs. As noted earlier, under the Internet program records were acquired only if they travelled through certain designated communications channels that were relatively likely to contain messages of counterterrorism interest — to build a metadata archive that would be, in relative terms, “richly populated” with terrorism-related communications.¹⁴⁴

¹³⁸ 2006 Mem. at 17.

¹³⁹ 2006 Mem. at 18 (citing *Board of Educ. v. Earls*, 536 U.S. 822, 829 (2002)).

¹⁴⁰ 2006 Mem. at 17.

¹⁴¹ 2006 Mem. at 15.

¹⁴² 2006 Mem. at 15.

¹⁴³ 2006 Mem. at 9.

¹⁴⁴ PR/TT Op. at 47.

The memorandum also did not discuss whether Section 215 permits the court to prospectively order a company to turn over new records as they are created, on a daily basis, for a set period of time. (The Internet metadata program was conducted under the authority of FISA's pen/trap provision, which is designed to authorize the *prospective* collection of communications metadata.) The memorandum neither identified any portion of Section 215 that authorized such a procedure nor discussed whether any language in the statute foreclosed it.

While the government's application requested that the telephone companies be ordered to provide their records to the NSA, its memorandum did not discuss the fact that Section 215 states that records obtained under its authority are to be "made available to," "obtained" by, and "received by" the FBI.¹⁴⁵

The government's application also did not discuss whether any legal impediment to its application was presented by the Electronic Communications Privacy Act ("ECPA"). That act makes it unlawful for a telephone company to share records about its customers with the government, except in response to certain designated circumstances. Those enumerated circumstances do not include the issuance of an order from the FISA court under Section 215.¹⁴⁶

On May 24, 2006, FISA court Judge Malcolm J. Howard signed an order approving the government's application.¹⁴⁷ The order was not accompanied by an opinion explaining the decision to grant the application. Judge Howard's ten-page order recited the specific findings called for by Section 215 and stated that the government's application satisfied those statutory requirements.¹⁴⁸ Much of the order was devoted to listing restrictions on the NSA's maintenance and use of the calling records it would receive.¹⁴⁹ In accordance with the conditions proposed by the government, a number of such rules were imposed. These rules were similar to, though less comprehensive than, the rules that govern the program today, and they included the requirement that Section 215 records could be

¹⁴⁵ See 50 U.S.C. § 1861(b)(2)(B), (d)(1), (d)(2)(B), (g)(1), (h). Similarly, while the memorandum explained the minimization procedures that *the NSA* would apply to the calling records it obtained under the proposed order, it did not discuss the statutory requirement that its application include "an enumeration of the minimization procedures adopted by the Attorney General . . . that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be *made available to the Federal Bureau of Investigation* based on the order requested in such application." 50 U.S.C. § 1861(b)(2)(B) (emphasis added).

¹⁴⁶ See 18 U.S.C. §§ 2702, 2703. The government brought this issue to the FISA court's attention in late 2008.

¹⁴⁷ See Order at 10, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 06-05 (FISA Ct. May 24, 2006) ("2006 Order").

¹⁴⁸ See 2006 Order at 3.

¹⁴⁹ See 2006 Order at 4-10.

searched only with selections terms for which there already was “reasonable, articulable suspicion” of a connection with terrorism.¹⁵⁰

The May 2006 order directed that each telephone company produce its call detail records to the NSA, “and continue production on an ongoing daily basis thereafter for the duration of th[e] order.”¹⁵¹

The court’s order expired approximately ninety days after issuance. At the end of that period, it was renewed for a similar amount of time. Since May 2006, the court has continuously renewed its authorization of the NSA’s telephone records program approximately every ninety days.

Under the authority granted by the FISA court pursuant to Section 215, the NSA was able to collect the same telephone calling records it had previously obtained through the President’s Surveillance Program. No break in collection was caused by the transition to FISA court authority.

V. NSA Violations of FISA Court Orders and Modifications to the Program

Between 2006 and 2009, the terms of the FISA court’s orders approving the NSA’s calling records program remained essentially unchanged. But a series of compliance issues brought to the attention of the FISA court in 2009 resulted in some modifications to the program.

¹⁵⁰ Under the order, calling records obtained by the NSA were to be “stored and processed on a secure private network that NSA exclusively will operate,” and access to the records was to be limited by means of software to authorized analysts. 2006 Order at 5. Five years after collection by the NSA, the calling records had to be destroyed. *Id.* at 8. Echoing the rules previously imposed on the analysis of bulk Internet metadata, the order provided that the calling records could be accessed “only when NSA 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” specific terrorist organizations. *Id.* at 5. While the FISA court’s order did not explain what it meant for a telephone number to be “associated with” a terrorist organization, it provided that a telephone number believed to be used by a U.S. person could not be regarded as associated with terrorism solely on the basis of activities that are protected by the First Amendment to the Constitution. *Id.* Searches targeting particular telephone numbers could be approved by only seven NSA officials, and the agency’s Office of General Counsel was ordered to “review and approve proposed queries of archived metadata based on seed accounts numbers [sic] reasonably believed to be used by U.S. persons.” *Id.* at 6-7. Any use of the calling records for analysis, the order directed, “shall be strictly tailored to identifying terrorist communications and shall occur solely according to the procedures described in the application.” *Id.* at 6. The order required that every analyst’s access to the archived data be automatically logged for auditing capability. It also imposed rules for the dissemination outside the NSA of information identifying a U.S. person, and required the NSA to periodically review the program, including assessing the adequacy of the management controls for the processing and dissemination of U.S. person information. *Id.* at 6-9. See Part 3 of this Report for a description of the rules that presently govern the program.

¹⁵¹ 2006 Order at 4.

A. Improper Searches of Records by Automated Systems

In January 2009, representatives from the DOJ attended an NSA briefing concerning the agency's bulk telephone records program.¹⁵² This briefing, along with subsequent communication between the DOJ and the NSA, confirmed that the NSA was operating an automated searching system that utilized the telephone records obtained under FISA court approval in a manner contrary to the court's orders.¹⁵³

The NSA had developed and implemented a software system, called an "alert list," that automatically scanned new telephone records obtained by the agency as those new records were input into the agency's databases. The alert list system was set up to search telephone numbers that were obtained by the NSA through a number of means, including through the Section 215 orders. The alert list had been developed and implemented at a time when the NSA's collection was undertaken pursuant to the President's Surveillance Program, and thus before the FISA court's rules on the use of the records were in place.¹⁵⁴

The alert list contained thousands of telephone numbers that were of interest to NSA analysts. Most of these numbers had never been approved for use in querying the Section 215 calling records, because no determination had been made that those numbers satisfied the "reasonable, articulable suspicion" or "RAS" standard. As of January 2009, fewer than 2,000 of the nearly 18,000 numbers on the alert list were RAS-approved. But when newly obtained telephone records entered the NSA's databases from any source — including from the telephone companies providing records under Section 215 — the alert list automatically searched the incoming data to see if it contained records of any telephone calls that matched numbers on the alert list. If so, the system notified analysts of the match. According to a filing later submitted to the FISA court, NSA personnel "appear to have viewed the alert list process as merely a means of identifying a particular identifier on the alert list that might warrant further scrutiny," which might then lead to a determination of whether analysis based on that number should take place. The alert list did not automatically create contact chains for the telephone numbers it identified that were not RAS-approved.¹⁵⁵

Using the alert list system to search the telephone records obtained through Section 215 violated the FISA court's orders, which stated that analysts could not query those records except by searching the contacts of a selection term that had been given RAS

¹⁵² Memorandum of the United States in Response to the Court's Order Dated January 28, 2009, at 5, *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Feb. 17, 2009) ("2009 Mem.").

¹⁵³ See 2009 Mem. at 6.

¹⁵⁴ 2009 Mem. at 8.

¹⁵⁵ 2009 Mem. at 8, 11-12.

approval.¹⁵⁶ It also contradicted the sworn attestations of several executive branch officials who filed declarations with the FISA court about the operation of the NSA's program.¹⁵⁷

Upon discovering these problems, the DOJ promptly reported them to the FISC.¹⁵⁸ At the same time, the NSA made several failed attempts to implement a software fix but, unable to do so, it shut down the alert list process completely.¹⁵⁹

Upon being notified about noncompliance and misrepresentations regarding the alert system, FISA court Judge Reggie B. Walton — the judge who had most recently reauthorized the NSA's program — ordered the government to file a written brief, with supporting documentation, to help the court determine what remedial or punitive steps should be taken in light of the disclosure.¹⁶⁰

Responding to the FISA court's order, the government acknowledged that "the NSA's descriptions to the Court of the alert list process" were "inaccurate" and that the court's orders "did not provide the Government with authority to employ the alert list in the manner in which it did."¹⁶¹ The government attributed this problem in part to the NSA's mistaken interpretation of the FISA court's orders, which applied restrictions to the NSA's "archived data." According to the government, the NSA believed these restrictions did not apply to records as they were being transmitted into the NSA's databases but before they had been formatted and "archived" for use by analysts.¹⁶²

In sum, the government stated, the NSA's violations resulted not from an intent to mislead or disobey the court's orders, but rather from misunderstanding among the personnel involved with running the program and describing it to the FISA court about exactly how certain aspects of the program operated. As explained in a supporting declaration filed by NSA Director Keith Alexander, "it appears there was never a complete understanding among the key personnel" who reviewed the agency's reports to the court "regarding what each individual meant by the terminology used" in the reports. "Furthermore, from a technical standpoint, there was no single person who had a complete technical understanding of the [program's] system architecture."¹⁶³

¹⁵⁶ See 2009 Mem. at 16.

¹⁵⁷ See Order Regarding Preliminary Notice of Compliance Incident Dated January 15, 2009, at 2, *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Jan. 28, 2009) ("Jan. 2009 Order").

¹⁵⁸ See Jan. 2009 Order at 2.

¹⁵⁹ 2009 Mem. at 17.

¹⁶⁰ Jan. 2009 Order at 2-3.

¹⁶¹ 2009 Mem. at 1-2.

¹⁶² See 2009 Mem. at 11-12, 25-26.

¹⁶³ Declaration of Lieutenant General Keith B. Alexander, at 18-19, *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Feb. 13, 2009).

The government argued, however, that in light of the “vital” role played by the calling records in the government’s ability to find and identify terrorist agents, along with a number of extensive corrective measures the NSA was undertaking, the FISA court should not rescind its orders approving the collection of telephone records or take any other remedial action.¹⁶⁴

The government also reported that the NSA reviewed all 275 intelligence reports that the agency had disseminated since 2006 based on analysis of telephone records obtained under Section 215. While thirty-one of those reports were prompted by the alert list process, the NSA did not identify any such report that resulted from the query of a telephone number that lacked RAS approval. In addition, the agency determined that in all instances where a U.S. number served as the initial “seed” number targeted for analysis since 2006 (which occurred in twenty-two of the 275 reports), the U.S. number was either already the subject of electronic surveillance approved by the FISA court or had been reviewed by the NSA’s Office of General Counsel to ensure that the RAS determination for that number was not based solely on activities protected by the First Amendment.¹⁶⁵

In a subsequent order, Judge Walton observed that, as illustrated in the government’s response, “since the earliest days of the FISC-authorized collection of call-detail records by the NSA, the NSA has on a daily basis, accessed the BR metadata for purposes of comparing thousands of non-RAS approved telephone identifiers on its alert list against the BR metadata in order to identify any matches.”¹⁶⁶ He further wrote that the agency’s professed misinterpretation of the court’s orders — viewing their restrictions as applying only to telephone records that had been “archived” in the agency’s databases — “strains credulity.”¹⁶⁷ As Judge Walton put it: “It is difficult to imagine why the Court would intend the applicability of the RAS requirement — a critical component of the procedures proposed by the government and adopted by the Court — to turn on whether or not the data being accessed has been ‘archived’ by the NSA in a particular database at the time of access.”¹⁶⁸ Such an “illogical interpretation,” Judge Walton continued, “renders compliance with the RAS requirement merely optional.”¹⁶⁹

Regardless of what factors contributed to the NSA’s misrepresentations to the Court, Judge Walton wrote, “the government’s failure to ensure that responsible officials

¹⁶⁴ 2009 Mem. at 22-28.

¹⁶⁵ 2009 Mem. at 17-18.

¹⁶⁶ Order at 4-5, *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Mar. 2, 2009) (“Mar. 2009 Order”).

¹⁶⁷ Mar. 2009 Order at 5.

¹⁶⁸ Mar. 2009 Order at 5.

¹⁶⁹ Mar. 2009 Order at 5.

adequately understood the NSA's alert list process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the government and the FISC from taking steps to remedy daily violations of the minimization procedures set forth in FISC orders," which were designed to protect call detail records that "could not otherwise have been legally captured in bulk."¹⁷⁰

After the alert list problems were brought to the FISA court's attention, the NSA undertook an end-to-end review of its technical and operational processes for handling telephone records obtained under Section 215.¹⁷¹ That review uncovered another automated system implemented by the NSA that routinely permitted searches of the Section 215 telephone records without RAS approval.¹⁷²

According to a filing notifying the FISC about the issue, this analytical tool "determined if a record of a telephone identifier was present in NSA databases and, if so, provided analysts with certain information regarding the calling activity associated with that identifier." When NSA analysts utilized the tool to search for particular numbers, the system would query the Section 215 database of calling records along with other NSA databases. The tool did not, however, "provide analysts with the telephone identifiers that were in contact with the telephone identifier that served as a basis for the query."¹⁷³

In response to this new discovery, in February 2009 the NSA restricted access to its Section 215 calling records to permit only manual queries based on RAS-approved telephone numbers, preventing any automated process from accessing the records.¹⁷⁴

B. Improper Searches of Records by Analysts

In 2008 and 2009, the government also brought to the attention of the FISA court a series of improper manual searches of telephone records by analysts that violated the court's orders.

During a five-day period in April 2008, the NSA determined, thirty-one NSA analysts queried the telephone records database "without being aware they were doing so."¹⁷⁵ Upon discovering this problem, Judge Walton later explained, "the NSA undertook a number of remedial measures, including suspending the 31 analysts' access pending additional

¹⁷⁰ Mar. 2009 Order at 8-9.

¹⁷¹ See Notice of Compliance Incidents, at 1, *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Feb. 26, 2009).

¹⁷² *Id.*

¹⁷³ Notice of Compliance Incidents, *supra*, at 2-3.

¹⁷⁴ Notice of Compliance Incidents, *supra*, at 3.

¹⁷⁵ Mar. 2009 Order at 9 (quoting government report).

training, and modifying the NSA's tool for accessing the data so that analysts were required specifically to enable access to the BR metadata and acknowledge such access."¹⁷⁶

These corrective steps did not entirely solve the problem. As the government informed the FISA court in December of that year, "one analyst had failed to install the modified access tool and, as a result, inadvertently queried the data using five identifiers for which NSA had not determined that the reasonable articulable suspicion standard was satisfied."¹⁷⁷

Similar problems continued, and in late January 2009 the government informed the court that, during December and January, two NSA analysts had used 280 foreign telephone numbers to query the records without determining that the RAS standard had been satisfied.¹⁷⁸ As Judge Walton noted upon being informed of this latest problem, those queries apparently were conducted "despite full implementation" of the software modifications and additional training that the NSA carried out in response to previous violations.¹⁷⁹

In February 2009, the NSA initiated an audit of all queries made of its Section 215 telephone records in the preceding three months. This audit identified more instances of improper analyst queries of the data: three analysts were responsible for fourteen instances of improper querying during that period. None of the improper queries resulted in any intelligence reporting and none of the identifiers used were associated with a U.S. telephone number or person. The NSA concluded that each analyst thought he or she was conducting queries of other repositories of telephone records not subject to the FISA court's orders. The government stated that software changes were made to ensure that analysts could access the Section 215 data only through one specific tool.¹⁸⁰

C. FISA Court Response to NSA Violations

By March 2009, all of the violations described above had been reported to the FISA court. After surveying the violations, Judge Walton reminded the government that the FISA court had authorized the bulk collection of telephone records based upon "(1) the government's explanation, under oath, of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and

¹⁷⁶ Mar. 2009 Order at 9-10.

¹⁷⁷ Mar. 2009 Order at 10.

¹⁷⁸ Mar. 2009 Order at 10.

¹⁷⁹ Mar. 2009 Order at 10.

¹⁸⁰ Supplemental Declaration of Lieutenant General Keith B. Alexander, at 8-9, *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Feb. 26, 2009).

include specific oversight requirements.”¹⁸¹ The judge noted that given the executive branch’s expertise in matters of national security, and the large scale of the collection program, “the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of U.S. persons as required by applicable minimization procedures.”¹⁸² Judge Walton wrote that he “no longer” had confidence “that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court’s orders.”¹⁸³

Observing that “from the inception of this FISA BR program, the NSA’s data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures,” Judge Walton concluded that “notwithstanding the remedial measures undertaken by the government . . . more is needed to protect the privacy of U.S. person information acquired and retained pursuant to the FISC orders issued in this matter.”¹⁸⁴ However, “given the government’s repeated representations that the collection of the BR metadata is vital to national security,” and in light of the court’s earlier determinations that the program met the statutory requirements of Section 215, when conducted “in compliance with appropriate minimization procedures,” Judge Walton decided that “it would not be prudent to order that the government’s acquisition of the BR metadata cease at this time.”¹⁸⁵

Instead, Judge Walton prohibited NSA analysts from conducting any searches of the telephone records without obtaining prior approval from the FISA court to search a particular number.¹⁸⁶ Once the NSA completed its end-to-end system engineering and process reviews, he ordered, it was to file a number of documents and affidavits with the FISA court regarding the results of this review, remedial steps taken, proposed oversight procedures for any future court order, and the national security value of the telephone records program.¹⁸⁷

D. Improper Dissemination of Call Records Outside the NSA

As the NSA was conducting its end-to-end review of the Section 215 program, the government reported to the FISA court another violation of its orders. As the government explained, calling records that had been analyzed by the NSA were made available to other

¹⁸¹ Mar. 2009 Order at 12 (quoting government report).

¹⁸² Mar. 2009 Order at 12.

¹⁸³ Mar. 2009 Order at 12.

¹⁸⁴ Mar. 2009 Order at 14-15, 17.

¹⁸⁵ Mar. 2009 Order at 17.

¹⁸⁶ Mar. 2009 Order at 18-19.

¹⁸⁷ Mar. 2009 Order at 19-20.

intelligence agencies without taking the steps that were required before such dissemination of information about U.S. persons was permitted. This violated not only the FISA court's orders but also the generally applicable dissemination rules governing all of the NSA's activities.

In June 2009, the government notified the FISA court that the unminimized results of some queries of Section 215 telephone records — meaning the results of contact-chaining searches, including information regarding U.S. persons — had been uploaded by the NSA into a database to which other intelligence agencies had access. Providing such access, the government explained, may have resulted in the dissemination of U.S. person information in violation of the NSA's general dissemination rules and the more restrictive rules on disseminations imposed by the FISA court in its Section 215 orders.¹⁸⁸ The government asserted that the NSA promptly terminated the access of outside agencies to these records and investigated the matter.¹⁸⁹

Judge Walton responded by ordering the government to file a weekly report listing each instance during the preceding week in which the NSA shared, in any form, information derived from the Section 215 program with anyone outside of the agency. He also directed the government to furnish a full explanation of how this violation came about in its forthcoming submissions reporting the results of its end-to-end systems review.¹⁹⁰

E. FISA Court Reauthorization of the Program with More Detailed Rules

In August 2009 the government submitted to the FISA court documents reporting the results of its end-to-end review and responding to the court's concerns regarding violations of its orders. These documents included a lengthy report to the court, a declaration from NSA Director Keith Alexander concerning incidents of NSA noncompliance with the court's orders, a declaration from General Alexander concerning the value of the NSA's bulk telephone records program, an affidavit from FBI Director Robert Mueller concerning the value of the program, and an NSA review of the program's operation.

Collectively, these documents sought to explain previous instances of NSA noncompliance with the FISA court's orders, identify new areas in which the agency's practices had not been fully or accurately described to the court, describe remedial steps taken to correct those deficiencies, articulate the value of the program in combating terrorism, and propose a set of expanded rules and restrictions for the continuation of the program.

¹⁸⁸ Order at 5, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 09-06 (FISA Ct. June 22, 2009) ("June 2009 Order").

¹⁸⁹ June 2009 Order at 6.

¹⁹⁰ June 2009 Order at 7-8.

As the program came up for renewal by the FISA court the following month, the government requested permission to resume analyzing calling records based on the NSA's own determinations that the RAS standard was satisfied — rather than by seeking prior permission of the FISA court, as the agency had been required to do for the previous six months. The government's application proposed a more detailed set of conditions restricting the NSA's handling and use of telephone records obtained under Section 215, in keeping with the results of the investigations carried out over the previous months. In early September 2009, Judge Walton granted the government's application, restoring the bulk telephone records program to its original footing with the addition of these more detailed conditions. The resulting primary order closely resembles the orders that have since been issued by the FISA court up to the present day.¹⁹¹

VI. Operation of the Program Between 2009 and the Present

Since 2009, there have been no major changes in the operation of the Section 215 program. Between late 2009 and late 2013, the government submitted notices to the FISA court reporting ten different types of violations of the court's orders. Nearly all of the incidents in question involved isolated violations that the NSA took steps to remedy and prevent in the future. Two incidents involved more widespread, though inadvertent, violations of the rules governing the Section 215 program.

The isolated incidents reported to the FISA court comprised the following violations: (1) The NSA inadvertently received a tiny amount of cell site location information from a provider on one occasion (the data was accessible only to technical personnel and was never available to intelligence analysts); (2) An analyst performed a query on a selection term whose RAS approval had expired earlier that month (the agency responded with technical modifications to prevent such incidents); (3) A RAS determination was made based on what was later discovered to be incorrect information (the resulting query results were destroyed, and no intelligence reports were issued based on the query); (4) On several occasions analysts shared the results of queries via email with NSA personnel who were not authorized to receive such information (the agency responded with new procedures for email distribution); (5) An analyst sent an email message containing information derived from the Section 215 data to the wrong person, due to a typographical error in the email address (the recipient reportedly deleted the message without reading it, recognizing the error); (6) Information about U.S. persons was on three occasions disseminated outside the NSA before any official made the determinations that are required for such disseminations (officials later concluded that the

¹⁹¹ See Primary Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 09-13 (FISA Ct. Sept. 3, 2009).

standards for dissemination were satisfied in each case); (7) The government filed nine reports with the FISA court that lacked certain information required to be in such reports (the missing information involved no wrongdoing or noncompliance, and it subsequently was furnished to the court); (8) The government filed a compliance report with the FISA court on a Monday, instead of on the deadline the previous Friday.

The two other noncompliance incidents were more far-reaching, although both represented inadvertent violations. In one incident, NSA technical personnel discovered a technical server with nearly 3,000 files containing call detail records that were more than five years old, but that had not been destroyed in accordance with the applicable retention rules. These files were among those used in connection with a migration of call detail records to a new system. Because a single file may contain more than one call detail record, and because the files were promptly destroyed by agency technical personnel, the NSA could not provide an estimate regarding the volume of calling records that were retained beyond the five-year limit. The technical server in question was not available to intelligence analysts.

In the other incident, the NSA discovered that it had unintentionally received a large quantity of customer credit card numbers from a provider. These related to cases in which a customer used a credit card to pay for a phone call. This problem, which involved cases in which customers used credit cards to pay for phone calls, resulted from a software change implemented by the provider without notice to the NSA. In response to the discovery, the NSA masked the credit card data so that it would not be viewable for intelligence analysis. It also asked providers to give advance notice of changes that might affect the data transmitted to the NSA. The agency later eliminated the credit card data from its analytic stores, although the data remained in the agency's non-analytic online stores and in back-up tapes. Despite repeated efforts to attempt a technical fix, six months later the agency was still receiving a significant amount of credit card information from the provider. As a result of additional efforts, this was reduced to fewer than five credit card numbers per month, and the provider continued to work to eliminate such production entirely.

In June 2013, the British newspaper *The Guardian* began publishing a series of articles regarding the Section 215 program and other secret NSA activities, based on unauthorized disclosures of classified documents by NSA contractor Edward Snowden. In the months following these disclosures, the executive branch declassified certain information about the telephone records program, and intelligence officials testified about it before Congress. In August 2013, the Obama Administration released a white paper setting forth the Administration's legal position on the statutory and constitutional

legitimacy of the program.¹⁹² Later that month, FISA court Judge Claire V. Eagan issued the first FISA court opinion that explained the court's rationale for approving the program.¹⁹³ On October 11, 2013, the FISA court again renewed the program, and Judge Mary A. McLaughlin issued a memorandum adopting and expanding on Judge Eagan's reasoning.¹⁹⁴ The FISA court reauthorized the Section 215 program most recently on January 3, 2014.

¹⁹² See Administration White Paper, Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act (Aug. 9, 2013).

¹⁹³ See Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

¹⁹⁴ Memorandum, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-158 (FISA Ct. Oct. 11, 2013).

Part 5:
STATUTORY ANALYSIS

I. Overview

Since 2006, the government has argued before the FISA court that Section 215 of the Patriot Act provides a legal basis for the NSA's bulk telephone records program. The FISA court has agreed and has authorized the program. In the wake of public disclosure of the program in June 2013, the government has further defended its statutory legitimacy in litigation and in a publicly issued white paper. Having independently examined this statutory question, the Board disagrees with the conclusions of the government and the FISA court. The Board believes that the following analysis is the most comprehensive analysis to date of Section 215 as it relates to the NSA's bulk telephone records program. We find that there are multiple and cumulative reasons for concluding that Section 215 does not authorize the NSA's ongoing daily collection of telephone calling records concerning virtually every American.

To be clear, the Board believes that this program has been operated in good faith to vigorously pursue the government's counterterrorism mission and appreciates the government's efforts to bring the program under the oversight of the FISA court. However, the Board concludes that Section 215 does not provide an adequate legal basis to support this program. Because the program is not statutorily authorized, it must be ended.

Section 215 is designed to enable the FBI to acquire records that a business has in its possession, as part of an FBI investigation, when those records are relevant to the investigation. Yet the operation of the NSA's bulk telephone records program bears almost no resemblance to that description.

First, the telephone records acquired under this program have no connection to any specific FBI investigation at the time the government obtains them. Instead, they are collected in advance to be searched later for records that do have such a connection. Second, because the records are collected in bulk — potentially encompassing all telephone calling records across the nation — they cannot be regarded as “relevant” to any FBI investigation without redefining that word in a manner that is circular, unlimited in scope, and out of step with precedent from analogous legal contexts involving the production of records. Third, instead of compelling telephone companies to turn over records already in their possession, the program operates by placing those companies under a continuing obligation to furnish newly generated calling records on a daily basis. This is an approach lacking foundation in the statute and one that is inconsistent with FISA as a whole, because it circumvents another provision that governs (and limits) the prospective collection of the

same type of information. Fourth, the statute permits only the FBI to obtain items for use in its own investigations. It does not authorize the NSA to collect anything.

In addition, the Board concludes that the NSA's program violates the Electronic Communications Privacy Act. That statute prohibits telephone companies from sharing customer records with the government except in response to specific enumerated circumstances — which do not include orders issued under Section 215.

Finally, the Board does not believe that these flaws are overcome because Congress twice delayed the expiration of Section 215 during the operation of the program without amending the statute. The “reenactment doctrine,” under which Congress is presumed to have adopted settled administrative or judicial interpretations of a statute, does not trump the plain meaning of a law, and it cannot save an administrative or judicial interpretation that contradicts the statute itself. Moreover, the circumstances presented here differ in pivotal ways from any in which the reenactment doctrine has ever been applied. Applying the doctrine here would undermine the public's ability to know what the law is and hold their elected representatives accountable for their legislative choices.

II. Connection Between Calling Records and Specific FBI Investigations

In order for business records or other tangible things to be acquired through Section 215, the government must provide a statement of facts showing reasonable grounds to believe that they are “relevant to an authorized investigation (other than a threat assessment)” to obtain foreign intelligence information or to protect against international terrorism or clandestine intelligence activities.¹⁹⁵

Before examining whether the massive quantity of telephone records acquired under Section 215 can plausibly be regarded as relevant to the government's counterterrorism efforts, given that nearly all of them are not connected to terrorism in any way, the latter part of the statutory formulation “relevant to *an authorized investigation*” merits independent consideration. Regardless of how expansively the word “relevant” may be construed, the statute demands some nexus between the records sought and a specific investigation.

Notably, Section 215 requires that records sought be relevant to “an” authorized investigation. Elsewhere, the statute similarly describes the records that can be obtained

¹⁹⁵ 50 U.S.C. § 1861(b)(2)(A) (“Each application under this section . . . shall 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) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities[.]”).

under its auspices as those sought “for an investigation.”¹⁹⁶ The use of the singular noun in these passages signals an expectation that the records are being sought for use in a specific, identified investigation. This interpretation is reinforced by the requirement that the FISA court make specific findings about the investigation for which the records are sought — that it is supported by a factual predicate, conducted according to guidelines approved by the Attorney General, and not based solely upon activities protected by the First Amendment when conducted of a U.S. person.¹⁹⁷

The government’s applications to the FISA court seeking renewal of the NSA’s program do not link the applications to a single counterterrorism investigation. Instead, the applications list multiple terrorist organizations, assert that the FBI is investigating all of them, and declare that the telephone records being sought are relevant to each of those investigations. The FISA court orders granting the government’s applications all contain a finding that there are reasonable grounds to believe that the records sought are relevant to authorized “investigations.”¹⁹⁸ The orders further conclude that these investigations satisfy the three criteria listed above.¹⁹⁹ The FISA court has stated that the purpose of the government’s applications “is to obtain foreign intelligence information in support of . . . individual authorized investigations to protect against international terrorism and concerning various international terrorist organizations.”²⁰⁰

The government’s approach, in short, has been to declare that the calling records being sought are relevant to *all* of the investigations cited in its applications. This approach, at minimum, is in deep tension with the statutory requirement that items obtained through a Section 215 order be sought for “an investigation,” not for the purpose of enhancing the government’s counterterrorism capabilities generally. Declaring that the calling records are relevant to every counterterrorism investigation cited by the government is little

¹⁹⁶ 50 U.S.C. § 1861(a)(1).

¹⁹⁷ By referring to an “authorized” investigation, “other than a threat assessment,” 50 U.S.C. § 1861(b)(2)(A), Section 215 excludes those FBI investigatory activities that “do not require a particular factual predicate” — limiting its reach to approved investigations that have been initiated “on the basis of any ‘allegation or information’ indicative of possible criminal activity or threats to the national security.” FBI Domestic Investigations and Operations Guide §§ 5.1, 6.2 (Oct. 15, 2011). The investigation for which the records are sought also must be “conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order),” and must “not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.” 50 U.S.C. § 1861(a)(2).

¹⁹⁸ See Primary Order at 2, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-158 (Oct. 11, 2013) (“Primary Order”).

¹⁹⁹ See Primary Order at 2.

²⁰⁰ Amended Memorandum Opinion at 4, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013) (“Amended Memorandum Opinion”).

different, in practical terms, from simply declaring that they are relevant to counterterrorism in general.

That is particularly so when the number of calling records sought is not limited by reference to the facts of any specific investigation. At its core, the approach boils down to the proposition that essentially all telephone records are relevant to essentially all international terrorism investigations. The Board does not believe that this approach comports with a fair reading of the statute.

Moreover, this approach undermines the value of an important statutory limitation on the government's collection of records under Section 215. The statute provides that records cannot be obtained for a "threat assessment," meaning those FBI investigatory activities that "do not require a particular factual predicate."²⁰¹ By excluding threat assessments from the types of investigations that can justify an order, Congress directed that Section 215 not be used to facilitate the broad and comparatively untethered investigatory probing that is characteristic of such assessments. But by collecting the nation's calling records *en masse*, under an expansive theory of their relevance to multiple investigations, the NSA's program undercuts one of the functions of the "threat assessment" exclusion: ensuring that records are not acquired by the government without some reason to suspect a connection between those records and a specific, predicated terrorism investigation. While the rules governing the program limit the *use* of telephone records to searches that are prompted by a specific investigation, the relevance requirement in Section 215 restricts the *acquisition* of records by the government.

III. Relevance

The government has argued, and the FISA court has agreed, that essentially the entire nation's calling records are "relevant" to every counterterrorism investigation cited in the government's applications to the court. This position is untenable. Moreover, the interpretation of Section 215 adopted by the FISA court is dangerously overbroad, leading to the implication that virtually all information may be relevant to counterterrorism and therefore subject to collection by the government.

Since the public disclosure of the NSA's program, two related rationales have been offered in support of the government's interpretation of the word "relevant" under Section

²⁰¹ FBI Domestic Investigations and Operations Guide §§ 5.1, 6.2 (Oct. 15, 2011). Although threat assessments do not require a factual predicate, they may not be based on "arbitrary or groundless speculation" or "solely on the exercise of First Amendment protected activities or on the race, ethnicity, national origin or religion of the subject." *Id.* § 5.1. *See also* The Attorney General's Guidelines for Domestic FBI Operations, § II (Sept. 29, 2008) (distinguishing between assessments and predicated investigations).

215. One is found in a FISA court opinion from August 2013, which reflects the interpretation presented to the court since 2006 in the government’s applications.²⁰² The other, related, rationale is found in a publicly issued administration white paper and in filings submitted to other courts by the government in response to legal challenges to the program.²⁰³ We address these two rationales in turn.

A. “Necessity”

While recognizing that the NSA collects telephone records indiscriminately under its Section 215 program — potentially acquiring the entire nation’s daily calling records — the FISA court has concluded that all of those records are relevant to the government’s counterterrorism investigations. The court’s reasoning: collecting telephone records in bulk is necessary to enable a particular analytic tool that the government wishes to employ in its investigations. Because this tool involves searching all calling records in order to identify those that are related to terrorism, all calling records are relevant to the government’s investigations.

In the FISA court’s words, its finding of relevance “most crucially depended on the conclusion that bulk collection is *necessary* for NSA to employ tools that are likely to generate useful investigative leads to help identify and track terrorist operatives.”²⁰⁴ As with an earlier NSA program that collected Internet metadata in bulk, the court determined that “bulk collections such as these are necessary to identify the much smaller number of [international terrorist] communications,” and the court explained that “it is this showing of necessity that led the Court to find that that the entire mass of collected metadata is relevant to investigating [international terrorist groups] and affiliated persons.”²⁰⁵ Because “the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity.”²⁰⁶ Therefore, according to the FISA court, “[a]ll of the metadata collected is thus

²⁰² See Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

²⁰³ See Administration White Paper, Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act, at 8-15 (Aug. 9, 2013); Defendants’ Memorandum of Law in Support of Motion to Dismiss the Complaint, at 20-29, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Aug. 26, 2013).

²⁰⁴ Amended Memorandum Opinion at 20 (quoting Memorandum Opinion, No. PR/TT [redacted] (FISA Ct. 2010)); see *id.* at 21 (“This case is no different.”).

²⁰⁵ Amended Memorandum Opinion at 20 (quoting Memorandum Opinion, No. PR/TT [redacted] (FISA Ct. 2010) (internal quotation marks omitted; brackets in Amended Memorandum Opinion)).

²⁰⁶ Amended Memorandum Opinion at 22.

relevant, because the success of this investigative tool depends on bulk collection.”²⁰⁷ A recent decision from the Southern District of New York adopted the same reasoning, stating that “aggregated telephony metadata is relevant because it allows the [NSA’s] querying technique to be comprehensive.”²⁰⁸

In the Board’s view, this interpretation of the statute is circular and deprives the word “relevant” of any interpretive value. All records become relevant to an investigation, under this reasoning, because the government has developed an investigative tool that functions by collecting all records to enable later searching. The implication of this reasoning is that if the government develops an effective means of searching through *everything* in order to find *something*, then *everything* becomes relevant to its investigations. The word “relevant” becomes limited only by the government’s technological capacity to ingest information and sift through it efficiently.

If Section 215’s relevance requirement is to serve any meaningful function, however, relevance cannot be premised on the government’s desire to use a tool whose very operation depends on collecting information without limit. We believe that a tool designed to capture *all* records of a particular type is simply incompatible with a statute requiring reasonable grounds to believe that “the tangible things sought are relevant to an authorized investigation.”²⁰⁹

We find such a result not only inconsistent with the text of Section 215 but dangerously overbroad. While terrorists use telephone communications to facilitate their plans, they also write emails, open bank accounts, use debit and credit cards, send money orders, rent vehicles, book hotel rooms, sign leases, borrow library books, and visit websites, among other things. Having information about *all* such transactions, as conducted by every person in the United States, would aid the government’s counterterrorism efforts so long as the government developed a technological means of sorting through the mass of data to find clues about suspected operatives. This elastic definition of relevance not only proves too much, but also supplies a license for nearly unlimited governmental acquisition of other kinds of transactional information.

This rationale also is inconsistent with Section 215’s requirement that the government provide “a statement of facts” showing that there are “reasonable grounds to

²⁰⁷ Amended Memorandum Opinion at 21 (quoting Mem. of Law in Support of App. for Certain Tangible Things for Investigations to Protect Against International Terrorism, at 15, No. BR 06-05 (May 23, 2006)).

²⁰⁸ Memorandum & Order at 35, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013). As the government has put it, the entire nation’s telephone calling records are relevant to the FBI’s counterterrorism investigations because “NSA’s analytic tools require the collection and storage of a large volume of metadata” and its querying process “is not feasible unless NSA analysts have access to telephony metadata in bulk.” Administration White Paper at 13.

²⁰⁹ 50 U.S.C. § 1861(b)(2)(A).

believe” that items sought are relevant to an investigation.²¹⁰ Such language calls upon the government to supply a fact-bound explanation of why the particular group of records it seeks may have some bearing on one of its investigations. But because the NSA’s program depends on collecting virtually all telephone records, only two facts are cited by the government in support of its applications: that terrorists communicate by telephone, and that it is necessary to collect records in bulk to find the connections that can be uncovered by NSA analysis.²¹¹

Neither of these facts shows why a particular group of telephone records may be relevant to an investigation, because the government has not limited its request to any particular group at all — only to a particular *type* of record (telephone calling records). But the *type* of records that can be acquired under Section 215 is defined elsewhere in the statute.²¹² Unless the relevance requirement imposes an additional restriction beyond those provisions, it serves no real function at all. Thus we disagree that “all telephony metadata is a relevant category of information” that the government may request under Section 215.²¹³ Because if the category “all telephony metadata” is acceptable, why not “all metadata”? Or simply “all data”? That is the future that can be expected if the government’s interpretation of Section 215 prevails.

B. Analogous Contexts

Noting that the word “relevant” is undefined in Section 215, the FISA court believed that it must be given its “ordinary meaning.”²¹⁴ In contrast, the government has argued in a white paper and in litigation that the concept of relevance “has developed a particularized legal meaning in the context of the production of documents and other things in conjunction with official investigations and legal proceedings.”²¹⁵ The government argues that Congress “legislated against that legal backdrop in enacting Section 215 and thus

²¹⁰ 50 U.S.C. § 1861(b)(2)(A).

²¹¹ As the FISA court put it: “The fact that international terrorist operatives are using telephone communications, and that it is necessary to obtain the bulk collection of a telephone company’s metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, is sufficient to meet the low statutory hurdle set out in Section 215 to obtain a production of records.” Amended Memorandum Opinion at 22-23.

²¹² Specifically, the statute authorizes production of “any tangible things (including books, records, papers, documents, and other items)” that “can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things.” 50 U.S.C. § 1861(a)(1), (c)(2)(D).

²¹³ Memorandum & Order, *ACLU v. Clapper*, *supra*, at 37.

²¹⁴ Amended Memorandum Opinion at 18 (citing *Taniguchi v. Ken Pacific Saipan, Ltd.*, 132 S. Ct. 1997, 2002 (2012)).

²¹⁵ Administration White Paper at 9.

'presumably kn[e]w and adopt[ed] the cluster of ideas that were attached to [the] word in the body of learning from which it was taken.'"²¹⁶

Accordingly, the government has cited decisions involving civil discovery, grand jury subpoenas, and administrative subpoenas, arguing that in these analogous contexts courts recognize that "the relevance standard permits requests for the production of entire repositories of records, even when any particular record is unlikely to directly bear on the matter being investigated, because searching the entire repository is the only feasible means to locate the critical documents."²¹⁷ More broadly, the government views this case law as illustrating that "the relevance standard permits discovery of large volumes of information in circumstances where the requester seeks to identify much smaller amounts of information within the data that directly bears on the matter."²¹⁸ A recent decision of the Southern District of New York cited some of these decisions for the same purpose.²¹⁹

We agree that the word "relevant" in Section 215 should be interpreted in light of precedent from analogous legal contexts involving the production of documents. But a close look at the decisions cited by the government, and others concerning the standards of relevance governing discovery and subpoenas, refutes the idea that the NSA's bulk collection of telephone records would be regarded as satisfying the relevance standard in any of those contexts.

The first problem is that, as the government acknowledges, "the cases that have been decided in these contexts do not involve collection of data on the scale at issue in the telephony metadata collection program."²²⁰ But the second and more fundamental problem is that these cases do not employ an analytical concept of "relevance" that matches the one being offered in support of the NSA's program. Simply put, there is no precedent for the notion that the government may collect a massive trove of records, of which virtually none can be expected to be pertinent to its investigation, merely because it has developed a technological tool that it believes will enable it to locate an infinitesimal fraction of pertinent records within that trove. Superficial similarities to that notion in the case law cited by the government dissolve upon further inspection.

It certainly is true that in the civil, grand jury, and administrative subpoena contexts, parties requesting materials may seek broad categories of documents, among which many of the individual records produced may prove unrelated. Such categories of materials can

²¹⁶ Administration White Paper at 9 (quoting *FAA v. Cooper*, 132 S. Ct. 1441, 1449 (2012)).

²¹⁷ Administration White Paper at 10.

²¹⁸ Administration White Paper at 10.

²¹⁹ Memorandum & Order, *ACLU v. Clapper*, at 37.

²²⁰ Administration White Paper at 11.

be regarded as “relevant” if obtaining them aids a party’s fact-finding efforts, even if not all of the records are expected to be directly pertinent. Civil litigants, grand juries, and administrative agencies, when pursuing the “discovery of evidence” or acting in their “investigative function,” need not be “limited [by] forecasts of the probable result of the investigation.”²²¹ The case law also shows that the sheer volume of a discovery request is not alone grounds for a finding of irrelevance — at least in the scenarios confronted so far by the courts, which have involved dramatically fewer materials.

These broad propositions are not sufficient to justify the NSA’s bulk collection of records under Section 215. In every decision cited by the government, the category of records sought has been limited in *some* way by reference to the facts of the specific investigation at hand. There is always some qualitative reason to suspect that the particular group of items requested has some special significance to the investigation, making the items in that category “relevant” even if many of them turn out to be immaterial. For instance, suspecting a doctor of health care fraud, the government may broadly subpoena that doctor’s records for evidence of wrongdoing. Or suspecting that an employer is discriminating against women, plaintiffs may obtain a wide range of human resource records to analyze for patterns of discrimination. The scope of the request is always defined and limited by the specific facts of the investigation.

Not so for the NSA’s bulk telephone records program, where the government seeks virtually all telephone calling records based on the premise that terrorists use telephones. The only limiting principle is that the government’s request is confined to a particular *type* of record: telephone calling records. As to that type of record, however, the government seeks access to virtually everything. Such a concept simply is not found in the case law that, as the government acknowledges, Congress presumably incorporated into Section 215’s definition of “relevant.”

Simply put, analogous precedent does not support anything like the principle that necessity equals relevance, or that a body of records can be deemed relevant when virtually all of them are known to be unrelated to the purpose for which they are sought. Regardless of the broad scope courts have afforded the relevance standard with respect to discovery and government subpoenas, there is always a qualitative limiting principle that connects the range of documents sought to the facts of the investigation at hand, thus placing a check on the power to acquire information. Relevance limitations are a shield that protects against overreaching, not a sword that enables it.

Below, we discuss in detail the case law from which we draw these conclusions. In doing so, we separate decisions from the civil, criminal, and administrative contexts, to

²²¹ *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 216 (1946) (quoting *Blair v. United States*, 250 U.S. 273, 282 (1919)).

better explain how particular holdings fit into the standards that govern each production or discovery regime.

1. Relevance in Civil Discovery

The relevance requirement in civil discovery is rooted in Rule 26 of the Federal Rules of Civil Procedure, which permits parties to obtain discovery “regarding any nonprivileged matter that is relevant to any party’s claim or defense” and authorizes courts to “order discovery of any matter relevant to the subject matter involved in the action.”²²² “Relevant information,” under Rule 26, “need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.”²²³

The phrase “relevant to the subject matter involved in the action” 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.”²²⁴ Thus, the scope of civil discovery under the Federal Rules “is traditionally quite broad,” and the test “is whether the line of interrogation is reasonably calculated to lead to the discovery of admissible evidence.”²²⁵ These standards also reflect the reality that a party cannot know in advance the content of all the materials it seeks. To some inevitable extent, therefore, “pretrial discovery is a fishing expedition and one can’t know what one has caught until one fishes.”²²⁶

Nevertheless, “discovery, like all matters of procedure, has ultimate and necessary boundaries.”²²⁷ As one court has put it, “practical considerations dictate that the parties should not be permitted to roam in shadow zones of relevancy and to explore matter which does not presently appear germane on the theory that it might conceivably become so.”²²⁸ And the broad scope of relevance “should not be misapplied” to permit overbearing requests.²²⁹ The “boundaries defining information that is relevant to the subject matter

²²² FED. R. CIV. P. 26(b)(1).

²²³ FED. R. CIV. P. 26(b)(1).

²²⁴ *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978) (citing *Hickman v. Taylor*, 329 U.S. 495, 501 (1947)).

²²⁵ *Lewis v. ACB Bus. Servs., Inc.*, 135 F.3d 389, 402 (6th Cir. 1998) (quotation marks omitted) (citing, *inter alia*, *Oppenheimer Fund, Inc.*, 437 U.S. at 351); accord *Daval Steel Products v. M/V Fakredine*, 951 F.2d 1357, 1367 (2d Cir. 1991) (“This obviously broad rule is liberally construed.”); *Nat’l Serv. Indus., Inc. v. Vafila Corp.*, 694 F.2d 246, 250 (11th Cir. 1982) (“This phrase is to be construed broadly.”); *Santiago v. Fenton*, 891 F.2d 373, 379 (1st Cir. 1989) (“As a general matter, parties are entitled to broad discovery.”).

²²⁶ *Nw. Mem’l Hosp. v. Ashcroft*, 362 F.3d 923, 931 (7th Cir. 2004).

²²⁷ *Oppenheimer Fund, Inc.*, 437 U.S. at 351 (quoting *Hickman*, 329 U.S. at 507); see *id.* at 354 (finding discovery request to be beyond “the scope of legitimate discovery”).

²²⁸ *In re Sur. Ass’n of Am.*, 388 F.2d 412, 414 (2d Cir. 1967) (citation & quotation marks omitted).

²²⁹ *Hofer v. Mack Trucks, Inc.*, 981 F.2d 377, 380 (8th Cir. 1992).

involved in the action are necessarily vague,” however, “and it is practically impossible to state a general rule by which they can be drawn[.]”²³⁰

The absence of clearly defined boundaries means that resolving disputes over relevance in civil discovery typically calls for an examination of analogous cases. To that end, the government has cited several decisions addressing the scope of civil discovery that, in its view, support the expansive concept of relevance embodied in the FISA court’s approval of the NSA’s telephone records program.²³¹ Some of these decisions simply are not germane, and none are sufficient to support that expansive definition.

The plaintiffs in *Goshawk Dedicated Ltd. v. Am. Viatical Servs., LLC*, two insurance companies, sought discovery from the defendant of “an underwriting database” maintained by the defendant that contained detailed actuarial data used by the defendant “in purchasing life insurance policies, in procuring insurance from Plaintiffs, and in analyzing whether its actuarial data was accurate.”²³² The defendant objected “that the database contains a significant amount of actuarial data not relevant to this litigation” — apparently meaning data that was not utilized in obtaining insurance from the plaintiffs. The defendant also contended “that the ‘methodologies, policies, and practices’ of its life expectancy evaluations are protected trade secrets and thus should not be subject to discovery.”²³³

The court rejected the defendant’s arguments as follows: “The problem with AVS’s contention is that its methodologies, policies, and practices of conducting life expectancy evaluations are themselves at the center of this litigation.” Stating that AVS’s legitimate confidentiality concerns were addressed through a confidentiality order, the court concluded that the database sought “is highly relevant to the claims and defenses in this litigation” and that “AVS has not come forth with a valid legal basis for resisting its disclosure.”²³⁴

The entire discussion in *Goshawk* is only three paragraphs long, and the court did not explicitly weigh in on whether, as the defendant maintained, the database truly “contain[ed] a significant amount of actuarial data not relevant to th[e] litigation.” But the court’s brief discussion suggests that it rejected the very notion that data relating to

²³⁰ *Food Lion, Inc. v. United Food & Commercial Workers Int’l Union, AFL-CIO-CLC*, 103 F.3d 1007, 1012 (D.C. Cir. 1997) (quoting 8 WRIGHT, MILLER & MARCUS, FEDERAL PRACTICE AND PROCEDURE: CIVIL 2d § 2008, at 105-06 (1994)).

²³¹ See Administration White Paper at 9-11.

²³² *Goshawk Dedicated Ltd. v. Am. Viatical Servs., LLC*, No. 05-2343, 2007 WL 3492762, at *1 (N.D. Ga. Nov. 5, 2007).

²³³ *Id.*

²³⁴ *Id.*

transactions with other insurers was immaterial. Such data revealed the defendant’s “methodologies, policies, and practices of conducting life expectancy evaluations,” which were “at the center” of the litigation.²³⁵

In other words, the court in *Goshawk* did not conclude that “searching the entire repository [was] the only feasible means to locate the critical documents.”²³⁶ It did not endorse the assertion that the database “contained a significant amount of irrelevant data”²³⁷ but order production nevertheless. Rather, the court appears to have concluded that *all* of the documents were critical, rejecting the premise that data pertaining to other insurers was irrelevant.

Another case cited by the government, *Chen-Oster v. Goldman, Sachs & Co.*, is even less on-point.²³⁸ In this gender-discrimination Title VII case, where former employees brought a putative class action against Goldman Sachs, the plaintiffs sought a discovery order requiring Goldman Sachs to extract certain human resources information from four separate and differently structured databases. The information was alleged to be “necessary for any statistical analysis of Goldman Sachs’ employment practices” at both the class-certification and merits stages.²³⁹ Goldman Sachs objected on proportionality grounds under Rule 26(b)(2)(C), citing the immense number of hours it would take to extract the requested information from its databases.²⁴⁰

The passage in this decision relied on by the government, which is not its holding, occurs during a discussion of less costly alternatives to the plaintiffs’ request. The court first floated the possibility of ordering Goldman Sachs to extract and analyze small samples from the database, but concluded that it lacked the expertise to unilaterally impose any particular technique on the parties.²⁴¹ “The other alternative — and one that the plaintiffs advocate — would require Goldman Sachs to produce in digital form all of the information contained in each of the databases. Goldman Sachs acknowledges that, at least in the short run, such a ‘data dump’ would impose less of a burden on it than a more targeted production.”²⁴² In the passage highlighted by the government, the court noted that “[t]here is no legal impediment to ordering production in that form,” but for pragmatic reasons the

²³⁵ *Id.*

²³⁶ Administration White Paper at 10.

²³⁷ Administration White Paper at 10 n.7.

²³⁸ *Chen-Oster v. Goldman, Sachs & Co.*, 285 F.R.D. 294 (S.D.N.Y. 2012).

²³⁹ *Id.* at 297.

²⁴⁰ *Id.* at 303-04.

²⁴¹ *Id.* at 304.

²⁴² *Id.* at 305.

court declined to order Goldman Sachs to proceed in this way.²⁴³ Instead, the court granted the plaintiffs' original request and ordered Goldman Sachs to extract the requested information from the databases.²⁴⁴

All that *Chen-Oster* provides, therefore, is a passing nod to the idea that civil plaintiffs can obtain compelled disclosure of an entire database from a defendant. And the plaintiffs in that case intended to analyze *all* of the information in those four databases, arguing that it was "relevant *in the aggregate* to perform the applicable analyses to show patterns of statistically significant shortfalls or effects of challenged policies."²⁴⁵

Chen-Oster cites two decisions in support of its observation that there was "no legal impediment" to ordering disclosure of a database. One is *Goshawk*, described above. The other is *High Point SARL v. Sprint Nextel Corp.*²⁴⁶

In *High Point*, a patent infringement case, one of the plaintiff's interrogatories asked Sprint to identify information about certain technical components within its cellular telephone network. In response, Sprint produced a spreadsheet drawn from its so-called "ATLAS" system, "the tool used by Sprint to comply with the internal control requirements of the Sarbanes–Oxley Act, as they relate to inventory and installed equipment."²⁴⁷ Sprint later produced a supplement to this spreadsheet, but the plaintiff notified Sprint that it thought this supplement was incomplete. Sprint then produced yet another supplemental spreadsheet. The plaintiff, High Point, told the court that it was "skeptical of how Sprint queried its ATLAS database given that each supplemental spreadsheet contained substantial new information." To address these concerns, High Point requested that Sprint be ordered to produce "the whole ATLAS database from which the report was generated."²⁴⁸

Sprint objected "that the ATLAS database in its entirety includes tremendous quantities of irrelevant information." Rejecting this argument, the court explained that "High Point has raised sufficient questions regarding whether Sprint's production of the spreadsheets generated from the ATLAS database includes all responsive information," and that "Sprint's only objection to this proposal appears to be that production of the database

²⁴³ *Id.*

²⁴⁴ *Id.*

²⁴⁵ *Id.* at 304 (emphasis in original); *see id.* at 305 (agreeing that "[t]he information in the databases is central to the plaintiffs' claims of gender discrimination in compensation, promotion, and evaluation").

²⁴⁶ *High Point SARL v. Sprint Nextel Corp.*, No. 09-2269, 2011 WL 4526770 (D. Kan. Sept. 28, 2011).

²⁴⁷ *High Point SARL*, 2011 WL 4526770, at *12.

²⁴⁸ *Id.*

would include large quantities of irrelevant information.” But “[t]his is not a persuasive argument against producing the ATLAS database.”²⁴⁹

In other words, the court in *High Point* ordered production of the entire database, irrelevant information and all, in response to specific facts undermining confidence that Sprint was querying the database in a manner that would retrieve all of the relevant information requested by its adversary. Only in that context did the court find disclosure of the entire database to be appropriate. Rather than constituting a statement on the scope of relevance, this opinion represents a court exercising its discretionary power to ensure fairness between adversaries and completeness of their mutual disclosures. Moreover, obtaining a database that includes “large quantities of irrelevant information” is different from obtaining one that consists nearly entirely of irrelevant information — much less all such databases.

In another case cited by the government, *Medtronic Sofamor Danek, Inc. v. Michelson*, “the parties [did] not seriously dispute the relevance of the electronic data at issue.”²⁵⁰ The question was who would be required to shoulder the considerable burden and cost of converting discoverable electronic data held by the plaintiff into a usable format.²⁵¹ The decision implicitly accepts that a party may request a “large volume of data” from the other party in discovery, and that such requests may return irrelevant materials along with those that prove to be relevant: it notes that the materials sought are relevant because they “may contain discoverable material, although neither party can estimate how much.”²⁵² Thus, the decision illustrates the basic proposition that civil litigants may request large numbers of records in discovery with the intention of sifting through them for those that support their case. But there is no suggestion that the likely proportion of relevant to irrelevant material in that case even approached that in the NSA’s Section 215 program. Indeed, the parties “could not estimate” how much discoverable material was within the request. In contrast, the government knows in advance that virtually everything produced in response to the FISA court’s orders will be irrelevant.

The last case cited by the government, *In re Adelpia Commc’ns Corp.* has nothing to do with the permissible breadth of discovery or the meaning of the word “relevance.”²⁵³ There, the party seeking discovery wanted production of *fewer* documents, not more, and the court noted that it “does not endorse a method of document production that merely

²⁴⁹ *Id.*

²⁵⁰ *Medtronic Sofamor Danek, Inc. v. Michelson*, 229 F.R.D. 550, 553 (W.D. Tenn. 2003).

²⁵¹ *Id.* at 552-53.

²⁵² *Id.* at 553.

²⁵³ *See In re Adelpia Commc’ns Corp.*, 338 B.R. 546 (Bankr. S.D.N.Y. 2005),

gives the requesting party access to a ‘document dump,’ with an instruction to the party to ‘go fish.’”²⁵⁴

In sum, it is clear that the “relevance” standard in civil discovery permits litigants to seek large batches of material even though *some* or even many of those materials may prove irrelevant. But the case law does not sanction requesting an entire class of records, without limit or any specific connection to the matter at hand, and with knowledge that only an infinitesimal portion of those records conceivably are pertinent.

2. Relevance and Grand Jury Subpoenas

The government has extraordinarily broad power to subpoena documents when investigating possible criminal activity with a grand jury. “The function of the grand jury is to inquire into *all information that might possibly bear on its investigation* until it has identified an offense or has satisfied itself that none has occurred. As a necessary consequence of its investigatory function, the grand jury paints with a broad brush.”²⁵⁵ Accordingly, a grand jury investigation “is not fully carried out until *every available clue has been run down* and all witnesses examined in every proper way to find if a crime has been committed.”²⁵⁶ The scope of its inquiry “is not to be limited narrowly by questions of propriety or forecasts of the probable result of the investigation, or by doubts whether any particular individual will be found properly subject to an accusation of crime.”²⁵⁷ When a subpoena is challenged on relevancy grounds, therefore, “the motion to quash must be denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury’s investigation.”²⁵⁸ After all, “the decision as to what offense will be charged is routinely not made until after the grand jury has concluded its investigation,” and “[o]ne simply cannot know in advance whether information sought

²⁵⁴ *Id.* at 551. In *Adelphia*, a bankruptcy trust conducting discovery against certain defendants objected when the defendants proposed to comply by “making their warehoused document archive available for inspection” by the trust — an archive containing “approximately 20,000 large bankers boxes of business records as well as over 600 boxes of business records deemed relevant to the various investigations underway.” The trust argued that Rule 34 does not allow production of requested materials “in the midst of a large quantity of un-requested, non-responsive materials.” *Id.* at 549. Instead, the trust argued that the defendants, rather than the trust, “should be forced to cull through the boxes and produce responsive documents.” *Id.* at 553. The court sided with the defendants, but on the condition that “any archived documents produced must be thoroughly indexed, the boxes accurately labeled and the depository kept in good order.” *Id.* at 551. A “document dump,” with instructions to “go fish,” was “emphatically not the situation presented to the Court in this matter,” where the defendants’ archive was “an orderly facility with neatly stacked rows of boxes organized by department and labeled as to content[.]” *Id.*

²⁵⁵ *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 297 (1991) (emphasis added).

²⁵⁶ *Id.* (quoting *Branzburg v. Hayes*, 408 U.S. 665, 701 (1972) (emphasis added)).

²⁵⁷ *Branzburg*, 408 U.S. at 688 (quoting *Blair*, 250 U.S. at 282).

²⁵⁸ *R. Enterprises, Inc.*, 498 U.S. at 301.

during the investigation will be relevant and admissible in a prosecution for a particular offense.”²⁵⁹

“The investigatory powers of the grand jury are nevertheless not unlimited. Grand juries are not licensed to engage in arbitrary fishing expeditions, nor may they select targets of investigation out of malice or an intent to harass.”²⁶⁰ While a grand jury need not restrict its inquiry to admissible evidence, the Fourth Amendment “provides protection against a grand jury subpoena duces tecum too sweeping in its terms ‘to be regarded as reasonable.’”²⁶¹ And where a grand jury subpoena implicates the freedom of speech or association, some courts have required the government to demonstrate “a compelling interest in and a sufficient nexus between the information sought and the subject matter of its investigation.”²⁶² “In sum, the fact that grand juries must have broad investigative powers does not resolve all questions of the permissible breadth and requisite specificity of a subpoena duces tecum.”²⁶³

To determine what might be the outer limits of a grand jury subpoena, we have examined both the cases cited by the government and others. There has never been a grand jury subpoena as broad as the FISA court’s Section 215 orders. And contrary to the government’s suggestion, the case law does not hold that the breadth of a grand jury subpoena is unlimited, but rather that a subpoena must be designed to address the circumstances of a specific investigation.

One decision, *In re Grand Jury Proceedings*, merely explains that district courts assessing the relevance of subpoenaed materials should not proceed “document-by-

²⁵⁹ *Id.* at 300; see *United States v. Triumph Capital Grp., Inc.*, 544 F.3d 149, 168 (2d Cir. 2008) (“[S]ubpoenas *duces tecum* are often drawn broadly, sweeping up both documents that may prove decisive and documents that turn out not to be. This practice is designed to make it unlikely that a relevant document will escape the grand jury’s notice.”); 3 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE, § 8.8(b) (3d. ed.) (explaining that “the nature of the criminal activity [the grand jury] seeks to investigate often requires consideration of a substantial amount of information that will prove in the end to be irrelevant”); 1 SARA SUN BEALE ET AL., GRAND JURY LAW AND PRACTICE § 6:21 (2d ed.) (noting that relevancy objections “are almost universally overruled”).

²⁶⁰ *R. Enterprises, Inc.*, 498 U.S. at 299 (internal citations omitted); see *In re Grand Jury Proceedings*, 616 F.3d 1186, 1203 (10th Cir. 2010) (explaining that “fishing is permissible so long as it is not an *arbitrary* fishing expedition” (emphasis in original)); *Gher v. Dist. Court In & For Adams Cnty.*, 516 P.2d 643, 644 (Colo. 1973) (quashing grand jury subpoena where district attorney attempted to use it as means of developing facts relating to municipal dispute that did not involve “any possible violation of criminal laws”).

²⁶¹ *United States v. Dionisio*, 410 U.S. 1, 11 (1973) (quoting *Hale v. Henkel*, 201 U.S. 43, 76 (1906)).

²⁶² *In re Grand Jury Subpoenas Duces Tecum*, 78 F.3d 1307, 1312 (8th Cir. 1996) (citing *In re Grand Jury Proceeding*, 842 F.2d 1229 (11th Cir. 1988), & *Glass v. Heyd*, 457 F.2d 562 (5th Cir. 1972)); accord *Burse v. United States*, 466 F.2d 1059, 1083 (9th Cir. 1972)).

²⁶³ *In re Grand Jury Subpoena: Subpoena Duces Tecum*, 829 F.2d 1291, 1297 (4th Cir. 1987); see *Dionisio*, 410 U.S. at 11 (“This is not to say that a grand jury subpoena is some talisman that dissolves all constitutional protections.”).

document,” but should instead evaluate whether each “broad category” of requested materials could contain possibly relevant documents. The former approach would “unduly disrupt the grand jury’s broad investigatory powers” and force the government “to justify the relevancy of hundreds or thousands (or more) of individual documents, which it has not yet even seen[.]” Often the government “is not in a position to establish the relevancy with respect to specific documents,” because “it may not know the precise content of the requested documents” and “it may not know precisely what information is or is not relevant at the grand jury investigative stage.”²⁶⁴ Accepting the “incidental” production of irrelevant documents, when measured by the hundreds or thousands, does not support the legitimacy of the Section 215 calling records program, in which the NSA potentially collects billions of records per day with full knowledge that virtually all of them are irrelevant.²⁶⁵

The broadest grand jury subpoena that the government cites is *In re Grand Jury Proceedings: Subpoenas Duces Tecum*.²⁶⁶ In that case, the Eighth Circuit upheld grand jury subpoenas for the records of all wire money transfers exceeding \$1,000 sent during a two-year period from a Western Union office at the Royale Inn in Kansas City, Missouri.

In rejecting the claim that the subpoenas were overbroad, the court stressed that only a single Western Union office was involved, and the “type of documents sought [was] precisely limited to those recording transactions of one thousand dollars or more occurring within a relatively short period of time.”²⁶⁷ As the decision explained, specific facts known to investigators pointed to the Royale Inn office as a focal point for illegitimate, drug-related money transfers.²⁶⁸

²⁶⁴ *In re Grand Jury Proceedings*, 616 F.3d 1186, 1200-03 (10th Cir. 2010); see also *Triumph Capital Group, Inc.*, 544 F.3d at 168 (“Grand jury subpoenas *duces tecum* are customarily employed to gather information and make it available to the investigative team of agents and prosecutors so that it can be digested and sifted for pertinent matter. Before the subpoenas are issued, the government often does not have at its disposal enough information to determine precisely what information will be relevant.”).

²⁶⁵ *In re Grand Jury Proceedings*, 616 F.3d at 1204-05.

²⁶⁶ *In re Grand Jury Proceedings: Subpoenas Duces Tecum*, 827 F.2d 301 (8th Cir. 1987).

²⁶⁷ *Id.* at 304. The court also relied on the presumption of regularity that attaches to grand jury subpoenas, and that “one challenging a grand jury subpoena has the burden of showing irregularity.” *Id.* at 304. This presumption distinguishes the grand jury context from Section 215, where the government bears an initial burden of providing a statement of facts showing reasonable grounds to believe that the items it seeks are relevant. See 50 U.S.C. § 1861(b)(2)(A).

²⁶⁸ See *id.* at 302 (“In particular, the agent’s affidavit stated that he had learned ‘from numerous sources that drug dealers are using Western Union to transfer funds from Kansas City to various locations including Florida, California, and out of the country.’ Further, the affidavit states that the agent had received information from the Kansas City, Missouri, Police Department that its Drug Enforcement Unit had discovered completed Western Union Money Transfer Applications during a search of ‘dope houses’ in the inner city. Jamaican nationals apparently operated these houses, and the applications revealed that funds were transmitted to the Miami area and Jamaica, both ‘well known centers of narcotics trafficking.’ The funds involved were wired from the Royale Inn.”).

The court emphasized that it was “upholding the subpoenas only as against the fourth amendment and Federal Communications Act challenges” brought by Western Union, pointedly mentioning that nothing would bar the trial court, upon proper motion, from “limiting the subpoenas to matters having a greater degree of general relevance to the subject matter of the investigation.”²⁶⁹ Noting that the government already knew what types of documents it was seeking (“records of wire transfers by numerous individuals to various points around the country”), the Eighth Circuit even suggested that the trial court “may therefore wish to consider the extent to which the government would be able to identify in advance those patterns or characteristics that would raise suspicion. These might include wire transfers to or from individual suspects, transfers to certain locales known to be sources of high volumes of illegal drugs, or other particular patterns designed to focus on illegal activity without taking in an unnecessary amount of irrelevant material.”²⁷⁰ Such an inquiry, the court said, “is appropriate to protect against unduly encroaching upon the expectations of innocent customers that their financial records will be kept confidential.”²⁷¹

The Western Union case does not support the expansive theory of relevance advanced in favor of the NSA’s calling records program. Even where the government’s request was limited to transactions over \$1,000, during a limited period of time, in a single office that had a demonstrable connection to specific unlawful activity, the court still was concerned about the potentially unreasonable scope of the subpoenas and inadequate showing of relevance, and it offered suggestions on how to narrow even those subpoenas. The aspects of the subpoenas that the Eighth Circuit found troubling are multiplied exponentially under the NSA’s calling records program, which collects the entire nation’s calling records, for an indefinite period of time (renewed every ninety days since May 2006), based only on the fact that terrorists use telephones.

3. Relevance and Administrative Subpoenas

The closest analogue to the power conferred by Section 215 is the administrative subpoena. Indeed, Congress crafted Section 215 as a substitute for the administrative subpoena authority sought by the Administration after the 9/11 attacks.²⁷²

An administrative agency may conduct an investigation even though it lacks probable cause to believe that any particular statute is being violated. Like a grand jury, it can “investigate merely on suspicion that the law is being violated, or even just because it

²⁶⁹ *Id.* at 305.

²⁷⁰ *Id.* at 305-06.

²⁷¹ *Id.* at 306.

²⁷² *See* H.R. Rep. No. 107-236(I), at 61 (2001).

wants assurance that it is not.”²⁷³ The relevance requirement for administrative subpoenas derives from the statutes authorizing such subpoenas, inherent limits on the powers of administrative agencies, and the reasonableness requirement of the Fourth Amendment.²⁷⁴ “Although ‘a governmental investigation . . . may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power, it is sufficient if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant.’”²⁷⁵

Therefore, “to be valid, an administrative subpoena must seek information that is ‘reasonably relevant’ to the ‘general purposes of the agency’s investigation.’”²⁷⁶ As with grand jury subpoenas, the materials sought “need only be relevant to the *investigation* — the boundary of which may be defined quite generally.”²⁷⁷ This relevance determination “cannot be reduced to formula; for relevancy and adequacy or excess in the breadth of the subpoena are matters variable in relation to the nature, purposes and scope of the inquiry.”²⁷⁸ Courts generally “defer to the agency’s appraisal of relevancy,”²⁷⁹ and some have said that, to be outside the bounds of a subpoena, information sought must be “plainly incompetent or irrelevant to any lawful purpose” of the agency.²⁸⁰

²⁷³ *United States v. Constr. Products Research, Inc.*, 73 F.3d 464, 470 (2d Cir. 1996) (quoting *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950)); see *United States v. Powell*, 379 U.S. 48, 57 (1964); *Oklahoma Press Publishing Co.*, 327 U.S. at 201.

²⁷⁴ In *United States v. Powell*, which addressed the scope of the IRS Commissioner’s subpoena power, the Supreme Court first articulated a standard that has since been applied to administrative subpoenas generally: the Commissioner was required to “show that the investigation will be conducted pursuant to a legitimate purpose, that the inquiry *may be relevant to the purpose*, that the information sought is not already within the Commissioner’s possession, and that the administrative steps required by the Code have been followed.” *Powell*, 379 U.S. at 57-58 (emphasis added); see *SEC v. Jerry T. O’Brien, Inc.*, 467 U.S. 735, 741-42 (1984) (characterizing these four requirements as “the general standards governing judicial enforcement of administrative subpoenas”); *Constr. Products Research, Inc.*, 73 F.3d at 471 (applying standards to evaluate reasonableness of Nuclear Regulatory Commission subpoena).

²⁷⁵ *United States v. Gurley*, 384 F.3d 316, 321 (6th Cir. 2004) (quoting *Morton Salt Co.*, 338 U.S. at 652 (internal citation omitted)).

²⁷⁶ *In re Sealed Case (Admin. Subpoena)*, 42 F.3d 1412, 1419 (D.C. Cir. 1994) (quoting *Linde Thomson Langworthy Kohn & Van Dyke, P.C. v. Resolution Trust Corp.*, 5 F.3d 1508, 1516 (D.C. Cir. 1993)); accord *In re McVane*, 44 F.3d 1127, 1135 (2d Cir. 1995); *NLRB v. Line*, 50 F.3d 311, 314 (5th Cir. 1995).

²⁷⁷ *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1090 (D.C. Cir. 1992) (emphasis in original).

²⁷⁸ *Oklahoma Press Pub. Co.*, 327 U.S. at 208-09; see, e.g., *FTC v. Turner*, 609 F.2d 743, 745 (5th Cir. 1980) (“The relevance of an F.T.C. subpoena request is measured against the purpose and scope of its investigation.”).

²⁷⁹ *In re Sealed Case*, 42 F.3d at 1419; see *RNR Enterprises, Inc. v. SEC*, 122 F.3d 93, 97 (2d Cir. 1997) (“We defer to the agency’s appraisal of relevancy, which must be accepted so long as it is not obviously wrong.”).

²⁸⁰ *Constr. Products Research, Inc.*, 73 F.3d at 472 (quoting *Endicott Johnson*, 317 U.S. at 509).

Courts must “be careful,” however, not to make relevance requirements “a nullity.”²⁸¹ It is not a valid purpose of a subpoena, for instance, to investigate “other wrongdoing, as yet unknown,” because such a broad mandate “makes it impossible . . . to determine whether the information demanded is ‘reasonably relevant.’”²⁸² And while the standards governing the permissible scope of administrative subpoenas are broad, they are not as expansive as the government suggests.²⁸³

Because the relevance standard governing administrative subpoenas “cannot be reduced to formula” and varies along with “the nature, purposes and scope” of an investigation, here too recourse must be had to precedent involving analogous factual scenarios.²⁸⁴ And here, once again, the case law fails to buttress the legitimacy of the NSA’s telephone records program.

²⁸¹ *EEOC v. Shell Oil Co.*, 466 U.S. 54, 69 (1984); *see id.* at 72 (rejecting argument that “would render nugatory the statutory limitation of the Commission’s investigative authority to materials ‘relevant’ to a charge”).

²⁸² *In re Sealed Case*, 42 F.3d at 1418.

²⁸³ The government has suggested that the relevance standard in the administrative subpoena context “affords an agency ‘access to virtually any material that might cast light on the allegations’ at issue in an investigation.” Administration White Paper at 9 (quoting *Shell Oil Co.*, 466 U.S. at 68-69). But the passage quoted from *Shell Oil* was addressed to subpoenas issued by the Equal Employment Opportunity Commission (“EEOC”), which fundamentally differ from most administrative subpoenas, because they confer access to materials only in connection with a specific charge of a violation that already has been filed. *See Shell Oil Co.*, 466 U.S. at 64 (“[T]he EEOC’s investigative authority is tied to charges filed with the Commission; unlike other federal agencies that possess plenary authority to demand to see records relevant to matters within their jurisdiction, the EEOC is entitled to access only to evidence ‘relevant to the charge under investigation.’” (quoting 42 U.S.C. § 2000e-8(a))). Other administrative subpoena statutes, similar to Section 215, permit discovery of materials relevant to *investigations*, which may not yet have coalesced around specific allegations or particular individuals. Thus, the broad standard articulated in *Shell Oil* — “virtually any material that might cast light on the allegations” — is from an anomalous context where the subpoena’s breadth is circumscribed by its link to specific charges already filed. *See EEOC v. Randstad*, 685 F.3d 433, 448 (4th Cir. 2012) (“Once a charge has placed the Commission on notice *that a particular employer is (or may be) violating Title VII or the ADA in a particular way*, the Commission may access ‘virtually any material that might cast light on the allegations against the employer.’” (quoting *Shell Oil Co.*, 466 U.S. at 68-69) (emphasis added)).

Similarly, the government has quoted a phrase from *United States v. Arthur Young & Co.*, 465 U.S. 805, 814 (1984), indicating that the IRS Secretary may obtain items “of even *potential* relevance to an ongoing investigation.” Administration White Paper at 10. But the Court in *Arthur Young* was merely explaining that “an IRS summons is not to be judged by the relevance standards used in deciding whether to admit evidence in federal court,” and it used the adjective “potential” to acknowledge that the IRS “can hardly be expected to know whether such data will in fact be relevant until it is procured and scrutinized.” The agency, therefore, “should not be required to establish that the documents it seeks are actually relevant in any technical, evidentiary sense.” *Arthur Young & Co.*, 465 U.S. at 814. The Court’s use of the phrase “potential relevance” here merely reaffirms the principles described earlier — that the government cannot always know in advance whether material is truly pertinent. It does not negate the more demanding requirement that “the information sought is *reasonably* relevant.” *California Bankers Ass’n v. Shultz*, 416 U.S. 21, 67 (1974) (quoting *Morton Salt Co.*, 338 U.S. at 652-53 (emphasis added)).

²⁸⁴ *Oklahoma Press Pub. Co.*, 327 U.S. at 209.

For example, the government quotes passages from *Carrillo Huettel, LLP v. SEC* that appear to echo the NSA's rationale for obtaining bulk calling records. On closer examination, the similarity does not bear out. In *Carrillo*, the SEC subpoenaed the bank records of one law firm, requesting all of its trust account information over a two-year period. The request covered financial records not just for the firm's forty-two clients already identified by the SEC as possibly implicated in the securities investigation, but the records for "all its clients," of whom "100 or more" had not yet been identified or tied in any way to the investigation. Despite Carillo's argument "that the subpoena will result in the production of financial records of many clients that are irrelevant to the investigation at issue," the court enforced the subpoena.²⁸⁵

Two circumstances distinguish *Carillo*. First, the SEC was investigating not only the law firm's clients but the firm itself — that is, the subpoena was issued to the target of the SEC's investigation, unlike the situation with respect to the telephone companies covered by the NSA's program. The SEC had "obtained evidence" that Carillo not only represented the entities and individuals being investigated but "may also be actively involved in the alleged violations."²⁸⁶ And this was the context in which the SEC argued that it "cannot effectively trace money through accounts without having records of all transactions," and that these records "may reveal concealed connections between unidentified entities and persons and those identified in the investigation thus far."²⁸⁷ The government's request was limited to a category of records — those of the Carillo firm — that it had a cognizable reason to suspect as a whole.

The second difference is in the proportion of relevant to irrelevant materials expected to be produced. Of the law firm's roughly 150 clients, nearly a third had already been directly tied to the investigation. On the basis of these facts, the court determined that, "[o]n balance," the subpoena satisfied the relevancy requirement: "Although not *every* responsive document produced . . . may be relevant," the court reasoned, "there is reason to believe that the records *overall* contain information relevant to the investigation."²⁸⁸ This conclusion was simply an application of the principle that a subpoenas duces tecum can be valid even if it may return some irrelevant materials — not that it can be valid where virtually *all* of the requested materials will be irrelevant.

In another case, *In re Subpoena Duces Tecum*, the government successfully compelled a doctor suspected of health care fraud to produce more than 15,000 patient files, "consisting of between 750,000 and 1.25 million pages of material," in spite of the

²⁸⁵ *Carrillo Huettel, LLP v. SEC*, No. 11-65, 2011 WL 601369, at *1-2 (S.D. Cal. Feb. 11, 2011).

²⁸⁶ *Id.* at *1; *see id.* at *2 ("The SEC contends that Carrillo's own conduct is at issue.").

²⁸⁷ *Id.*

²⁸⁸ *Id.* (emphasis added).

doctor's relevancy objection. The court explained that the "sheer volume of documents" could not be the sole criterion of reasonableness, and noted that the doctor had rejected the government's offer of accommodation under which he could maintain many of the files, subject to the U.S. Attorney expressing a need to review them.²⁸⁹ The court also noted the government's argument "that it would be 'an oddity of jurisprudence' if a physician with a high-volume, government-subsidized practice could avoid complying with such subpoenas, whereas a physician with a lower volume and therefore with a narrower potential scope of fraud would have to comply," while observing that "to define the reasonableness of a subpoena based on the volume of items identified for production would be to require the government to ascertain, before issuing a subpoena, the extent of any wrongdoing. But ascertaining the extent of wrongdoing is itself a primary purpose for the issuance of the subpoena."²⁹⁰

Like *Carillo*, this decision shows that volume alone does not doom a subpoena's validity, and that some amount of over-collection is an inevitable byproduct of government investigations. But as in *Carillo*, the subpoena sought the records of an entity that was itself under investigation, and its broad reach reflected the government's desire to investigate this entity's conduct vis-à-vis the third parties to whom the records pertained. In both cases, the government's request was defined, and limited, by the facts of the investigation at hand. And in both cases the government had an articulable reason to suspect that the category of records it sought, so defined, would include a significant proportion of records pertinent to the investigation. These cases might support collecting all of a telephone company's calling records if, for instance, the company was suspected of fraudulently overbilling its customers — not because some of those customers might later turn out to be associated with an unrelated crime.

In sum, precedent involving relevance in the administrative subpoena context simply teaches the same lessons evident in the grand jury and civil discovery contexts, lessons that do not support the unbounded definition of relevance embodied in the FISA court's approval of the Section 215 program.²⁹¹

²⁸⁹ *In re Subpoena Duces Tecum*, 228 F.3d 341, 345, 350-51 (4th Cir. 2000).

²⁹⁰ *Id.* at 350-51.

²⁹¹ The government also has cited two decisions for the proposition that "[f]ederal agencies exercise broad subpoena powers or other authorities to collect and analyze large data sets in order to identify information that directly pertains to the particular subject of an investigation." Administration White Paper at 10 (citing *F.T.C. v. Invention Submission Corp.*, 965 F.2d at 1090, and *Associated Container Transp. (Australia) Ltd. v. United States*, 705 F.2d 53, 58 (2d Cir. 1983)). That broad proposition, and the cases cited, do not involve anything like the NSA's telephone records program — in which all records of a particular type are collected indiscriminately and preemptively in order to facilitate later searches of an infinitesimal fraction of those records. Similarly, the government has invoked decisions involving warrants that permit computer hard drives to be copied and later searched for incriminating evidence, *see id.* at 10-11, but these cases, involving seizures based on a finding of probable cause, have little bearing on the meaning of "relevance."

4. Expanding Relevance Beyond its Normal Legal Meaning

As illustrated above, precedent from other legal contexts involving the production of records does not support a concept of relevance like the one proffered by the government in support of the NSA's bulk calling records program. To be sure, the case law regarding civil discovery, grand jury subpoenas, and administrative subpoenas shows that relevance is interpreted broadly, and that incidental production of unrelated materials is accepted as essential to enable fulsome investigative efforts. Standards of relevance thus permit parties and the government to engage in a degree of fishing, so long as it is not arbitrary or in bad faith. But the case law makes equally clear that the definition of relevance is not boundless. And no case that we have found supports the interpretation of relevance embodied in the NSA's program.

Tacitly acknowledging that case law from analogous contexts is not adequate to support its position, the government suggests that Section 215 calls for "an even more flexible standard" of relevance.²⁹² But none of the government's arguments, in our view, supports a definition of "relevant" as broad as the one the government proffers.

First, had Congress wished to inscribe a standard of relevance in Section 215 even less exacting than those developed in analogous legal contexts, it could have done so. But contemporary statements from legislators, highlighted by the government itself, evince an intent to match Section 215 to the standards used in those contexts.²⁹³ The reference to grand jury subpoenas added to the statute in 2006 was meant to reassure those with concerns about the scope of Section 215 that the statute was consistent with practice in other fields.²⁹⁴

Second, the fact that Section 215 requires only "reasonable grounds to believe" that records sought are relevant to an "investigation," as the government emphasizes, does not call for a different standard of relevance than the one used in all other contexts.²⁹⁵ By demanding only "reasonable grounds to believe," rather than certainty, that items sought are relevant to an investigation, the statute ensures that Section 215 is consistent with the analogous civil and criminal contexts — where the requester need not show that every item sought *actually* is relevant in an evidentiary sense, but merely that the items

²⁹² See Administration White Paper at 11-13.

²⁹³ See Defendants' Memorandum of Law, *ACLU v. Clapper*, at 23 (citing 152 Cong. Rec. S1598, 1606 (Mar. 2, 2006) (statement of Sen. Kyl) ("We all know the term 'relevance.' It is a term that every court uses The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation, and for each and every one of the 335 different administrative subpoenas currently authorized by the United States Code.")).

²⁹⁴ See 50 U.S.C. § 1861(c)(2)(D).

²⁹⁵ See 50 U.S.C. § 1861(b)(2)(A).

reasonably may be. The statute's reference to a reasonable *belief* about the items requested shows that it contemplates the same scenario faced in the subpoena and discovery arenas: the government seeks a category of items that it reasonably suspects, but cannot be sure, includes material pertinent to its investigation. That scenario, and the legal standards that govern it, still require some factual correlation between the category of documents defined by the government and the circumstances of the investigation for which they are sought. Indeed, Section 215's requirement of a "statement of facts" supporting the government's belief underscores the importance of that context-specific inquiry.

Thus, even if the qualifier "reasonable grounds to believe" imposes a lower burden of proof on the government than if the statute simply authorized production of "relevant" documents, Section 215 still embodies the assumption that specific facts will link the government's investigation to the particular group of records it seeks. That assumption is incompatible with a continuously renewed request for the daily acquisition of all records of a particular type.

Third, the unique characteristics of national security investigations do not warrant interpreting "relevance" expansively enough to support the NSA's program. The government argues, and we agree, that the scope of relevance varies based on the nature of the investigation to which it is applied.²⁹⁶ Accordingly, the government cites the "remarkable breadth" of the national security investigations with which Section 215 is concerned, as contrasted with ordinary criminal matters, and emphasizes that these investigations "often focus on *preventing* threats to national security from causing harm, not on the retrospective determination of liability or guilt for prior activities."²⁹⁷

These valid distinctions, in our view, simply mean that the government will be able to make qualitative showings of relevance more often in national security investigations than in others. Because the government is investigating a broader scope of actors, over a longer period of time, across a wider geographic range, and before any specific offense has been committed, more information can be expected to be legitimately relevant to its efforts. Such considerations do not call for the wholesale elimination of relevance as a meaningful check on the government's acquisition of items.

Finally, the heightened importance of counterterrorism investigations, as compared with typical law enforcement matters, does not alter the equation. Items either are relevant to an investigation or they are not — the significance of that investigation is a separate matter. No matter how critical national security investigations are, therefore, *some* articulable principle must connect the items sought to those investigations, or else the

²⁹⁶ See Administration White Paper at 11.

²⁹⁷ Administration White Paper at 12.

word “relevant” is robbed of meaning. Congress added a relevance requirement to Section 215 in 2006 knowing full well that the statute governs national security investigations. It cannot, therefore, have meant for the importance of such investigations to efface that requirement entirely.²⁹⁸

In sum, we find the government’s interpretation of the word “relevant” in Section 215 to be unsupported by legal precedent and a subversion of the statute’s manifest intent to place *some* restriction, albeit a generous and flexible one, on the scope of the items that can be acquired under its auspices.²⁹⁹

IV. Prospective Orders for Daily Disclosure of New Telephone Records

Every FISA court order renewing the bulk telephone records program puts telephone companies under a continuing obligation, over a period of ninety days, to provide the NSA with their newly generated calling records on a daily basis. In other words, when telephone companies receive an order from the FISA court, they are not directed to turn over whatever calling records they have in their possession at the time. Instead, every day for the next ninety days after receiving the order, they must furnish the NSA with the new calling records generated that day by their customers.

This arrangement differs from the normal practice that characterizes discovery between parties and the production of records in response to a subpoena. Typically, persons who receive a subpoena or court order must hand over documents already in their possession by a given date. They are not required to supply newly generated documents on a regular basis for a set period of time. Nor is this arrangement akin to the rolling production schedules sometimes approved by courts for the disclosure of records.³⁰⁰ Rolling schedules merely dictate when documents that are already in existence must be made available to the opposing party, allowing the disclosures to be spread over a period of

²⁹⁸ Congress amended Section 215 to clarify that there must be reasonable grounds to believe that records obtained under the statute are “relevant to” an investigation, not merely sought “for” an investigation; it further required “a statement of facts” supporting that belief. *See* 50 U.S.C. § 1861(b)(2)(A). It inserted the concept of “relevance” into the statute not to broaden it, but to reassure those with concerns that the statute was tethered to concepts well known in other areas.

²⁹⁹ In analyzing the concept of relevance under Section 215, both the government and the FISA court have also cited the oversight mechanisms inscribed in the statute and devised for the bulk telephone records program that are not found in the analogous contexts of criminal or administrative subpoenas. *See* Administration White Paper at 13; Amended Memorandum Opinion at 23. We do not see how these oversight mechanisms bear on whether items are relevant to an authorized investigation.

³⁰⁰ *See, e.g., Global Client Solutions, LLC v. Executive Risk Indem., Inc.*, No. 13-0035, 2013 WL 4482992, at *1 (N.D. Okla. Aug. 19, 2013); *Prism Technologies, LLC v. Research in Motion, Ltd.*, No. 08-0537, 2010 WL 1254940, at *2 (D. Neb. Mar. 24, 2010); *In re September 11 Litig.*, 236 F.R.D. 164, 167 (S.D.N.Y. 2006).

time. That concession to the limits of human resources fundamentally differs from establishing an ongoing daily obligation to furnish new materials as they are created.

The government has offered a statutory defense of this practice.³⁰¹ But we conclude that it contravenes Section 215 for three reasons. First, the statute does not purport to authorize such orders, and case law involving the production of records in analogous contexts indicates that such authority cannot be inferred from statutory silence. Second, the text of Section 215 strongly suggests that it contemplates only the acquisition of items that already are in existence at the time the court issues an order. Third, interpreting Section 215 to permit the prospective collection of *telephone records* renders superfluous another provision of FISA that directly authorizes such collection — circumventing the limitations associated with that other provision and violating the interpretive principle that one provision in a statute should not be construed to make another superfluous.

For the reasons explained below, therefore, we believe that the language of Section 215 cannot support the government’s interpretation on this matter. In our view, acceptance of that interpretation plays a key role in transforming the function of Section 215 — from a means of gathering business records for intelligence investigations (in a manner similar to the use of subpoenas in other types of investigations) into an ongoing surveillance tool.

A. Absence of Express or Implied Authorization

No language in Section 215 purports to authorize the FISA court to issue orders requiring the ongoing daily production of records not yet in existence. The government does not contend that any such language exists. Instead, it emphasizes the lack of an explicit prohibition against such orders and argues that the prospective production of records has been deemed appropriate in analogous contexts.³⁰² While the government highlights case law from two contexts in support of that argument, neither supports the issuance of Section 215 orders that prospectively require the daily disclosure of new records as they are generated.

The first set of cases to which the government points arise in civil discovery, where a party has been directed by a subpoena to produce materials by a deadline, the so-called return date of the subpoena. As the government notes, “courts have held that the Federal Rules of Civil Procedure give a court the ‘authority to order [the] respondent to produce materials created after the return date of the subpoena.’”³⁰³

³⁰¹ See Administration White Paper at 16.

³⁰² See Administration White Paper at 16.

³⁰³ Administration White Paper at 16 (quoting *Chevron v. Salazar*, 275 F.R.D. 437, 449 (S.D.N.Y. 2011)).

These decisions, however, do not involve the type of obligation imposed by the FISA court under Section 215 — directing a party to produce as-yet-nonexistent records on an ongoing basis for a set period of time. Instead, they involve situations in which a party was ordered by the court to *supplement* its prior disclosures after the return date of a traditional subpoena. The decisions acknowledge that under Rule 26(e) of the Federal Rules of Civil Procedure, entitled “Supplementing Disclosures and Responses,” courts may order parties to supplement or correct their disclosures after the subpoena’s return date.³⁰⁴ And the decisions further recognize that the power “to order a respondent to supplement or correct its disclosure or response to a subpoena . . . includes the authority to order a respondent to produce materials created after the return date of the subpoena.”³⁰⁵ This conclusion rests on “the plain language” of Rule 26(e).³⁰⁶ At the time of a supplementary court order issued under Rule 26(e), therefore, the documents ordered to be produced already exist. They merely did not exist on the original date that disclosures were due.

All that these decisions illustrate, in other words, is that the civil rules contain a specific provision authorizing courts to order parties to *supplement or correct* their existing discovery responses, even after the return date of a subpoena. This does not imply that a valid subpoena may, in the first instance, require the ongoing daily production of newly generated records for the duration of a specified period. And therefore these decisions provide no basis for inferring that Section 215 implicitly authorizes the FISA court to impose such an obligation.

Second, the government discerns support for its position in decisions holding that a provision in the Stored Communications Act (“SCA”) permits orders for the prospective disclosure of records.³⁰⁷ These decisions involve the prospective disclosure of a particular type of telephone metadata — cell site location information. But the courts that have approved prospective orders for cell site location information have done so through a so-called “hybrid theory” that invokes “the combined authority of the Pen Register Statute and the Stored Communications Act.”³⁰⁸ Under this hybrid theory, the Pen Register and Trap

³⁰⁴ See FED. R. CIV. P. 26(e)(1)(B) (“A party who has made a disclosure under Rule 26(a) — or who has responded to an interrogatory, request for production, or request for admission — must supplement or correct its disclosure or response . . . as ordered by the court.”).

³⁰⁵ *Chevron*, 275 F.R.D. at 449 (citing *United States v. IBM Corp.*, 83 F.R.D. 92, 96 (S.D.N.Y. 1979) (internal quotation marks omitted)).

³⁰⁶ *IBM Corp.*, 83 F.R.D. at 96.

³⁰⁷ See Administration White Paper at 16 (citing *In re Application of the United States for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices*, 632 F. Supp. 2d 202, 207 n.8 (E.D.N.Y. 2008)).

³⁰⁸ *In re Application of United States for an order relating to Target Phone 2*, 733 F. Supp. 2d 939, 941 (N.D. Ill. 2009).

and Trace Statute³⁰⁹ provides the authority to install a pen register or trap and trace device that prospectively records call detail information. But because a different statute prohibits the acquisition of cell site location information “solely” under the pen register/trap and trace authority, courts must rely also “on some additional statutory authority when ordering the disclosure of prospective cell site information under the Pen Register Statute.”³¹⁰ Under the hybrid theory, the SCA serves as that additional authority, as it permits the government to obtain records from telephone companies and other electronic communications service providers.³¹¹ In accepting this hybrid theory, some courts have concluded that the language of the SCA is compatible with orders for the prospective disclosure of records as they are created.³¹² It is this conclusion to which the government points in support of its Section 215 argument.

Regardless of the merits of the hybrid theory — which “the majority of courts” have rejected³¹³ — it does not support the government’s argument regarding Section 215. To the contrary, it rebuts that argument.

First, the hybrid theory depends on the contribution of the pen register statute, which provides the affirmative authorization (and means) to collect telephone metadata prospectively. The SCA plays only the “supporting role” of allowing a particular *type* of data, cell site location information, to be included within that collection.³¹⁴ In the context of the NSA’s program, however, no companion statute is being used in combination with Section

³⁰⁹ 18 U.S.C. §§ 3121 *et seq.*

³¹⁰ *In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d 448, 454 (S.D.N.Y. 2006).

³¹¹ *See id.* (explaining the hybrid theory). The premise of this theory “is that the Stored Communications Act will be used in *combination with* the Pen Register Statute[.]” *Id.* at 459 (emphasis in original).

³¹² *See, e.g., Two Pen Register & Trap & Trace Devices*, 632 F. Supp. 2d at 207 & n.8 (“Because the SCA in no way limits the ongoing disclosure of records to the Government as soon as they are created, the cell-site information the Government seeks is subject to disclosure to the Government[.]”).

³¹³ *In re Application of U.S. for an order relating to Target Phone 2*, 733 F. Supp. 2d 939, 940 44 & n.1 (N.D. Ill. 2009) (citing decisions); *see Two Pen Register & Trap & Trace Devices*, 632 F. Supp. 2d at 204 (“Courts are divided, with a majority denying the Government’s requests.”). Courts in the majority have disagreed with the precise argument on which the government here relies — that the text of the SCA is compatible with prospective disclosure orders. *See In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006) (“A number of the magistrate judges to address this question have held that Section 2703, although it might cover historical cell site data, does not authorize the disclosure of such data on a ‘real-time’ or forward-looking basis.”) (citing decisions).

³¹⁴ *See Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 459 (“The Stored Communications Act is being asked to play only the supporting role of providing the required additional authorization for the disclosure of information already permitted by the Pen Register Statute.”).

215 to provide an affirmative source of authority for the prospective collection of records.³¹⁵

Second, merely because the SCA might be compatible with orders that prospectively require the disclosure of new records does not mean that Section 215 is compatible with such orders. Section 215 has its own unique language, which, as discussed below, suggests that it authorizes only the production of already existing records. And unlike the SCA, Section 215 is part of a broader statutory scheme under FISA that provides a framework for the prospective collection of telephone metadata when specific conditions are met; its language must be construed in that broader statutory context.³¹⁶

In sum, the case law discussed above offers no basis for discerning implied authority under Section 215 for prospective disclosure orders. The analogies cited by the government actually show that a statutory obligation to disclose business records is not enough to require the prospective, daily disclosure of such records. Some additional authority is needed, which is lacking here.

B. Language Suggesting Incompatibility with Prospective Orders

Apart from the lack of express or implied authority in Section 215 for orders that require the disclosure of newly created records prospectively, the text of the statute suggests that such orders are not within its scope. First, Section 215 permits the FISA court to issue orders “approving *the release* of tangible things.”³¹⁷ Approving an item’s *release* — “the act or an instance of liberating or freeing (as from restraint)”³¹⁸ — implies removing barriers to the disclosure of something that already exists.

More tellingly, a production order under Section 215 must “include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available.”³¹⁹ By referring to “the date,” in the singular, “on which” the tangible things must be provided, the statute suggests that the requested materials will be turned over on a single date — not “on an

³¹⁵ If statutory silence implied a grant of authority for prospective disclosure orders, then the SCA would *alone* permit the government to acquire a telephone company’s new calling records every day, making the government’s recourse to the hybrid theory unnecessary.

³¹⁶ Objections to the hybrid theory have been based on considerations unique to the language of the SCA, such as the requirement that records be “stored” and the statute’s definition of “electronic communication.” See *Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 459; *Two Pen Register & Trap & Trace Devices*, 632 F. Supp. 2d at 207; *Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 460. The dismissal of those objections by some courts sheds no light on the (different) language of Section 215, discussed below.

³¹⁷ 50 U.S.C. § 1861(c)(1) (emphasis added).

³¹⁸ MERRIAM WEBSTER ONLINE DICTIONARY (2013).

³¹⁹ 50 U.S.C. § 1861(c)(2)(B).

ongoing daily basis” for a period of ninety days.³²⁰ Furthermore, the fact that the statute permits a reasonable period of time in which the items “can be assembled and made available” further signals an expectation that the items already exist, but that time may be needed to marshal them for delivery.

Notably *absent* from Section 215 is any language for situations in which the items to be disclosed have not yet been created. Where Congress has expressly authorized prospective orders, either through electronic surveillance or the use of pen registers, it has set forth limits and procedures regarding the permissible scope and duration of those orders. Such limits and procedures are conspicuously missing from Section 215, indicating that Congress did not intend Section 215 to be used in this way.

C. Incompatibility with FISA as a Whole

Even if Section 215 were compatible with orders for the prospective disclosure of items that do not yet exist, orders requiring the daily disclosure of new *telephone calling records* are inconsistent with the structure of FISA as a whole. A different portion of that statute directly authorizes the prospective collection of telephony metadata through pen registers or trap and trace devices.³²¹ Construing Section 215 to permit ongoing acquisition of the very same data renders FISA’s pen register provision superfluous. It also allows the government to evade the limitations in that provision that govern such prospective monitoring.

Under FISA’s pen register provision, the government may apply for an order authorizing the installation and use of a pen register or trap and trace device in a counterterrorism investigation.³²² Such devices capture the same dialing, routing, and addressing information that is included in the calling records obtained by the NSA under Section 215 — the date, time, and duration of calls, along with the participating telephone numbers.³²³ Orders approving the use of these devices generally must be renewed after ninety days.³²⁴

³²⁰ Primary Order at 3, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-158 (Oct. 11, 2013) (“Primary Order”).

³²¹ See 50 U.S.C. § 1842.

³²² See 50 U.S.C. § 1842(a)(1).

³²³ See 18 U.S.C. § 3127(3), (4). FISA’s pen register provision also permits the government to request and obtain customer or subscriber information related to the telephone line or other facility to which the device is to be applied. See 50 U.S.C. § 1842(d)(2)(C). When the government obtains calling records under Section 215, however, it can obtain customer or subscriber information about particular numbers through several means under the Electronic Communications Privacy Act. See 18 U.S.C. § 2703(c).

³²⁴ See 50 U.S.C. § 1842(e)(1) (establishing ninety-day limit). If a government applicant certifies that the information likely to be obtained from the device is foreign intelligence information not concerning a U.S. person, orders may last up to a year. 50 U.S.C. § 1842(e)(2).

Construing Section 215 to authorize orders directing the daily transmission of the same information for ninety-day periods renders FISA's pen register provision redundant. "The Government's reading is thus at odds with one of the most basic interpretive canons, that '[a] statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant[.]'"³²⁵

Interpreting Section 215 in this way also circumvents language in FISA's pen register statute that restricts the use of such devices to individually targeted persons, telephone lines, or facilities. Orders issued under the auspices of the pen register provision must specify the identity, if known, of "the person" who is the subject of the investigation and the identity, if known, of "the person" to whom is leased or in whose name is listed "the telephone line or other facility" to which the pen register or trap and trace device is to be applied.³²⁶ Any order also must specify "the attributes of the communications to which the order applies," such as "the number or other identifier" for the account or phone line with which the device will be used.³²⁷

This language calls for a nexus between a government investigation and the particular telephone line or facility from which the government seeks to acquire telephony metadata. The government's interpretation of Section 215 renders that requirement a nullity, essentially permitting pen registers to be installed on every telephone line in the country, based on an expectation that this practice will, in the aggregate, produce information that is relevant to the government's investigations. Because Section 215 must be construed so as to be in harmony with FISA as a whole, such an interpretation is unsustainable.

V. Acquisition of Records by the NSA

Under the Section 215 bulk telephone records program, the NSA acquires a massive number of calling records from telephone companies each day, potentially including the records of every call made across the nation. Yet Section 215 does not authorize the NSA to acquire anything at all. Instead, it permits the FBI to obtain records for use in its own investigations. If our surveillance programs are to be governed by law, this clear

³²⁵ *Corley v. United States*, 556 U.S. 303, 314 (2009) (quoting *Hibbs v. Winn*, 542 U.S. 88, 101 (2004)); see *Marx v. Gen. Revenue Corp.*, 133 S. Ct. 1166, 1178 (2013) (stating that "the canon against surplusage is strongest when an interpretation would render superfluous another part of the same statutory scheme"). Although "[t]here are times when Congress enacts provisions that are superfluous," *Corley*, 556 U.S. at 325 (Alito, J., dissenting), there is no reason to suspect that Congress intended such redundancy here.

³²⁶ 50 U.S.C. § 1842(d)(2)(A)(i), (ii).

³²⁷ 50 U.S.C. § 1842(d)(2)(A)(iii).

congressional determination about which federal agency should obtain these records must be followed.

Section 215 expressly allows only the FBI to acquire records and other tangible things that are relevant to its foreign intelligence and counterterrorism investigations. Its text makes unmistakably clear the connection between this limitation and the overall design of the statute. Applications to the FISA court must be made by the director of the FBI or a subordinate.³²⁸ The records sought must be relevant to an authorized FBI investigation.³²⁹ Records produced in response to an order are to be “made available to,” “obtained” by, and “received by” the FBI.³³⁰ The Attorney General is directed to adopt minimization procedures governing the FBI’s retention and dissemination of the records it obtains pursuant to an order.³³¹ Before granting a Section 215 application, the FISA court must find that the application enumerates the minimization procedures that the FBI will follow in handling the records it obtains.³³²

These features of the statute are bound up with its purpose. As the government acknowledges: “Section 215 was enacted because the FBI lacked the ability, in national security investigations, to seek business records in a way similar to its ability to seek records using a grand jury subpoena in a criminal case or an administrative subpoena in civil investigations.”³³³ Because records sought under Section 215 must be requested by FBI officials, on the grounds that they are relevant to FBI investigations, and with promises made about the procedures that the FBI will follow in handling them, those records are to be obtained by the FBI, a point to which the statute makes reference five times.³³⁴

Under the bulk telephone records program, however, the FBI does not receive any records in response to the FISA court’s orders. While FBI officials sign every application seeking to renew the program, the calling records produced in response to the court’s orders are never “made available to the Federal Bureau of Investigation” or “received by

³²⁸ 50 U.S.C. § 1861(a)(1), (a)(3).

³²⁹ 50 U.S.C. § 1861(b)(2)(A), (c)(1).

³³⁰ 50 U.S.C. § 1861(b)(2)(B), (d)(1), (d)(2)(B), (g)(1), (h).

³³¹ 50 U.S.C. § 1861(g)(1).

³³² 50 U.S.C. § 1861(b)(2)(B), (c)(1).

³³³ Administration White Paper at 6 n.2. The legislative history of what ultimately became Section 215 supports the government’s assertion about its purpose. *See* H.R. Rep. No. 107-236(I), at 61 (2001) (“The Administration had sought administrative subpoena authority without having to go to court. Instead, section 156 amends title 50 U.S.C. § 1861 by providing for an application to the FISA court for an order directing the production of tangible items such as books, records, papers, documents and other items upon certification to the court that the records sought are relevant to an ongoing foreign intelligence investigation.” (emphasis removed)).

³³⁴ *See* 50 U.S.C. § 1861(b)(2)(B), (d)(1), (d)(2)(B), (g)(1), (h).

the Federal Bureau of Investigation,” as called for by the statute.³³⁵ Instead, the FISA court’s orders specifically direct telephone companies to “produce to NSA” their calling records — thwarting congressional intentions regarding the role each agency is to play in counterterrorism efforts that involve the collection of information within the United States about Americans.³³⁶

In compliance with the FISA court’s orders, telephone companies that are subject to this program transmit their calling records to the NSA. The records are not delivered to the FBI and are never passed on to the FBI by the NSA. Instead, the NSA stores the records in its own databases, conducts its own analysis of them, and provides reports to various federal agencies — including but not limited to the FBI — with information about telephone communications that “the NSA concludes have counterterrorism value.”³³⁷ While these reports are based on information derived from the calling records, the records themselves stay with the NSA. Indeed, the NSA is ordered by the FISA court to “store and process” those records “in repositories within secure networks under NSA’s control.”³³⁸

What’s more, the NSA is *prohibited* from sharing with the FBI information that it derives from the calling records it obtains, except under conditions outlined in the FISA court’s orders.³³⁹ Among those conditions, the NSA may share information with the FBI that contains information about U.S. persons only if designated NSA officials (not the FBI agents who are conducting the investigations to which the records are supposed to be relevant) determine that the information “is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.”³⁴⁰ The NSA must even file monthly reports with the FISA court listing every instance during the previous month in which the NSA shared such information with any entity, including the FBI.³⁴¹

The fact that the NSA, not the FBI, obtains the records produced causes the program to depart from the statute in another, related manner. Section 215 requires that any

³³⁵ 50 U.S.C. § 1861(b)(2)(B), (h).

³³⁶ Primary Order at 3.

³³⁷ Shea Decl. ¶ 16; *see* Primary Order at 4 (referring to “any *information* the FBI receives as a result of this Order (information that is disseminated to it by NSA)”) (emphasis added).

³³⁸ Primary Order at 4.

³³⁹ *See* Primary Order at 6 n.5 (“NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.”).

³⁴⁰ Primary Order at 13; *see id.* at 16-17.

³⁴¹ Primary Order at 16 (“Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with *anyone* outside NSA.” (emphasis added)).

records obtained through a FISA court order be handled according to “specific minimization procedures” adopted by the Attorney General to govern the “retention and dissemination by the Federal Bureau of Investigation” of the items or information it receives.³⁴² Before granting an application under Section 215, a FISA court judge must find that the application provides “an enumeration of the minimization procedures adopted by the Attorney General . . . that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.”³⁴³

Because the FBI does not receive anything from the telephone companies, it is impossible for the FISA court to make this finding. The court’s orders therefore finesse the statutory language by stating that “the Court finds . . . [t]he application includes an enumeration of the minimization procedures *the government* proposes to follow with regard to the tangible things sought.”³⁴⁴ The orders then set forth detailed minimization procedures for *the NSA* to follow with regard to the calling records it obtains.³⁴⁵ As a result, despite Congress’ clear direction that one agency’s minimization procedures must be followed (the FBI’s), the current process substitutes another agency’s procedures (the NSA’s).

In sum, the bulk telephone records program violates the requirement that records produced in response to a Section 215 order are to be obtained by the FBI, not the NSA, and that their retention and dissemination is to be governed by rules approved specifically for the FBI’s handling of those items. Those requirements are integral to the overall design of the statute, under which records can be obtained only when they are relevant to a specific FBI investigation. As the operation of this program illustrates, allowing the NSA to acquire calling records in bulk and subject them to the tools it possesses for mass data analysis significantly expands the nature and scope of the activity authorized by Section 215.

By no means are we suggesting that the NSA should not be allowed to collaborate with the FBI on its investigations. To the contrary, their partnership can be critical in linking the Signals Intelligence collected by the former with the latter’s efforts to disrupt terrorist attacks. The perils of inadequate cooperation among different agencies tasked with combating terrorism is a lesson learned from 9/11. But that cooperation must be

³⁴² 50 U.S.C. § 1861(g)(1).

³⁴³ 50 U.S.C. § 1861(b)(2)(B) (emphasis added); *see id.* § 1861(c)(1).

³⁴⁴ Primary Order at 2 (emphasis added).

³⁴⁵ *See* Primary Order at 4-16. Regarding the FBI, the FISA court’s orders set rules only for “any information the FBI receives as a result of this Order . . . information that is disseminated to it by NSA[.]” Primary Order at 4. With respect to such information, the orders direct that “the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General’s Guidelines for Domestic FBI Operations* (September 29, 2008).” *Id.*

rooted in the law. We are simply asking whether this specific statute, as written, authorizes the NSA to undertake this specific counterterrorism program, as presently conducted. We conclude that the statute does not provide that authorization. Permitting the NSA to acquire domestic, international, and foreign telephone records in bulk under Section 215 allows the statute to be used for a fundamentally different — and far broader — purpose than the one indicated by its text: enabling the FBI to obtain records that are relevant to specific investigations being conducted by the Bureau.³⁴⁶

VI. Violation of the Electronic Communications Privacy Act

In addition to concluding that the NSA's bulk telephone records program is unauthorized by Section 215, we also believe that it violates the Electronic Communications Privacy Act ("ECPA").

ECPA limits the circumstances under which a telephone company or other electronic communication service provider may divulge records about its customers.³⁴⁷ Apart from certain enumerated exceptions, a provider "shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity."³⁴⁸ These enumerated exceptions, among others, include situations in which the government secures a warrant, obtains a court order under ECPA, or utilizes a subpoena.³⁴⁹ But the statute does not authorize telephone companies to disclose customer information to the government in response to an order issued under Section 215.³⁵⁰

In late 2008, the government submitted an application to the FISA court seeking to renew the NSA's bulk telephone records program. This application was the first in which the government identified ECPA as potentially bearing on whether the FISA court properly

³⁴⁶ The disjunction between Section 215 and the telephone records program is further illustrated by the fact that the FBI already has the power to obtain telephone records that are relevant to its counterterrorism investigations, through so-called national security letters authorized by the Electronic Communications Privacy Act. *See* 18 U.S.C. §§ 2703(c), 2709. The Bureau makes extensive use of that power, and the purpose of Section 215, as the government has acknowledged, was to furnish the FBI with a more global subpoena-like authority that would cover the many types of records for which no subpoena authority existed.

³⁴⁷ *See* 18 U.S.C. § 2702(c). These provisions fall within a portion of ECPA called the Stored Communications Act.

³⁴⁸ 18 U.S.C. § 2702(a)(3).

³⁴⁹ *See* 18 U.S.C. §§ 2702(c), 2703(c).

³⁵⁰ *See id.*

could issue orders under Section 215 directing telephone companies to disclose their calling records to the NSA.³⁵¹

The FISA court concluded that its orders authorizing the NSA's program were consistent with ECPA. In reaching this conclusion, the court first determined that the terms of Section 215 and ECPA were in tension. Both statutes could not both be given "their full, literal effect," wrote the court, because Section 215 authorizes the production of "any tangible things," and applying the prohibitions of ECPA would limit the meaning of the word "any."³⁵²

The court then reasoned as follows. Observing that ECPA's prohibition on disclosures includes an exception for "national security letters" issued pursuant to 18 U.S.C. § 2709, the court stated that it would have been "anomalous" for Congress to permit this exception while making no comparable exception for Section 215 orders. This is so, the court wrote, because Section 215 requires a judge to agree with the government's assessment that items being sought are relevant to an investigation, whereas national security letters merely require the FBI to certify that the items sought are relevant. Therefore, the court concluded, ECPA should be interpreted to contain an implicit exception for orders issued under Section 215.³⁵³ The FISA court's reasoning was adopted recently in a decision from the Southern District of New York.³⁵⁴

While we acknowledge that the matter is not free from doubt, we believe that these decisions are wrong. "[I]t is a commonplace of statutory construction that the specific governs the general," the Supreme Court has said.³⁵⁵ "That is particularly true where . . . Congress has enacted a comprehensive scheme and has deliberately targeted specific problems with specific solutions."³⁵⁶ It would be difficult to imagine a more appropriate place to apply that principle than here. ECPA sets forth a detailed, multi-faceted set of provisions governing privacy in stored electronic communications and in records about the customers of electronic communication service providers. This comprehensive scheme

³⁵¹ See Supplemental Opinion at 1, *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Dec. 12, 2008).

³⁵² Supplemental Opinion at 1-2.

³⁵³ See Supplemental Opinion at 4-5.

³⁵⁴ Memorandum & Order at 26-28, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013). That court also reasoned that ECPA does not present a problem because "Section 215 authorizes the Government to seek records that may be obtained with a grand jury subpoena," and "Section 215 orders are functionally equivalent to grand jury subpoenas." *Id.* at 27.

³⁵⁵ *RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065, 2071 (2012) (quoting *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 384 (1992)); see *HCSC-Laundry v. United States*, 450 U.S. 1, 6 (1981) (stating that "a specific statute . . . controls over a general provision").

³⁵⁶ *RadLAX Gateway Hotel, LLC*, 132 S. Ct. at 2071 (quoting *Varity Corp. v. Howe*, 516 U.S. 489, 519 (1996) (Thomas, J., dissenting) (quotation marks omitted)).

directly targets the problem of when the government may gain access to such records and provides specific solutions, including court orders issued pursuant to 18 U.S.C. § 2703(d) and national security letters sent pursuant to 18 U.S.C. § 2709. The terms of Section 215, in contrast, could not be more general, simply referencing “any tangible things (including books, records, papers, documents, and other items).”³⁵⁷

As the FISA court acknowledged, the very statute that created Section 215, the Patriot Act, also amended ECPA “in ways that seemingly re-affirmed that communications service providers could divulge records to the government only in specified circumstances” — without including FISA court orders issued under Section 215.³⁵⁸ The fact that the same statute both created Section 215 and amended ECPA, but without adding an exception to ECPA for Section 215 orders, undermines the notion that ECPA and Section 215 are in conflict, and provides an additional basis for strictly adhering to ECPA’s prohibitions by not inferring unwritten exceptions to those prohibitions. It also demonstrates that another fundamental canon of statutory construction applies here — that the inclusion of some implies the exclusion of others not mentioned.³⁵⁹ “Where there is an express exception, it comprises the only limitation on the operation of the statute and no other exceptions will be implied.”³⁶⁰ Congress did not add an exception to ECPA for Section 215 orders, even though it amended ECPA in other ways at the same time that it created Section 215. That omission should be respected.

³⁵⁷ Before the Patriot Act substituted the phrase “any tangible things,” FISA’s business records statute permitted the government to obtain four specific types of records, one of which was records from a “common carrier.” Since that term can include telephone companies, the statute offered somewhat more specificity in its pre-Patriot Act state, but it was still considerably more general than ECPA.

³⁵⁸ Supplemental Opinion at 3. As the FISA court noted, legislative history indicates that before the passage of the Patriot Act, at least one senator was concerned that Section 215’s reference to “any tangible things” would “effectively trump” federal and state privacy protections. *See* 147 CONG. REC. 19,530 (2001) (statement of Sen. Feingold). Without discussion, the Senate tabled an amendment offered by Senator Feingold that was meant to “make[] it clear that existing Federal and State statutory protections for the privacy of certain information are not diminished or superseded by section 215.” *Id.* The Senate’s rejection of this amendment could have signaled a desire for Section 215 to override those other statutes, as Senator Feingold feared, or it could have reflected disagreement that Section 215’s language could possibly be interpreted so broadly. There are no statements shedding any light on the motivation of the senators who voted to reject the amendment. Such ambiguous legislative history does not warrant ignoring the clear statutory text of ECPA and the basic canons of statutory construction that counsel in favor of adhering to it. *See Milner v. Dep’t of Navy*, 131 S. Ct. 1259, 1266 (2011) (“Those of us who make use of legislative history believe that clear evidence of congressional intent may illuminate ambiguous text. We will not take the opposite tack of allowing ambiguous legislative history to muddy clear statutory language.”).

³⁵⁹ Or: “*Expressio unius est exclusio alterius.*” *Leatherman v. Tarrant Cnty. Narcotics Intelligence & Coordination Unit*, 507 U.S. 163, 168 (1993).

³⁶⁰ *Copeland v. Toyota Motor Sales U.S.A., Inc.*, 136 F.3d 1249, 1257 (10th Cir. 1998) (quoting NORMAN J. ZINGER, 2A SUTHERLAND’S STATUTES AND STATUTORY CONSTRUCTION § 47.11 (5th ed. 1992)).

The only apparent basis for permitting the general language of Section 215 to override the comprehensive and specific language of ECPA is a judgment about what it would have been logical for Congress to have enacted. The FISA court decided that Congress could not have intended to permit the government to obtain telephone calling records through a national security letter, which requires only an executive branch certification of relevance, while prohibiting the government from obtaining the same records through Section 215, which requires a court to agree with the government's assessment of relevance.³⁶¹

But there very well may be legitimate reasons to have included an exception in ECPA for national security letters but not for Section 215 orders. Because Congress appears to have intended Section 215 to allow the FBI to obtain types of records it could not already obtain, it may have expected that the various national security letter statutes would continue to cover the specific categories of data to which they relate (telephone metadata in the case of ECPA), and that Section 215 would apply to any other categories of records. Moreover, whereas Section 215 demands only reasonable grounds to believe that items sought (of whatever kind) are relevant to an investigation, the national security letter statute requires a more specific certification "that the name, address, length of service, and toll billing records" being sought are relevant.³⁶²

More fundamentally, however, we do not believe that courts should interpret statutes like ECPA based on their assessment of what would have been sensible for Congress to enact, at least not when that interpretation overrides detailed statutory language and violates basic methods of interpreting statutes. The identification of an apparent "anomaly"³⁶³ is not a sufficient basis for judicial revision of clear statutory text. And while "absurd results are to be avoided" in interpreting statutes,³⁶⁴ the perceived oddity of permitting telephone records to be acquired through NSLs but not through Section 215 is hardly extreme enough to call for this doctrine, which is used "to override unambiguous legislation" only "rarely."³⁶⁵ In other words, this is not "one of those rare

³⁶¹ See Supplemental Opinion at 4-5.

³⁶² 18 U.S.C. § 2709(b)(1). Furthermore, Section 215 originally permitted records to be obtained without any assertion that they were relevant to an investigation, much less a judicial finding of relevance. The government needed merely to state in its application that the records concerned were "sought for" an authorized investigation. 50 U.S.C. § 1861(b)(2) (2002). Until 2006, therefore, when Section 215 was amended, it imposed a lower standard for obtaining records than the certification required to issue a national security letter under ECPA.

³⁶³ Supplemental Opinion at 5.

³⁶⁴ *United States v. Wilson*, 503 U.S. 329, 334 (1992) (citing *United States v. Turkette*, 452 U.S. 576, 580 (1981)).

³⁶⁵ *Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 441 (2002); see Memorandum & Order at 27 (stating that "to allow the Government to obtain telephony metadata with an NSL but not a section 215 order would lead to an absurd result").

cases where the application of the statute as written will produce a result ‘demonstrably at odds with the intentions of its drafters.’”³⁶⁶ Because the perceived anomaly identified by the FISA court is not “so bizarre that Congress ‘could not have intended’ it,” therefore “the remedy lies with the law making authority, and not with the courts.”³⁶⁷

Inferring an unwritten exception to ECPA based on an “anomaly” is particularly questionable when that exception is then used to permit the NSA’s bulk collection of telephone records. As noted, the FISA court concluded that it would be irrational to prohibit the government from obtaining telephone records through Section 215, which requires a judge to agree that the records are relevant to an investigation, when the FBI can obtain those same records through a national security letter, which requires no prior judicial approval. But the FBI already widely obtains telephone records through national security letters, and the FISA court’s ruling simply permits a second agency, the NSA, to obtain *all* telephone records. Even if an aggressive reading of Section 215 permits that result — which we believe is not the case — it clearly is not what Congress intended to achieve when it enacted Section 215.

VII. The Reenactment Doctrine

In 2010, and again in 2011, Congress prevented Section 215 from expiring by extending its sunset date. Courts and the government have concluded that by twice extending the expiration date of Section 215, while the NSA’s bulk telephone records program was ongoing, Congress implicitly adopted an interpretation of Section 215 that legitimizes the program.³⁶⁸ This conclusion rests on the principle that “Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change.”³⁶⁹ On multiple grounds, however, we believe that principle has no place here.

The “reenactment doctrine” does not trump the plain meaning of a law, but rather is one of many interpretive tools that come into play when statutory ambiguity demands an

³⁶⁶ *Demarest v. Manspeaker*, 498 U.S. 184, 190 (1991) (quoting *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 571 (1982)).

³⁶⁷ *Demarest*, 498 U.S. at 191 (quoting *Griffin*, 458 U.S. at 575); *Griffin*, 458 U.S. at 575 (quoting *Crooks v. Harrelson*, 282 U.S. 55, 60 (1930)).

³⁶⁸ See Amended Memorandum Opinion at 23-28, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013); Memorandum & Order at 28-32, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013); Administration White Paper at 17-19.

³⁶⁹ *Forest Grove Sch. Dist. v. T.A.*, 557 U.S. 230, 239-40 (2009) (quoting *Lorillard v. Pons*, 434 U.S. 575, 580 (1978)).

inquiry into congressional intent. Reenactment, in other words, “cannot save” an administrative or judicial interpretation that contradicts the requirements of the statute itself.³⁷⁰ And for the many reasons explained above, any interpretation of Section 215 that would authorize the NSA’s telephone records program is irreconcilable with the plain words of the statute, its manifest purpose, and its role within FISA as a whole.

Even if Section 215 were sufficiently ambiguous to justify an inquiry into congressional intent, the circumstances presented here are unlike any in which the reenactment doctrine has ever been applied — and the differences are pivotal. First, there was no judicial interpretation of Section 215 of which Congress could have been aware in 2010 or 2011: at that time the FISA court had never issued any opinion explaining the legal rationale for the NSA’s program under Section 215, but had merely signed orders authorizing the program. Second, even if the FISA court’s orders, combined with the government’s applications to the court, are viewed as an “interpretation” of Section 215, members of Congress may have been prohibited from reading those orders and those applications (except for members of the intelligence and judiciary committees) by operation of committee rules. Thus, to apply the reenactment doctrine here, Senators and Congressmen must be presumed to have adopted an “interpretation” that they had no ability to read for themselves. Third, even if being apprised of the NSA’s program were equivalent to being made aware of a judicial interpretation of a statute, applying the reenactment doctrine is improper where members of Congress must try to comprehend a secret legal interpretation without the aid of their staffs or outside experts and advocates. That scenario robs lawmakers of a meaningful opportunity to gauge the legitimacy and implications of the legal interpretation in question. Fourth, Congress did not reenact Section 215 at all in 2010 and 2011, but merely delayed its expiration. To our knowledge, no court has applied the reenactment doctrine under a combination of circumstances remotely like this.

Finally, even if Section 215 were ambiguous about whether it authorizes the NSA’s bulk collection of telephone records, and even if the reenactment doctrine could be extended to the novel circumstances presented here, doing so would undermine the ability of the American public to know what the law is, and to hold their elected representatives accountable for their legislative choices. Applying the reenactment doctrine to legitimize the government’s interpretation of Section 215, therefore, is both unsupported by legal precedent and unacceptable as a matter of democratic accountability.

In truth, what is urged here is not the traditional reenactment doctrine, but rather a new variant: where the executive branch makes classified information available to

³⁷⁰ *Leary v. United States*, 395 U.S. 6, 25 (1969) (quoting *Commissioner of Internal Revenue v. Acker*, 361 U.S. 87, 93 (1959)).

Congress that a secret program is being conducted under the auspices of a particular statute, and where Congress subsequently delays the expiration of that statute without amending it, Congress's action renders the program legally authorized even if the words of the statute do not support it. This is a novel proposition that we do not accept.

A. Background

When Congress last amended Section 215, it provided that the statute would expire by 2010.³⁷¹ Early that year, Congress extended the statute's "sunset" date for another year, and in 2011 Congress further extended the sunset date for another four years.³⁷²

Before these two extensions, the intelligence and judiciary committees in the House and Senate were provided with the FISA court's initial order authorizing the NSA's bulk telephone records program and the government's initial application.³⁷³ Those committees also were briefed by the executive branch about the program.³⁷⁴

Other members of the House and Senate were prohibited from reading the FISA court's order or the government's application. In 2009, prior to the first extension of Section 215's sunset date, the executive branch provided the intelligence committees with a five-page briefing paper on the NSA's bulk telephone and Internet metadata programs, encouraging the committees to make this document available to all members of Congress.³⁷⁵ Before the second extension in 2011, the executive branch provided a similar

³⁷¹ See USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 102(b)(1), 120 Stat. 191, 195 (2006) ("Effective December 31, 2009, the Foreign Intelligence Surveillance Act of 1978 is amended so that sections 501, 502, and 105(c)(2) read as they read on October 25, 2001.").

³⁷² See An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111-141, 124 Stat. 37 (Feb. 27, 2010); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (May 26, 2011). Section 215 is now set to sunset on June 1, 2015.

³⁷³ Administration White Paper at 18. Twice a year, the Attorney General is required to submit to the House and Senate intelligence and judiciary committees "a summary of significant legal interpretations" of FISA involving matters before the FISA court or its companion appellate court, the Foreign Intelligence Surveillance Court of Review, "including interpretations presented in applications or pleadings" filed with those courts. 50 U.S.C. § 1871(a)(4). This summary must be accompanied by "copies of all decisions, orders, or opinions" of the two courts "that include significant construction or interpretation" of the provisions of FISA. 50 U.S.C. § 1871(a)(5). In addition, on an annual basis the Attorney General must "inform" the House and Senate intelligence committees and the Senate judiciary committee "concerning all requests" for the production of items under Section 215. 50 U.S.C. § 1862(a).

³⁷⁴ See Administration White Paper at 18 & n.14.

³⁷⁵ See Letter from Assistant Attorney General Ronald Weich to the Honorable Silvestre Reyes, Chairman, House Permanent Select Committee on Intelligence, at 1 (Dec. 14, 2009) ("2009 Letter"); Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Act Reauthorization (2009) ("2009 Report").

briefing paper to the intelligence committees.³⁷⁶ Each time, the executive branch specified that the briefing paper was “being provided on the understanding that it will be provided only to Members of Congress (and cleared SSCI, Judiciary Committee, and leadership staff), in a secure location in the SSCI’s offices, for a limited time period to be agreed upon, and consistent with the rules of the SSCI regarding review of classified information and non-disclosure agreements.”³⁷⁷ The letters also specified: “No photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location.”³⁷⁸

Before the first extension of Section 215’s sunset date, the House and Senate committees made this briefing paper available to all members of Congress under the aforementioned conditions.³⁷⁹ Before the second extension, in 2011, the Senate intelligence committee made this briefing paper available to all Senators, but the House intelligence committee did not make it available to all House members.³⁸⁰

The briefing paper provided to the intelligence committees does not contain any legal analysis or explanation of how the NSA’s bulk telephone records program fits within the terms of Section 215. Instead the paper describes in general terms the operation of the NSA’s telephone and Internet metadata collection programs, indicating that they involve obtaining “large amounts of transactional data obtained from certain telecommunications service providers in the United States.”³⁸¹ The briefing paper further explains that “NSA is authorized to collect from telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call,” and that FISA court orders “generally require production of the business records (as described above) relating to substantially all of the telephone calls handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.”³⁸² The document characterizes the program as an essential tool for combating terrorism,

³⁷⁶ See Letter from Assistant Attorney General Ronald Weich to the Honorable Dianne Feinstein and the Honorable Saxby Chambliss, Chairman and Vice Chairman, Senate Select Committee on Intelligence, at 1 (Feb. 2, 2011) (“2011 Letter”); Report on the National Security Agency’s Bulk Collection Programs Affected by USA PATRIOT Act Reauthorization (2011) (“2011 Report”).

³⁷⁷ 2011 Letter at 1; see 2009 Letter at 2

³⁷⁸ 2011 Letter at 1-2; see 2009 Letter at 2.

³⁷⁹ See Administration White Paper at 17-18.

³⁸⁰ See Administration White Paper at 18 n.13.

³⁸¹ 2011 Report at 2.

³⁸² 2011 Report at 3.

emphasizes the strict rules governing it, discloses that it has generated compliance issues, and includes certain details of the program that illustrate its limitations.³⁸³

B. Discussion

“When Congress reenacts statutory language that has been given a consistent judicial construction,” the Supreme Court “often adhere[s] to that construction in interpreting the reenacted statutory language.”³⁸⁴ In other words, “Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change.”³⁸⁵

“There is an obvious trump to the reenactment argument, however, in the rule that ‘[w]here the law is plain, subsequent reenactment does not constitute an adoption of a previous administrative construction.’”³⁸⁶ Congressional reenactment “has no interpretive effect where regulations clearly contradict [the] requirements of [a] statute,”³⁸⁷ and in such cases reenactment “cannot save” the faulty interpretation.³⁸⁸ Rather: “In a statutory construction case, the beginning point must be the language of the statute, and when a statute speaks with clarity to an issue judicial inquiry into the statute’s meaning, in all but the most extraordinary circumstance, is finished.”³⁸⁹ An interpretation that “flies against the plain language of the statutory text exempts courts from any obligation to defer to

³⁸³ While the briefing paper explains that the NSA’s program operates “on a very large scale” and involves “substantially all” of the calling records generated by “certain” telephone companies, it does not make explicit that the program is designed to collect the records of essentially all telephone calls. And while the document explains certain operational details about the program that confine its reach — such as the fact that “[b]efore NSA analysts may query bulk records, they must have reasonable articulable suspicion . . . that the number or e-mail address they submit is associated with” a terrorist organization — it omits other details having the opposite implication, such as the fact that a single query permits analysts to view the full calling records of all telephone numbers that are two “hops” away from the target, which generally means thousands of numbers. 2011 Report at 3-4. Similarly, while document cites “a number of technical compliance problems and human implementation errors” reported to the FISA court, highlighting the absence of “any intentional or bad-faith violations,” it does not hint at the full scope of these compliance issues, reflected in the FISA court’s 2009 declaration that “from the inception of this FISA BR program, the NSA’s data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures.” Order at 14-15, *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Mar. 2, 2009).

³⁸⁴ *Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 185 (1994) (citing *Keene Corp. v. United States*, 508 U.S. 200, 212-13 (1993), *Pierce v. Underwood*, 487 U.S. 552, 567 (1988), & *Lorillard v. Pons*, 434 U.S. at 580-81).

³⁸⁵ *Forest Grove Sch. Dist. v. T.A.*, 557 U.S. at 239-40 (quoting *Lorillard*, 434 U.S. at 580).

³⁸⁶ *Brown v. Gardner*, 513 U.S. 115, 121 (1994) (quoting *Demarest v. Manspeaker*, 498 U.S. 184, 190 (1991)).

³⁸⁷ *Brown*, 513 U.S. at 121 (citing *Massachusetts Trustees of Eastern Gas & Fuel Associates v. United States*, 377 U.S. 235, 241-42 (1964)).

³⁸⁸ *Leary v. United States*, 395 U.S. 6, 25 (1969) (citing *Massachusetts Trustees of Eastern Gas and Fuel Associates*, 377 U.S. at 241-42).

³⁸⁹ *Estate of Cowart v. Nicklos Drilling Co.*, 505 U.S. 469, 475 (1992) (citing *Demarest*, 498 U.S. at 190).

it,”³⁹⁰ because Congress cannot “add to or expand” a statute by “impliedly” approving an interpretation that “conflicts with the statute.”³⁹¹ Thus, a “poor fit” between statutory language and an administrative or judicial construction, or the “eccentricity” of such a construction in light of the statutory text, prevents the reenactment doctrine from legitimizing that construction.³⁹²

For the many reasons explained earlier, Section 215 is not ambiguous about whether it authorizes the NSA to collect the entire nation’s telephone records on an ongoing daily basis: the only way to interpret Section 215 in that fashion is to add words to the statute that it does not contain, subtract words that it does contain, and reinterpret other words beyond recognition. Because “the text and reasonable inferences from it give a clear answer,” that is “the end of the matter.”³⁹³

Even if Section 215 were ambiguous on this question, the reenactment doctrine cannot credibly be applied to the circumstances presented here, which differ in pivotal ways from any circumstances in which the doctrine has been applied. To begin with, Congress did not actually reenact Section 215 in 2010 or 2011, but merely postponed the sunset dates on which the statute would expire.³⁹⁴ More importantly, at the time of these extensions, there was no judicial interpretation of Section 215 by the FISA court of which Congress can be presumed to have been aware. Until 2013, the FISA court never issued any opinion explaining how Section 215 authorized the NSA’s telephone records program. And while the government’s applications to the FISA court seeking authorization for the program contained the executive branch’s position on that question, members of Congress outside of the intelligence and judiciary committees were prohibited from reading those applications (or the FISA court orders granting them). At most, these Senators and Representatives had access to a five-page document describing the program in general terms, along with the opportunity for briefings by executive branch officials.

³⁹⁰ *Brown*, 513 U.S. at 122 (citing *Dole v. Steelworkers*, 494 U.S. 26, 42 43 (1990), and *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 842 43 (1984)).

³⁹¹ *Leary*, 395 U.S. at 25 (quoting *Commissioner of Internal Revenue v. Acker*, 361 U.S. 87, 93 (1959)); see William N. Eskridge, Jr., *Interpreting Legislative Inaction*, 87 MICH. L. REV. 67, 83 (1988) (“Where the prior interpretation is flatly inconsistent with relatively clear statutory language or history, the Court may abandon the *Lorillard* presumption that Congress was aware of and adopted the prior line of interpretation.”).

³⁹² *Brown*, 513 U.S. at 119-21.

³⁹³ *Brown*, 513 U.S. at 120 (quoting *Good Samaritan Hospital v. Shalala*, 508 U.S. 402, 409 (1993) (internal quotation marks omitted)).

³⁹⁴ See An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111-141, 124 Stat. 37 (2010) (striking “February 28, 2010” and inserting “February 28, 2011”); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011) (striking “May 27, 2011” and inserting “June 1, 2015”).

While this document gave notice of the existence of the NSA's program, it cannot be regarded as a judicial or administrative interpretation of a statute — because it lacks any explanation of how Section 215 can be interpreted to authorize the program. (Indeed, it contains no legal analysis at all.) And even this document was never made available to the full House of Representatives before the most recent extension of Section 215's sunset date. While the briefing paper may have been intended to help lawmakers make informed policy choices, simply providing notice of an ongoing program is not the same as making Congress aware of an administrative or judicial interpretation of a statute.

Moreover, even if having access to the executive branch's briefing paper were equivalent to being aware of an administrative or judicial interpretation of a statute, the reenactment doctrine would still be out of place here. The doctrine has never been applied to secret interpretations of the law summarized in classified papers that members of Congress must comprehend without the aid of their own staffs or outside experts.³⁹⁵ When legislators set about determining whether to reenact a statute, they normally are aided by the insights and advice of their staff as well as commentary by legal scholars, practitioners, journalists, advocates, and others regarding how that statute has been interpreted. Thus, before reenacting a statute that has been interpreted in a particular way, legislators have the means of becoming educated about the nature of that interpretation, its strength as a doctrinal matter, and its full ramifications as a practical matter. By contrast, when the only means through which legislators can try to understand a prior interpretation of the law is to read a short description of an operational program, prepared by executive branch officials, made available only at certain times and locations, which cannot be discussed with others except in classified briefings conducted by those same executive branch officials, legislators are denied a meaningful opportunity to gauge the legitimacy and implications of the legal interpretation in question. Under such circumstances, it is not a legitimate method of statutory construction to presume that these legislators, when reenacting the statute, intended to adopt a prior interpretation that they had no fair means of evaluating.

Finally, even if the reenactment doctrine were a valid means of discerning congressional intent under these circumstances, its application would have unacceptable consequences for the public's ability to know what the law is. When a secret court accepts a counterintuitive reading of a law — one that could not possibly be guessed by reading the

³⁹⁵ Personal staff for members of Congress are not eligible to obtain the level of security clearance required for access to Section 215 program information. *See, e.g.*, Office of Senate Security, United States Senate Security Manual, § III.5 (Apr. 2007) ("There are three 'levels' of security clearance, which correspond with the three levels of classification: Confidential, Secret and Top Secret. *In addition, certain categories of classified information require special clearances and access approval. These special clearances and approvals are granted on a rigidly controlled need-to-know basis, and are not granted to personal staff.*" (emphasis added)). Therefore, many members of Congress — anyone who does not sit on a committee where review of classified information is common — have no staff who would have been able to assist them in reviewing the classified descriptions of the Section 215 program.

statutory language alone, and which invests the government with significant new powers — permitting congressional reenactment to enshrine that novel interpretation deprives the public of any ability to know that the law is, much less have any voice in changing it.

For these reasons, we believe that the statutory legitimacy of the NSA's bulk telephone records program must be assessed only with reference to the words of the law that purportedly authorizes it.

VIII. Conclusion

The NSA's bulk telephone records program was initiated more than four years before the government sought authorization for it under Section 215 of the Patriot Act. In light of that history, it may not be surprising that the operation of the program bears almost no relationship to the text of the statute — which is designed to confer subpoena-like authority on the FBI, not to enable nationwide bulk data collection by the NSA. As we believe the foregoing analysis has demonstrated, sanctioning the NSA's program under Section 215 requires an impermissible transformation of the statute: Where its text fails to authorize a feature of the program (such as the daily production of new telephone records), such authority must be inferred from silence. Where its text uses limiting words (such as "relevant"), those words must be redefined beyond their traditional meaning. And where its text simply cannot be reconciled with the program (such as its direction that the FBI, not the NSA, receive any items produced), those words must be ignored.

It may have been a laudable goal for the executive branch to bring this program under the supervision of the FISA court. Ultimately, however, that effort represents an unsustainable attempt to shoehorn a preexisting surveillance program into the text of a statute with which it is not compatible. Because Section 215 does not provide a sound legal basis for the NSA's bulk telephone records program, we believe the program must be ended.

Part 6:
CONSTITUTIONAL ANALYSIS

I. Overview

The NSA's bulk telephone records program potentially implicates both the First and Fourth Amendments to the United States Constitution. Yet evaluating the legitimacy of the program under those amendments presents a challenge: while constitutional analysis involves drawing inferences and conclusions from existing precedent, the scope and duration of the Section 215 telephone records program go beyond anything ever before confronted by the courts. In addition, as a result of technological development, the government now possesses capabilities to collect, store, and analyze data that were not available when key portions of the existing case law were decided. For these reasons, a mechanical application of cases decided many years ago regarding the particularized collection of limited amounts of data may miss the point. In future decisions, the courts will take account of those technological developments, as they have begun to do in other cases applying the Fourth Amendment to new technological realities. In this section, we do not try to predict the future path of constitutional doctrine. We do, however, note where existing doctrine seems an ill fit for evaluating the Section 215 telephone records program and where that doctrine may be unsustainable given the realities of modern technology. And we recommend as a policy matter that all three branches of government, in developing and assessing data collection programs, look beyond the application of cases decided in a very different environment and instead consider how to preserve the underlying constitutional principles in the face of modern communications technology and surveillance capabilities.

We first consider the Fourth Amendment, which prohibits unreasonable searches and seizures by the government. Analysis of the NSA's telephone records program under the Fourth Amendment must begin by asking whether the agency's collection of calling records qualifies as a "search" within the meaning of the Amendment. If not, as the government has argued in defense of the program, the Fourth Amendment and its restrictions do not apply to the NSA's activity.

The Supreme Court has ruled that the Fourth Amendment does not provide individuals with a right of privacy in the numbers that they dial from their telephones. More broadly, the Court has concluded, any information that a person voluntarily discloses to a business or other entity loses all Fourth Amendment protection. This rule, referred to as the "third-party doctrine," means that when government agents obtain records about a person that are held by a telephone company, bank, or other institution, that does not qualify as a search under the Constitution.

Although the Section 215 program encompasses much more information than the telephone numbers that a person dials, all of the information that the NSA collects under the program has been disclosed to telephone companies by their customers. Therefore, under the broad reading of the third-party doctrine widely adopted in the federal courts, none of the information is constitutionally protected, and the NSA may collect it without seeking a warrant or ensuring that its behavior satisfies the Fourth Amendment's standard of reasonableness.

The third-party doctrine has long been criticized as permitting undue government intrusion into personal privacy. Those criticisms have gained particular force in light of two trends stemming from modern technological developments. First, Americans increasingly must share personal information with institutions in order to conduct business and avail themselves of services that have become commonplace features of contemporary life. Second, new technology has dramatically enhanced the government's ability to collect, aggregate, and analyze immense quantities of information. Moreover, until last year, no court had considered whether there is any limit to the third-party doctrine in the context of the collection of data about essentially all individuals nationwide on an ongoing, indefinitely renewable basis.³⁹⁶

It is possible that the third-party doctrine or its scope will be judicially revised. The Supreme Court has recognized the danger that technological developments may erode Fourth Amendment privacy guarantees if constitutional law does not respond to those developments. In addition, a majority of Justices recently indicated that the rise of powerful new surveillance tools demands that not everything an individual reveals to another person is undeserving of Fourth Amendment protection.

To date, however, the Supreme Court has not modified the third-party doctrine or overruled its conclusion that the Fourth Amendment does not protect telephone dialing records. Most courts continue to follow those precedents, and government lawyers are entitled to rely on them, including in their formulation and defense of the Section 215 program.

Furthermore, a reversal or narrowing of these principles would establish only that the NSA's collection of telephone records is a "search" under the Fourth Amendment. Additional questions would then follow about whether this type of search required a warrant and whether it was reasonable within the meaning of the amendment.

³⁹⁶ See Memorandum & Order, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013); Memorandum Opinion, *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013); Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

Notwithstanding the agreement of most federal courts that telephony metadata lacks Fourth Amendment protection, however, the collection of telephone calling records by the government clearly implicates considerable privacy interests. Those interests, accordingly, deserve significant weight when the value of the NSA's telephone records program is balanced with its effects on privacy and civil liberties, an analysis we undertake in the next section of this Report.

We also consider in this section whether the telephone records program may impact rights under the First Amendment, which, among other safeguards, provides protection for the freedoms of speech and association. The Supreme Court has recognized that the freedom of association involves the rights of people to join together in support of their common beliefs on political, religious, cultural, economic and other matters. To the extent that the NSA's telephone records program reveals the patterns of individuals' connections and associations, this may implicate such First Amendment rights.

The Supreme Court has ruled that government programs can violate the First Amendment freedom of association even if they are not directly aimed at limiting the ability of people to join together for a common purpose. Indirect actions that have the effect of "chilling" the right of association can also infringe this constitutional right. In other words, the government can interfere with this constitutional protection by making people afraid to exercise their freedom of association.

The Supreme Court has explored the constitutional freedom of association in depth in connection with challenges to government actions that force disclosure of individuals' associations to the government. In this context, the Court has recognized that the freedom of association includes protection for the privacy of associations, so that individuals will not be afraid to join together in exercising their rights. This right to privacy of association was grounded in the need to protect people who promote controversial or dissident beliefs, and has also been recognized where revealing associations to the government could subject an individual to adverse consequences. Courts have also found that surveillance programs can have a chilling effect on the freedom of association. However, due to the doctrine of standing, the Supreme Court has never reached the question of whether a surveillance program can create a "chilling effect" sufficient to violate the First Amendment.

The First Amendment right of association is not absolute, but courts will review challenges under the "exacting scrutiny" test. Government actions that may chill associational conduct must be supported by a sufficiently important government interest, and must be designed to limit the intrusions on First Amendment rights.

Just as with the Fourth Amendment, changes in technology have altered the analysis. There has never been a program of the scope of the one being conducted under Section 215, and the government has never had at its disposal the analytic tools now

available. Our analysis of the NSA telephone records program concludes that the collection of telephone metadata records for all Americans' phone calls extending over a five year time period implicates the First Amendment freedom of association. Although the program is supported by a compelling government interest in combatting terrorism, which can justify some intrusions on First Amendment rights, it is not narrowly tailored. The extraordinary breadth of this collection program creates a chilling effect on the First Amendment rights of Americans, and we factor this concern into our policy analysis later in this Report.

II. THE FOURTH AMENDMENT

A. Protections of the Fourth Amendment against Unreasonable Searches

The Fourth Amendment to the United States Constitution prohibits unreasonable searches and seizures by the government. The Amendment reads:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Before conducting most types of searches, government agents must obtain a warrant from a judge that describes what they plan to search, after demonstrating probable cause to believe that the search will yield evidence of a criminal offense.³⁹⁷ Requiring agents to obtain a warrant before conducting a search limits the potential for abuse of their authority, the Supreme Court has explained, by requiring them to “present their estimate of probable cause for detached scrutiny by a neutral magistrate,” to “observe precise limits established in advance by a specific court order,” and “to notify the authorizing magistrate in detail of all that had been seized.”³⁹⁸

Warrants are not required for government searches in “a few specifically established and well-delineated exceptions.”³⁹⁹ Even searches that fall within those

³⁹⁷ See *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (stating that “searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment — subject only to a few specifically established and well-delineated exceptions”) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)).

³⁹⁸ *Katz*, 389 U.S. at 356.

³⁹⁹ *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).

exceptions violate the Fourth Amendment if they are not “reasonable.”⁴⁰⁰ Whether a search is reasonable, the Supreme Court has said, “is determined by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.”⁴⁰¹

While Fourth Amendment questions are raised most frequently in criminal prosecutions, where defendants can argue that evidence against them was obtained unconstitutionally, its protections are not limited to situations where law enforcement officers are searching for evidence of a crime.⁴⁰² “The Amendment guarantees ‘the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government,’ without regard to whether the government actor is investigating crime or performing another function.”⁴⁰³ This means that the executive branch must comply with the Fourth Amendment and may not engage in unreasonable searches when performing other vital functions of the government, such as protecting the nation from terrorism.⁴⁰⁴

The Fourth Amendment’s restrictions come into play, however, only when the government carries out a search (or seizure). Whether a particular action taken by the government qualifies as a search is sometimes a difficult question. The quintessential example of a Fourth Amendment search occurs when government agents enter someone’s home to look through his or her belongings, but the Amendment covers many other types of intrusions into personal privacy.

The telephone records program carried out by the NSA under Section 215 of the Patriot Act begins with the collection of individual Americans’ calling records from private telephone companies. The NSA does not obtain these records from Americans themselves by probing their mail or computers, nor does it intercept the records in transmission or use any special technical means to gather them. Instead, private telephone companies disclose the records to the NSA, as ordered by the Foreign Intelligence Surveillance Court (“FISC” or “FISA court”).⁴⁰⁵ In defense of the NSA’s program, the government argues that collecting telephone calling records in this manner does not qualify as a “search” within the meaning of the Fourth Amendment.

⁴⁰⁰ See *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013) (“Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution.”).

⁴⁰¹ *Samson v. California*, 547 U.S. 843, 848 (2006); accord *Maryland v. King*, 133 S. Ct. at 1970.

⁴⁰² *Quon*, 130 S. Ct. at 2627.

⁴⁰³ *Quon*, 130 S. Ct. at 2627 (quoting *Skinner v. Railway Labor Executives’ Ass’n*, 489 U.S. 602, 613-614 (1989)).

⁴⁰⁴ *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008).

⁴⁰⁵ See Part 3 this Report for a description of this process.

If the government is correct, the Fourth Amendment does not apply at all to the NSA's telephone records program, meaning that the program may be conducted without obtaining warrants and without meeting the constitutional standard of reasonableness. While the government has devised a strict set of rules limiting the NSA's use and dissemination of the records it collects — recognizing that many individuals feel a privacy interest in their calling records, particularly with respect to governmental access to those records — these rules place no limits on the government's initial *collection* of telephone records. The question, then, is whether the NSA's collection of these records constitutes a search under the Fourth Amendment.

B. Telephone Eavesdropping and Reasonable Expectations of Privacy

Through the middle of the last century, defining a “search” was relatively simple because the Fourth Amendment was understood to protect certain *places* and *things* — such as one's home or vehicle — from unreasonable government searches. As a result, Fourth Amendment law was linked with the concept of property.⁴⁰⁶ When government agents physically invaded a person's home or seized personal property to gather information; that conduct was regarded as a search and was subject to the restrictions of the Fourth Amendment.⁴⁰⁷

In a landmark 1967 decision, however, the Supreme Court clarified that “the Fourth Amendment protects people, not places” and ruled that government investigatory conduct can qualify as a search even where agents do not interfere with an individual's private property.⁴⁰⁸ That decision, *Katz v. United States*, involved eavesdropping on telephone conversations. FBI agents had attached a listening device to the outside of a public telephone booth that was frequently used by a criminal suspect, allowing them to hear the words that he spoke into the telephone receiver. Although the agents did not physically intrude into the suspect's home or even into the telephone booth, the Supreme Court declared their eavesdropping to be a “search” under the Fourth Amendment, explaining that what a person “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”⁴⁰⁹

A person in a telephone booth, the Court said in *Katz*, “is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world[.]”⁴¹⁰

⁴⁰⁶ See *United States v. Jones*, 132 S. Ct. 945, 949 (2012); *Kyllo v. United States*, 533 U.S. 27, 31-32 (2001) (citing, *inter alia*, *Olmstead v. United States*, 277 U.S. 438, 465-66 (1928)).

⁴⁰⁷ See *Jones*, 132 S. Ct. at 949; *id.* at 955 (Sotomayor, J., concurring).

⁴⁰⁸ *Katz v. United States*, 389 U.S. 347, 351 (1967); see *Jones*, 132 S. Ct. at 949 (quoting *Katz*, 389 U.S. at 351).

⁴⁰⁹ *Katz*, 389 U.S. at 351.

⁴¹⁰ *Katz*, 389 U.S. at 352.

Therefore, the act of “electronically listening to and recording the [suspect’s] words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a ‘search and seizure’ within the meaning of the Fourth Amendment.”⁴¹¹

The *Katz* decision made clear that, unless an exception applied, government eavesdropping on private telephone conversations without a warrant violates the Constitution. As the Court put it a few years later: “Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance.”⁴¹²

More broadly, *Katz* established a two-part test for determining whether government conduct qualifies as a “search” under the Fourth Amendment. This “twofold requirement,” from Justice John Marshall Harlan’s concurring opinion, requires “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”⁴¹³ Justice Harlan’s two-part test was soon adopted by the Court itself and ever since has been the Fourth Amendment standard.⁴¹⁴ Thus, “a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.”⁴¹⁵

Unlike the surveillance addressed by the Supreme Court in *Katz*, the NSA’s calling records program does not allow the government to listen to the content of telephone conversations. Indeed, because calling records are transmitted to the NSA by the telephone companies only after the calls have been completed, and because the telephone companies do not record these calls, the program gives the agency no means of listening to phone conversations. The government does not argue that the NSA could eavesdrop on purely domestic telephone calls without obtaining a warrant.

Under the Supreme Court’s guidance, therefore, determining whether the NSA’s collection of telephone records qualifies as a search involves applying the two-part test set forth above, and asking whether individuals have a subjective expectation of privacy in their calling records that society recognizes as reasonable. Answering that two-part question, however, requires taking into account another important Fourth Amendment doctrine.

⁴¹¹ *Katz*, 389 U.S. at 353.

⁴¹² *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 313 (1972).

⁴¹³ *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

⁴¹⁴ *Mancusi v. DeForte*, 392 U.S. 364, 368 (1968).

⁴¹⁵ *See, e.g., Kyllo*, 533 U.S. at 33 (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

C. The “Third-Party Doctrine”

Government agents have other ways of obtaining information about people besides eavesdropping on their conversations or searching their property. One method is to subpoena information about a person from a third party. In the 1976 decision *United States v. Miller*, the Supreme Court concluded that law enforcement agents, without a warrant, could use a grand jury subpoena to obtain a customer’s personal financial records from a bank. The Court rejected the customer’s argument that under *Katz* he had a reasonable expectation of privacy in his bank records. The Court noted that “checks are not confidential communications but negotiable instruments to be used in commercial transactions.” They are “voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.” A bank customer has “neither ownership nor possession” of such records, the Court said, which “are the business records of the banks.”⁴¹⁶ A bank depositor, the Court reasoned, “takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.”⁴¹⁷

This situation was different from the one in *Katz*, where government agents covertly recorded a suspect’s conversation from the outside of a telephone booth. The suspect in *Katz* had attempted to keep his conversation private from everyone except for the other participant, and so the government, without a warrant, could learn what was said in that conversation only from the other participant. The difference in *Miller* was that the government obtained the suspect’s bank records directly from the bank, which itself participated in every financial transaction catalogued in its customers’ records. “All of the documents obtained,” therefore, “including financial statements and deposit slips, contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”⁴¹⁸

In fashioning the third-party doctrine and applying it to business records, the Court thus concluded “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.”⁴¹⁹ That principle, said the Court, holds true even where, as in *Miller*, the Bank Secrecy Act forced banks to create

⁴¹⁶ *United States v. Miller*, 425 U.S. 435, 440, 442-43 (1976).

⁴¹⁷ *Miller*, 425 U.S. at 443 (citing *United States v. White*, 401 U.S. 745, 751-52 (1971)).

⁴¹⁸ *Miller*, 425 U.S. at 442.

⁴¹⁹ *Miller*, 425 U.S. at 443 (citing *White*, 401 U.S. at 752, *Hoffa*, 385 U.S. at 302, and *Lopez v. United States*, 373 U.S. 427 (1963)); see also *S.E.C. v. Jerry T. O’Brien, Inc.*, 467 U.S. 735, 743 (1984).

and maintain certain records about their customers, and where a bank was later compelled by a grand jury subpoena to turn over those records to the government.⁴²⁰

D. Warrantless Collection of Telephone Records

The rule that the Fourth Amendment does not protect information that a person has voluntarily conveyed to a third party was the foundation for the 1979 Supreme Court decision *Smith v. Maryland*, in which the Court concluded that individuals have no constitutional right of privacy in the numbers that they dial from their telephones. That decision is now the lynchpin of the government's constitutional rationale underlying the NSA's telephone records program.⁴²¹

Given the significance of the *Smith* decision, its facts bear recounting in some detail. In 1976, Michael Lee Smith robbed a woman in Baltimore, Maryland. After the robbery, he began to make threatening and obscene telephone calls to her, identifying himself as the robber, and at least once drove his car by her house to intimidate her. The police learned Smith's address from his license plate number, and asked the telephone company to install a "pen register" at its central office to record the numbers dialed from the telephone at Smith's home.⁴²² A pen register is a device that, at the time, was attached to a telephone line and recorded the numbers dialed from a telephone but was not capable of hearing or recording telephone conversations themselves. While the technology of pen registers has evolved since the 1970s, the Supreme Court explained then that the machines "decode outgoing telephone numbers by responding to changes in electrical voltage caused by the turning of the telephone dial (or the pressing of buttons on pushbutton telephones) and present the information in a form to be interpreted by sight rather than by hearing."⁴²³ The machine's name derives from the fact that early models used a pen to mark dashes on a piece of paper corresponding to each pulse from a rotary spin dial.⁴²⁴

In the *Smith* case, the police did not obtain a warrant or court order before having the pen register installed at the telephone company. On the same day that the device was installed, it revealed that a call was placed to the victim's home from Smith's telephone.

⁴²⁰ *Miller*, 425 U.S. at 443-45.

⁴²¹ *See, e.g.*, Administration White Paper, Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act, at 19-20 (Aug. 9, 2013) (citing *Smith v. Maryland*, 442 U.S. 735 (1979)).

⁴²² *Smith*, 442 U.S. at 737.

⁴²³ *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977).

⁴²⁴ "A pen register is a mechanical instrument attached to a telephone line, usually at a central telephone office, which records the outgoing numbers dialed on a particular telephone. In the case of a rotary dial phone, the pen register records on a paper tape dots or dashes equal in number to electrical pulses which correspond to the telephone number dialed." *Application of U.S. in Matter of Order Authorizing Use of a Pen Register*, 538 F.2d 956, 957 (2d Cir. 1976), *rev'd sub nom. United States v. New York Tel. Co.*, 434 U.S. 159 (1977).

Based on this and other evidence, the police then secured a warrant to search his residence, where incriminating evidence was found ultimately leading to his conviction.⁴²⁵ Appealing this conviction, Smith's attorneys argued in the Supreme Court that the installation of the pen register without a warrant violated his Fourth Amendment rights.

Because the pen register was installed at the telephone company's office, there was no trespass to Smith's property. Therefore, the Supreme Court explained, under the *Katz* test the question was whether Smith had a "legitimate expectation of privacy" that had been "invaded by government action."⁴²⁶

A divided Court concluded that no legitimate privacy interest had been violated by warrantless use of the pen register. The five-Justice majority emphasized that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications." In fact, "a law enforcement official could not even determine from the use of a pen register whether a communication existed."⁴²⁷ As the Court explained:

These devices do not hear sound. They disclose only the telephone numbers that have been dialed — a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.⁴²⁸

"Given a pen register's limited capabilities," the Court said, Smith's argument that its installation and use constituted a "search" rested upon a claim that he had a "legitimate expectation of privacy regarding the numbers he dialed on his phone."⁴²⁹

The Court rejected that claim, expressing doubt "that people in general entertain any actual expectation of privacy in the numbers they dial." All telephone users "realize that they must 'convey' phone numbers to the telephone company," the Court continued, "since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."⁴³⁰ In short, according to the Supreme Court, telephone customers have no actual, subjective expectation that the numbers they dial are private,

⁴²⁵ *Smith*, 442 U.S. at 737.

⁴²⁶ *Smith*, 442 U.S. at 740.

⁴²⁷ *Smith*, 442 U.S. at 741 (emphasis in original).

⁴²⁸ *Smith*, 442 U.S. at 741 (quoting *New York Tel. Co.*, 434 U.S. at 167).

⁴²⁹ *Smith*, 442 U.S. at 742 (internal quotation marks omitted).

⁴³⁰ *Smith*, 442 U.S. at 742.

because they “typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.”⁴³¹

Even if Michael Lee Smith did harbor a personal, subjective expectation that the numbers he dialed were private, the Court continued, that expectation was not “one that society is prepared to recognize as ‘reasonable,’” and therefore the expectation was not protected by the Fourth Amendment.⁴³² This was so, the Court said, because under the third-party doctrine described above “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”⁴³³

Applying this principle in *Smith*, the Court concluded that the suspect, by using his telephone, “voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business.”⁴³⁴ Just as a person who reveals information to a friend or associate assumes the risk that his confidant will share it with the government, a person making telephone calls assumes the risk that the telephone company will share with the government the numbers he has dialed.

The upshot of *Smith v. Maryland* is that under the Constitution the government does not need a warrant to use a pen register to obtain the telephone numbers that a person dials from his or her telephone. The government can intercept that information, as the police did in *Smith*, by installing a pen register to record those numbers.⁴³⁵ Similarly, the courts have concluded, warrants are not constitutionally required to install and use a “trap and trace” device, which monitors the *inbound* calls made to a particular telephone, much like caller-ID service.⁴³⁶ In lieu of using such devices for real-time collection, the government can issue a subpoena to the telephone company for the stored calling records of one of its customers.⁴³⁷

⁴³¹ *Smith*, 442 U.S. at 743.

⁴³² *Smith*, 442 U.S. at 743 (quoting *Katz*, 389 U.S. at 361).

⁴³³ *Smith*, 442 U.S. at 743-44.

⁴³⁴ *Smith*, 442 U.S. at 744.

⁴³⁵ In 1986, Congress adopted legislation requiring governmental entities to obtain a court order to install and use a pen register. The standard for such orders is much lower than the standard required for issuance of a warrant: a court must issue an order if the government certifies that the evidence sought is relevant to an ongoing criminal investigation. *See* 18 U.S.C. §§ 3121-3127.

⁴³⁶ *See, e.g., United States v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009); *United States v. Hallmark*, 911 F.2d 399, 402 (10th Cir. 1990). The pen register statute adopted in 1986 also requires court orders for the installation and use of trap and trace devices.

⁴³⁷ *See* 18 U.S.C. §§ 2703(c)(2), 2709.

While *Smith v. Maryland* addresses law enforcement tools of a more primitive technological era — the decision declares that the equipment that processes dialed telephone numbers “is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber” — it remains the law of the land.⁴³⁸ Many recent court decisions have relied on a broad reading of *Smith* to conclude, among other things, that there is no Fourth Amendment expectation of privacy in email addressing information, such as the “to” and “from” lines in an email.⁴³⁹

E. Comparing the NSA’s Telephone Records Program with the Surveillance Approved in *Smith v. Maryland*

In the view of the government and the FISA court, *Smith v. Maryland* settles the question of whether the NSA’s telephone records program constitutes a search under the Fourth Amendment: because people have no reasonable expectation of privacy in the numbers that they dial, collecting those numbers from a telephone company is not a “search” within the meaning of the Fourth Amendment, and therefore the Amendment simply does not apply.⁴⁴⁰ As previously noted, *Smith v. Maryland* still stands as the law of the land, and government attorneys were entitled to rely on it as the telephony metadata program was developed and approved by the court.

However, the case does not provide a good fit for the telephone records program, particularly in light of rapid technological changes and in light of the nationwide, ongoing nature of the program. The NSA’s Section 215 program gathers significantly more information about each telephone call and about far more people than did the pen register surveillance approved in *Smith* (essentially everyone in the country who uses a phone) and it has collected that data now for nearly eight years without interruption.⁴⁴¹ In contrast, the pen register approved in *Smith v. Maryland* compiled only a list of the numbers dialed from Michael Lee Smith’s telephone. It did not show whether any of his attempted calls were actually completed — thus it did not reveal whether he engaged in any telephone conversations at all. Naturally, therefore, the device also did not indicate the duration of any conversations. Furthermore, the pen register provided no information about incoming telephone calls placed to Smith’s home, only the outbound calls dialed from his telephone.

⁴³⁸ *Smith*, 442 U.S. at 744; but see Memorandum Opinion at 45, *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013) (concluding that *Smith v. Maryland* does not apply to the NSA telephone metadata program).

⁴³⁹ See, e.g., *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008).

⁴⁴⁰ See Administration White Paper at 19-20; Amended Memorandum Opinion at 6-9, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013); Memorandum at 4-6, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Oct. 11, 2013).

⁴⁴¹ The court orders authorizing the program last for only ninety days, but the concept of the program is one of indefinite collection, and since May 2006 there has never been a lapse in court approval.

The pen register was in operation for no more than two days.⁴⁴² And finally, the device recorded only the dialing information of one person: Smith himself. The police had no computerized ability to aggregate Smith's dialing records with those of other individuals and gain additional insight from that analysis.

In contrast, for each of the millions of telephone numbers covered by the NSA's Section 215 program, the agency obtains a record of all incoming and outgoing calls, the duration of those calls, and the precise time of day when they occurred. When the agency targets a telephone number for analysis, the same information for every telephone number with which the original number has had contact, and every telephone number in contact with any of those numbers. And, subject to regular program renewal by the FISA court, it collects these records every day, without interruption, and retains them for a five year time period. Sweeping up this vast swath of information, the government has explained, allows the NSA to use "sophisticated analytic tools" to "discover connections between individuals" and reveal "chains of communication" — a broader power than simply learning the telephone numbers dialed by a single targeted individual.⁴⁴³

To illustrate the greater scope of the NSA's program, the pen register discussed in *Smith* might have shown that, during the time that Michael Lee Smith's telephone was monitored, he dialed another number three times in a single day. That information could have simply evinced three failed attempts to reach the other number. The NSA's collection program, however, would show not only whether each attempted call connected but also the precise duration and time of each call. It also would reveal whether and when the other telephone number called Smith and the length and time of any such calls. Because the NSA collects records continuously and stores them for five years, it would be in a position to see how frequently those two numbers contacted each other during the preceding five years and the pattern of their contact. And because the agency would have full access to the calling records of the other telephone number as well, it could examine the activity of that other number and see, for instance, whether it ever communicated with any of the same numbers as Smith over a five-year period, or what numbers it communicated with around the time of its calls with Smith. The agency could then do the same thing for every other number that Smith had communicated with in the past five years, employing what it calls contact-chaining analysis. It could then go further and analyze the complete calling records of every number that was called by any of the numbers that ever communicated with Smith — going three "hops" from the original number.

⁴⁴² *Smith*, 442 U.S. at 737.

⁴⁴³ Administration White Paper at 13-14.

The NSA's Section 215 program, therefore, is dramatically broader than the practice approved by the Supreme Court in *Smith*, which was directed at a single criminal suspect and gathered only "the numbers he dialed on his phone" during a limited period.⁴⁴⁴

The government argues that these differences are irrelevant under the Fourth Amendment. It argues that the third-party doctrine described earlier applies whether the government is obtaining data on one person or hundreds of millions. All of the information collected by the NSA in its calling records program is recorded by telephone companies for their own business purposes. Thus, just like the numbers that a telephone user dials, all of this information has been shared with telephone companies by their customers. As long as the third-party doctrine remains in force and assuming it applies regardless of the breadth of the data acquired, the NSA's collection of calling records is not a search under the Fourth Amendment.

F. Privacy-Based Criticisms of *Smith v. Maryland* and the Third-Party Doctrine

The third-party doctrine, which serves as the constitutional underpinning of the NSA's telephone records program, has been heavily criticized by legal scholars and others. The leading academic treatise on the Fourth Amendment calls the Supreme Court's decision in *United States v. Miller*, which concluded that there are no privacy rights in bank records, "dead wrong," asserting that its "woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection the Court had developed in *Katz*."⁴⁴⁵ The same treatise opines that the Court's rationale in *Smith v. Maryland*, which applied the doctrine to telephone calling records, "makes a mockery of the Fourth Amendment."⁴⁴⁶ Even some defenders of the doctrine express the view that the Supreme Court "has never offered a clear argument in its favor."⁴⁴⁷ A number of state supreme courts have rejected the doctrine with respect to the privacy guarantees of their own constitutions, even where those constitutions mimic the language of the Fourth Amendment.⁴⁴⁸ A number of such courts have explicitly disagreed with *Smith v. Maryland's*

⁴⁴⁴ *Smith*, 442 U.S. at 742.

⁴⁴⁵ 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT §§ 2.7(b), (c) (5th ed.).

⁴⁴⁶ *Id.*

⁴⁴⁷ Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009) ("The closest the Court has come to justifying the doctrine has been its occasional assertion that people who disclose communications to a third party 'assume the risk' that their information will end up in the hands of the police. But assumption of risk is a result rather than a rationale: A person must assume a risk only when the Constitution does not protect it. Exactly why the Constitution does not protect information disclosed to third parties has been left unexplained.").

⁴⁴⁸ As of 2006, eleven states had rejected the federal third-party doctrine and ten others had given some reason to believe that they might reject it. See Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 376 (2006).

reasoning and have concluded that the use of pen registers or the collection of telephone calling records implicates protected privacy interests.⁴⁴⁹ A number of federal magistrates and judges have rejected the doctrine as applied to cell site information transmitted or stored in connection with cell phone calls.⁴⁵⁰

Many criticisms of the third-party doctrine were first voiced by Supreme Court Justices who vigorously dissented from the decisions that established it. One such critique is that the doctrine is premised on an unrealistic view of privacy expectations. In *Smith*, for example, Justice Potter Stewart argued in dissent that the “central question” was whether a person making telephone calls from his home is entitled to assume that the numbers he dials, like the words he speaks, “will not be broadcast to the world.”⁴⁵¹ In Justice Stewart’s view, “[w]hat the telephone company does or might do with those numbers is no more relevant to this inquiry than it would be in a case involving the conversation itself.”⁴⁵² Although the numbers dialed from a telephone are “more prosaic than the conversation,” he wrote, “I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person’s life.”⁴⁵³

Justice Thurgood Marshall, joined by Justice William Brennan, similarly observed in his own *Smith* dissent: “Just as one who enters a public telephone booth is ‘entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,’ so too, he should be entitled to assume that the numbers he dials in the privacy of his home will be recorded, if at all, solely for the phone company’s business purposes.”⁴⁵⁴ The legitimacy of privacy expectations, in Justice Marshall’s view, depended “not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society.”⁴⁵⁵ The use of pen registers, he continued, was an “extensive intrusion” into privacy, because of “the vital role

⁴⁴⁹ See, e.g., *Commonwealth v. Melilli*, 555 A.2d 1254, 1258 59 (Pa. 1989); *Shaktman v. State*, 553 So.2d 148, 149 51 (Fla. 1989); *State v. Thompson*, 760 P.2d 1162, 1164 67 (Idaho 1988); *State v. Gunwall*, 720 P.2d 808, 814 16 (Wash. 1986); *People v. Sporleder*, 666 P.2d 135, 140 42 (Colo. 1983); *State v. Hunt*, 450 A.2d 952, 954 57 (N.J. 1982).

⁴⁵⁰ See Testimony of Magistrate Judge Stephen W. Smith before the Subcommittee on the Constitution, Civil Rights and Civil Liberties of the House Judiciary Committee, Hearing on ECPA reform and the Revolution in location based Technologies and Service (June 24, 2010).

⁴⁵¹ *Smith*, 442 U.S. at 747 (Stewart, J., dissenting) (quoting *Katz*, 389 U.S. at 352).

⁴⁵² *Smith*, 442 U.S. at 747 (Stewart, J., dissenting).

⁴⁵³ *Smith*, 442 U.S. at 748 (Stewart, J., dissenting).

⁴⁵⁴ *Smith*, 442 U.S. at 752 (Marshall, J., dissenting) (quoting *Katz*, 389 U.S. at 352).

⁴⁵⁵ *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

telephonic communication plays in our personal and professional relationships.”⁴⁵⁶ The prospect of unregulated governmental monitoring of calling records, Justice Marshall wrote, would “undoubtedly prove disturbing even to those with nothing illicit to hide”:

Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society.⁴⁵⁷

A related critique of the third-party doctrine is that it reflects an all-or-nothing approach to privacy, under which a person’s entitlement to keep information secret is entirely vitiated whenever he or she shares that information with anyone, “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” (as the Supreme Court put it in *Miller*).⁴⁵⁸ The result of this approach is that a person who shares information with a telephone company, bank, Internet service provider, credit card company, hospital, library, pharmacy, or any other institution — even on the understanding that the information will be kept confidential — forfeits any Fourth Amendment right to prevent the government from obtaining that information from the institution with which it was shared.

In *Smith*, Justice Marshall took issue with this all-or-nothing approach: “Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.”⁴⁵⁹ Regarding bank records, for instance, he wrote: “The fact that one has disclosed private papers to the bank, for a limited purpose, within the context of a confidential customer-bank relationship, does not mean that one has waived all right to the privacy of the papers.”⁴⁶⁰ Likewise, merely because people know “that a phone company monitors calls for internal reasons, it does not follow that they expect this information to be made available to the public in general or the government in particular.”⁴⁶¹

⁴⁵⁶ *Smith*, 442 U.S. at 751 (Marshall, J., dissenting).

⁴⁵⁷ *Smith*, 442 U.S. at 751 (Marshall, J., dissenting) (internal citations omitted).

⁴⁵⁸ *Miller*, 425 U.S. at 443.

⁴⁵⁹ *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

⁴⁶⁰ *California Bankers Ass’n v. Shultz*, 416 U.S. 21, 95-96 (1974) (Marshall, J., dissenting).

⁴⁶¹ *Smith*, 442 U.S. at 749 (Marshall, J., dissenting). The fact that a bank or telephone company is itself a participant in its customers’ transactions, according to Justice Marshall, “is irrelevant to the question of

The implications of this all-or-nothing approach to privacy have grown since the 1970s, as Americans increasingly must share personal information with companies in order to avail themselves of services and products that have become typical features of modern living. Another major criticism of the third-party doctrine, which has gained increased salience in light of these developments, challenges the notion that a customer of such companies, simply by “revealing his affairs to another,” truly chooses to risk “that the information will be conveyed by that person to the Government.”⁴⁶² This criticism rejects the idea that conducting business that is essential to contemporary life represents a voluntary decision to lay bare the details of one’s habits to governmental scrutiny.

“For all practical purposes,” Justice Brennan observed in his *Miller* dissent, “the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account.”⁴⁶³ Justice Marshall, dissenting in *Smith*, expanded on this point:

Implicit in the concept of assumption of risk is some notion of choice. At least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications. By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of “assuming” risks in contexts where, as a practical matter, individuals have no realistic alternative.⁴⁶⁴

There are cases in which the Supreme Court has rejected the notion that there is no privacy interest in what is disclosed to a third party.⁴⁶⁵ The third-party doctrine was recently questioned at the Supreme Court by Justice Sonia Sotomayor, who wrote in *United States v. Jones* that the assumption-of-risk approach “is ill suited to the digital age, in which

whether a Government search or seizure is involved.” *California Bankers Ass’n*, 416 U.S. at 95 (Marshall, J., dissenting).

⁴⁶² *Miller*, 425 U.S. at 443 (citing *White*, 401 U.S. at 751-52); see *Smith*, 442 U.S. at 744.

⁴⁶³ *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) (quoting *Burrows v. Superior Court*, 529 P.2d 590, 596 (Cal. 1974)); see *id.* (“In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography.”).

⁴⁶⁴ *Smith*, 442 U.S. at 749-50 (Marshall, J., dissenting) (internal citations omitted).

⁴⁶⁵ See Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 41-43 (2011). See also *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989) (in FOIA case, finding a privacy interest in the FBI’s compilation of police rap sheets, even though the events summarized in the rap sheets had previously been disclosed to the public, noting: “In an organized society, there are few facts that are not at one time or another divulged to another.”).

people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks,” including “the phone numbers that they dial or text,” “the URLs that they visit and the e-mail addresses with which they correspond,” and “the books, groceries, and medications they purchase.”⁴⁶⁶ As this comment suggests, the lack of any meaningful option to withhold personal information from third-party institutions is even greater today than it was at the time of *Smith v. Maryland*, because of intervening developments in communications and commerce.

G. Fourth Amendment Implications of Technological Advancements

The societal developments noted above, abetted by changes in technology, have increased the range of information available to government investigators without a warrant. Meanwhile, the same technological advances fueling this trend have markedly heightened the government’s capacity to collect, aggregate, and analyze immense quantities of information — a development amply demonstrated by the NSA’s telephone records program. The Supreme Court has acknowledged that new technology has the potential to erode Fourth Amendment protections,⁴⁶⁷ and that it can also alter societal conceptions about the legitimacy of certain privacy expectations.⁴⁶⁸ Given these considerations, the Supreme Court’s decision in *Smith v. Maryland* may not forever settle the question of whether individuals have a reasonable expectation of privacy in their telephone calling records, especially in the context of bulk and indefinite collection.

The potential for enhanced surveillance technology to undermine privacy guarantees was already evident in the 1970s when the third-party doctrine was being developed by the Supreme Court — leading some Justices to warn in dissents that unless constitutional jurisprudence were to evolve in response to such developments, the liberty secured by the Fourth Amendment would irredeemably wither.

In *United States v. Miller*, for instance, Justice Brennan in his dissenting opinion noted that Fourth Amendment doctrine had long condemned “violent searches and invasions of an individual’s right to the privacy of his dwelling,” yet “[t]he imposition upon privacy, although perhaps not so dramatic, may be equally devastating when other methods are employed.”

⁴⁶⁶ *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

⁴⁶⁷ *See Kyllo*, 533 U.S. at 33-34.

⁴⁶⁸ *See Quon*, 130 S. Ct. at 2629-30 (“Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . [T]he Court would have difficulty predicting how employees’ privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable.”).

Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.⁴⁶⁹

A failure of constitutional law to respond to developing technology, Justice Marshall similarly observed in a dissent, would functionally diminish the Amendment's protections against the very sort of evils that it was designed to shield against: "Our Fourth Amendment jurisprudence should not be so wooden as to ignore the fact that through micro-filming and other techniques of this electronic age, illegal searches and seizures can take place without the brute force characteristic of the general warrants which raised the ire of the Founding Fathers."⁴⁷⁰

More recently, the Supreme Court has acknowledged that it "would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."⁴⁷¹ The Court recognized that it must sometimes confront the question of "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."⁴⁷² In a case involving a thermal-imaging device aimed at a private home from a public street, which revealed details about the interior of the home that previously could have been known only by physical entry, the Court declared use of the device to be a "search," rejecting a rigid interpretation of the Fourth Amendment that "would leave the homeowner at the mercy of advancing technology."⁴⁷³

Such technological advancement during the past thirty years, particularly in the storage, transmission, and manipulation of digital information, has allowed the NSA to institute a program of amassing and analyzing telephone records that is exponentially more far-reaching than the pen register surveillance addressed by the Supreme Court in

⁴⁶⁹ *Miller*, 425 U.S. at 451-52 (Brennan, J., dissenting) (quoting *Burrows*, 529 P.2d at 593-96).

⁴⁷⁰ *California Bankers Ass'n*, 416 U.S. at 95 (Marshall, J., dissenting) (citing *Entick v. Carrington*, 19 How. St. Tr. 1029 (1765), and *Stanford v. Texas*, 379 U.S. 476, 483-84 (1965)); see also *Smith*, 442 U.S. at 746 (Stewart, J., dissenting) (echoing observation that "the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards" (quoting *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. at 313)).

⁴⁷¹ *Kyllo*, 533 U.S. at 33-34.

⁴⁷² *Kyllo*, 533 U.S. at 34.

⁴⁷³ *Kyllo*, 533 U.S. at 35, 40.

1979. At the same time, the ubiquity of mobile phone technology has increasingly placed telephone-based connections at the center of human interaction.⁴⁷⁴

Given the unprecedented breadth of the NSA's collection of telephone records under Section 215 of the Patriot Act, coupled with the agency's enhanced ability to sift through those records and map out an individual's communications network, and in light of changes in Americans' habits caused by modern technology, it is possible that the contemporary Supreme Court — if called upon to evaluate the NSA's program under the Fourth Amendment — would not consider *Smith v. Maryland* to have resolved the question.

Reaching the conclusion that a Fourth Amendment interest was implicated by bulk, ongoing calling record collection would require the Court to scale back the third-party doctrine, a step the Court has not taken. But a recent decision, involving Global-Positioning-System ("GPS") monitoring, indicates that a majority of Justices believes that the rise of novel technological tools for the collection, aggregation, and analysis of large quantities of information demands judicial recognition that not everything an individual exposes to the public loses Fourth Amendment protection.

In *United States v. Jones*, the Supreme Court ruled that placing a GPS device on a Jeep driven by a criminal suspect, and then using the device to track the Jeep's movements continuously for four weeks, was a "search" under the Constitution. The Court's majority opinion based this conclusion on traditional, trespass-related Fourth Amendment principles: by installing a GPS device on the Jeep, the Court wrote, the government "physically occupied private property for the purpose of obtaining information," and the Court had "no doubt" that "such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."⁴⁷⁵

By focusing on the physical placement of a GPS device on the vehicle, the opinion left unresolved whether its driver reasonably could expect privacy in its whereabouts — a matter that he exposed to others by driving on public streets. "It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy," the majority said, "but the present case does not require us to answer that question."⁴⁷⁶

⁴⁷⁴ See *In re Orders Authorizing Use of Pen Registers & Trap & Trace Devices*, 515 F. Supp. 2d 325, 328 (E.D.N.Y. 2007) ("Telephone use has expanded rapidly since the constitutionality of pen registers was examined in 1979. Today, Americans regularly use their telephones not just to dial a phone number, but to manage bank accounts, refill prescriptions, check movie times, and so on.").

⁴⁷⁵ *Jones*, 132 S. Ct. at 949. As Justice Sotomayor's concurring opinion put it: "The Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection." *Id.* at 954 (Sotomayor, J., concurring).

⁴⁷⁶ *Jones*, 132 S. Ct. at 954.

Justice Samuel Alito, joined by three other justices, agreed with the majority's result, but not its reasoning, which he wrote "largely disregards what is really important . . . the use of a GPS for the purpose of long-term tracking."⁴⁷⁷ He would instead have applied the two-part *Katz* test to the GPS surveillance, asking whether monitoring the suspect's vehicle continuously for four weeks "involved a degree of intrusion that a reasonable person would not have anticipated."⁴⁷⁸ Answering that question, he concluded that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy," because in such cases "society's expectation has been that law enforcement agents and others would not — and indeed, in the main, simply could not — secretly monitor and catalogue every single movement of an individual's car for a very long period."⁴⁷⁹

Similar concerns are reflected in the concurring opinion written by Justice Sotomayor, who provided the fifth vote for the majority opinion. Agreeing with Justice Alito "that, at the very least, longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy," Justice Sotomayor wrote that, even with respect to short-term monitoring, the ability of modern technology to generate "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations" has Fourth Amendment implications deserving of special attention.⁴⁸⁰ That is particularly so, she wrote, because the government "can store such records and efficiently mine them for information years into the future."⁴⁸¹ Thus, in assessing the constitutionality of such technology with respect to GPS tracking, Justice Sotomayor wrote that the proper question is "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."⁴⁸²

The observations of Justices Alito and Sotomayor echo the rationale of the Court of Appeals decision in *Jones*, which rested on the insight that knowing the whole of a person's activity is different from knowing only parts of it, "because that whole reveals more — sometimes a great deal more — than does the sum of its parts."⁴⁸³ Prolonged surveillance, the appellate court wrote, "reveals types of information not revealed by short-term

⁴⁷⁷ *Jones*, 132 S. Ct. at 961 (Alito, J., concurring in the judgment) (emphasis in original).

⁴⁷⁸ *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

⁴⁷⁹ *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

⁴⁸⁰ *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

⁴⁸¹ *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

⁴⁸² *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

⁴⁸³ *United States v. Maynard*, 615 F.3d 544, 558 (D.C. Cir. 2010), *aff'd on other grounds sub nom. United States v. Jones*, 132 S. Ct. 945 (2012). The circuit court invoked the term "mosaic theory" to describe this phenomena.

surveillance,” and these types of information “can each reveal more about a person than does any individual trip viewed in isolation.”⁴⁸⁴

Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one’s not visiting any of these places over the course of a month. The sequence of a person’s movements can reveal still more; a single trip to a gynecologist’s office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.⁴⁸⁵

“A person who knows all of another’s travels,” the court continued, “can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts.”⁴⁸⁶

If this approach were applied to the NSA’s collection of telephone records under Section 215, it might lead to the conclusion that customers’ disclosure of calling information to a telephone company — to enable the completion and billing of individual calls — is different from relinquishing the totality of their calling histories over a five-year period for digitally facilitated analysis. Just as the sum of one’s movements in a vehicle over a four-week period tells a different story than a smattering of individual trips, the comprehensive record of a person’s entire telephone communication history over five years reveals much more than the log of a day’s worth of calls.

We stress that there is no indication that the government has used the telephone records collected under Section 215 to trace religious or political affiliations or deduce other sensitive matters. But in *Jones*, the government likewise was not using the location data to deduce who was a weekly churchgoer, a heavy drinker or an unfaithful husband, yet five Justices agreed nevertheless that the long-term collection of location data constituted a search under the Fourth Amendment.

Justice Sotomayor’s *Jones* concurrence explicitly drew a connection between her analysis of GPS monitoring and *Smith v. Maryland* and other decisions applying the third-party doctrine.⁴⁸⁷ Her concurrence suggested that “it may be necessary to reconsider the

⁴⁸⁴ *Maynard*, 615 F.3d at 562.

⁴⁸⁵ *Maynard*, 615 F.3d at 562.

⁴⁸⁶ *Maynard*, 615 F.3d at 562.

⁴⁸⁷ In defense of warrantless GPS monitoring, the government’s brief had relied on *Smith v. Maryland*, arguing that disclosure of one’s location to the public is like the disclosures of calling information to a telephone company. See Brief for the United States at 20-21, 23-24, 31-33, *United States v. Jones*, No. 10-1259 (U.S. Aug. 2011).

premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”⁴⁸⁸ She elaborated:

This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.⁴⁸⁹

As the disclosure of such information to third parties becomes more and more unavoidable, Justice Sotomayor observed, American society may or may not develop concomitant expectations of privacy in the confidentiality of this information vis-à-vis the government. But such expectations “can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.”⁴⁹⁰ Echoing and citing Justice Marshall’s dissenting opinion in *Smith v. Maryland*, Justice Sotomayor concluded: “I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.”⁴⁹¹

H. Relevance of the Third-party Doctrine to the NSA Telephone Records Program

Beyond generalized criticisms of the third-party doctrine, the more pertinent question may be whether the doctrine can be stretched to exempt from Fourth Amendment scrutiny a program as broad and long-running as the Section 215 telephone metadata program. That program goes far beyond anything that has ever before been upheld under the doctrine. As suggested by the observations of Justices Alito and Sotomayor in *United States v. Jones*, collectively representing the views of five Justices, the Supreme Court might find that the third-party doctrine, regardless of its validity as applied to traditional pen/trap devices and particularized subpoenas, does not apply to the compelled disclosure of data on a scope as broad and persistent as the NSA’s telephone records program. One district court has recently stated an argument for limiting the third-party doctrine in a case challenging the constitutionality of the NSA telephone records program. In *Klayman v. Obama*, Judge Richard Leon analyzed in detail the changes in technology since *Smith* was

⁴⁸⁸ *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

⁴⁸⁹ *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

⁴⁹⁰ *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

⁴⁹¹ *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing *Smith*, 442 U.S. at 749 (Marshall, J., dissenting)).

decided in 1979 and compared the capabilities of the pen register at issue in *Smith* to the scope of the NSA telephone records program. He concluded that “present-day circumstances” are “so thoroughly unlike those considered by the Supreme Court thirty-four years ago” that *Smith* should not apply to analysis of the telephone records program.⁴⁹²

However, the decision in *Klayman v. Obama*, which the government has appealed, represents the opinion of a single district court judge. Illustrating the deep split among courts over the breadth of the third-party doctrine, a different district court has upheld the 215 program on the basis of *Smith v. Maryland*.⁴⁹³ Until the Supreme Court rules otherwise, *Smith v. Maryland* and the third-party doctrine remain in force today. Government lawyers are entitled to rely on them when appraising the constitutionality of a given action.

I. Implications of Regarding the Metadata Program as a “Search”

If the Supreme Court reversed or narrowed *Smith*, for example, by holding that certain bulk collections of data were covered by the Fourth Amendment, this would establish only that the NSA’s collection of telephone records pursuant to Section 215 of the Patriot Act is a “search” under the Fourth Amendment. The next question would be whether this search — carried out to prevent international terrorism, not to prosecute ordinary crimes after they have been committed — requires a warrant. The Supreme Court has left open the question of whether there is a “foreign intelligence exception” to the Fourth Amendment’s warrant requirement that permits the executive branch to engage in warrantless surveillance “with respect to the activities of foreign powers, within or without this country.”⁴⁹⁴ A number of lower courts have concluded that such an exception exists “when the object of the search or the surveillance is a foreign power, its agent or collaborators.”⁴⁹⁵

⁴⁹² Memorandum Opinion at 45, *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013).

⁴⁹³ See Memorandum & Order at 38-44, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013).

⁴⁹⁴ *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. at 308. When the Court ruled in *Katz* that warrantless government eavesdropping on telephone conversations violates the Constitution, it was careful to note that “a situation involving the national security” might call for a different result, and that in such situations “safeguards other than prior authorization by a magistrate” might satisfy the Fourth Amendment’s reasonableness requirement. *Katz*, 389 U.S. at 358 n.23. A few years later, the Court concluded that there is no exception to the Fourth Amendment’s warrant requirement for domestic national security surveillance that does not involve foreign powers. *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. at 324. The legitimacy of warrantless foreign intelligence surveillance has never been resolved by the Court, see *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1010 (FISA Ct. Rev. 2008), in part because the passage of FISA in the late 1970s established a statutory framework for such surveillance that was followed by the executive branch until the events of September 11, 2001.

⁴⁹⁵ *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980); accord *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973). In more recent years, the

If no warrant is required for the government to collect telephone records in pursuit of foreign intelligence, a further decision would have to be made about whether the NSA's collection of these records under Section 215 is constitutionally "reasonable," which would involve balancing the governmental interests at stake with the program's intrusion into privacy.⁴⁹⁶

J. "Just Because We Can Do Something Doesn't Mean We Necessarily Should"⁴⁹⁷

To hold, as most courts have, that telephony metadata enjoys no privacy protection under the Fourth Amendment does not mean that such data is without privacy implications. Telephone calling records, especially when assembled in bulk, clearly implicate privacy interests as a matter of public policy. The significance of those privacy implications is magnified in the digital era. Although the government may rely on *Smith v. Maryland* and the third-party doctrine when formulating legal arguments, whether it should, as matter of sound public policy, make use of the fullest extent of its authority under current Fourth Amendment doctrine is a different question. The comprehensive scope of the 215 program is enabled by technology that did not exist when the Supreme Court decided *Smith v. Maryland*. While reaping the benefit of such technological prowess, the NSA's program relies on a legal doctrine formulated before the privacy implications of such technology could be factored into the Court's Fourth Amendment calculus. This legal doctrine, moreover, was fashioned at a time when American life did not involve sharing confidential information with as wide a range of institutions as it does today, and before telephone-based communication was as pervasive a feature of life.

It should be remembered that the *Katz* standard for evaluating the application of the Fourth Amendment was not always the standard. For almost forty years, from 1928, in *Olmstead v. United States*, reinforced by *Goldman v. United States*, in 1942, the Fourth Amendment trigger was physical penetration. The development of electronic surveillance technology, allowing the government to listen to and record telephone booth conversations electronically, led the Supreme Court to revise its approach to the Fourth Amendment. Now, forty-seven years after *Katz*, with dramatic changes in technology, including the

Foreign Intelligence Surveillance Court of Review has found such an exception for surveillance "directed at a foreign power or an agent of a foreign power reasonably believed to be located outside the United States." *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d at 1011.

⁴⁹⁶ In *Klayman v. Obama*, the court concluded that, in light of "serious doubts about the efficacy of the metadata collection program" and the program's infringement on "that degree of privacy" that the Founders enshrined in the Fourth Amendment, the "plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government's interest in collecting and analyzing bulk telephony metadata and therefore the NSA's bulk collection program is indeed an unreasonable search under the Fourth Amendment." Memorandum Opinion at 62-64, *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013).

⁴⁹⁷ Press Conference by the President (Dec. 20, 2013), available at <http://www.whitehouse.gov/the-press-office/2013/12/20/press-conference-president>.

ability to record calling data for almost every citizen on an ongoing basis, may be the occasion for the Supreme Court to, once again, expand on the Fourth Amendment to protect citizens' calling patterns. These Fourth Amendment questions are currently being litigated in several cases pending in federal court which may ultimately find their way to the Supreme Court. We explore the policy questions in the next section of this Report, where we weigh the privacy interests implicated by the Section 215 program against the national security benefits it provides.

III. FIRST AMENDMENT

The First Amendment to the United States Constitution protects several fundamental rights including the freedoms of speech and association. The Amendment reads:

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Although the amendment's text does not explicitly refer to a freedom of association, the Supreme Court has long held that the First Amendment freedom of speech encompasses the "freedom to associate with others for the common advancement of political beliefs and ideas."⁴⁹⁸

A. Freedom of Association Entails Privacy of Association

The Court first described the freedom of association as a critical constitutionally protected right in *NAACP v. Alabama* in 1958. In that case, the NAACP challenged a state court order requiring it to disclose its membership lists. The NAACP objected that revealing the identities of its members would impair the rights of these individuals to engage in "lawful association in support of their common beliefs." In finding that this claim deserved constitutional protection, the Supreme Court stated: "Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly."⁴⁹⁹ In subsequent years, the Supreme

⁴⁹⁸ *Kusper v. Pontikes*, 414 U.S. 51, 56-57 (1973).

⁴⁹⁹ *NAACP v. Alabama*, 357 U.S. 449, 460 (1958) (internal citations omitted). The Court rejected the State of Florida's assertion that it was entitled to the membership lists in order to assess whether the NAACP was doing business in the state without properly registering.

Court made clear that this freedom of association is grounded in the First Amendment.⁵⁰⁰ The freedom of association is thus protected as “an indispensable means of preserving” the First Amendment right of freedom of speech and other individual liberties.⁵⁰¹ It protects not only actual speech, but also the associations among people, especially when they come together to advance common beliefs such as those on political, religious, cultural or economic matters.⁵⁰²

Government action may impinge on such First Amendment rights even if it is not directly aimed at limiting freedom of speech or association. The Supreme Court has recognized that the First Amendment “rights of free speech and association . . . are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference.”⁵⁰³ In particular, disclosure of associations among individuals, and of connections between individuals and advocacy groups, can have a chilling effect on the exercise of associational rights that impinges on these constitutional freedoms. In originally outlining the freedom of association in *NAACP v. Alabama*, the Court explained that individuals should be free not only to join together in advocacy but also to do so without fear that their associations will be revealed, noting that:

It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one’s associations.⁵⁰⁴

The Court continued by noting that this safeguard was particularly important “where a group espouses dissident beliefs.”⁵⁰⁵ Thus, the constitutional guarantee of

⁵⁰⁰ See *Buckley v. Valeo*, 424 U.S. 1, 15 (1976) (noting that after *NAACP v. Alabama*, “[s]ubsequent decisions have made clear that the First and Fourteenth Amendments guarantee freedom to associate with others for the common advancement of political beliefs and ideas”) (internal quotation marks omitted).

⁵⁰¹ *Roberts v. U.S. Jaycees*, 468 U.S. 609, 618 (1984).

⁵⁰² See *NAACP v. Alabama*, 357 U.S. at 460-61.

⁵⁰³ *Gibson v. Florida Legislative Investigation Committee*, 372 U.S. 539, 544 (1963) (internal citations and quotation marks omitted) (finding disclosure requirement chilled freedom of association); see also *NAACP v. Alabama*, 357 U.S. at 461 (“In the domain of these indispensable liberties, whether of speech, press, or association . . . abridgement of such rights, even though unintended, may inevitably follow from varied forms of governmental action.”). An *indirect* intrusion on First Amendment rights, such as that caused by disclosure requirements, can still have a serious chilling effect on associational rights and be subject to exacting scrutiny as described below.

⁵⁰⁴ *NAACP v. Alabama*, 357 U.S. at 462.

⁵⁰⁵ *NAACP v. Alabama*, 357 U.S. at 462.

associational rights under the First Amendment “encompasses protection of privacy of association in organizations.”⁵⁰⁶

The protection for privacy of association stems from recognition that individuals who support controversial causes may be subject to harassment or intimidation if their connections with organizations promoting these causes are disclosed.⁵⁰⁷ The Court has also acknowledged the need to protect privacy where revealing associations to the government could subject an individual to detrimental government action. For example, the Court struck down a requirement that public school teachers identify all the organizations in which they were members, noting that “the pressure upon a teacher to avoid any ties which might displease those who control his professional destiny would be constant and heavy.”⁵⁰⁸

Since first recognizing this right to privacy in one’s associations, the Court has found in numerous cases that rules requiring disclosure of affiliations violated the First Amendment because they had a chilling effect that undermined the freedom of association.⁵⁰⁹ However, the Court has held that a disclosure requirement can be consistent with the First Amendment where it is closely tied to a compelling state interest.⁵¹⁰

Accordingly, the right to associate privately is not absolute, nor are all government actions that reveal connections among individuals constitutionally suspect. The test to be applied in assessing whether the government action violates the First Amendment depends

⁵⁰⁶ *Gibson*, 372 U.S. at 544.

⁵⁰⁷ Early cases recognized the pressures on NAACP supporters in the civil rights era. *See NAACP v. Alabama*, 357 U.S. at 462; *Gibson v. Florida Legislative Investigation Committee*, 372 U.S. at 556-57 (finding that privacy of association is “all the more essential here, where the challenged privacy is that of persons espousing beliefs already unpopular with their neighbors”). Later cases recognized the same dynamic in the case of minor political parties such as the Socialist Workers Party. *See Brown v. Socialist Workers ‘74 Campaign Comm.*, 459 U.S. 87 (1982).

⁵⁰⁸ *Shelton v. Tucker*, 364 U.S. 479, 486 (1960).

⁵⁰⁹ *See, e.g., Brown*, 459 U.S. at 88 (holding Ohio law requiring disclosure of political party’s campaign contributors and recipients of campaign disbursements violated First Amendment freedom of association); *Baird v. State Bar of Arizona*, 401 U.S. 1 (1971) (holding that the “First Amendment’s protection of association” prohibits states from inquiring about individuals’ membership in Communist Party in connection with applications for law licenses); *Gibson*, 372 U.S. at 558 (prohibiting state from compelling organization to reveal which of its members also appeared on a list of suspected members of the Communist party); *see also Buckley v. American Constitutional Law Foundation, Inc.*, 525 U.S. 182, 204 (1999) (holding that rules requiring disclosure of identities of individuals who paid to circulate ballot initiatives violated First Amendment).

⁵¹⁰ *See John Doe No. 1*, 130 S. Ct. 2811 (2010) (upholding state public records requirement that to initiate any citizen referendum, proponents must file petition disclosing names of signers, where most referenda involved uncontroversial matters and state had important interest in preserving integrity of electoral process).

on the strength of the chilling effect. Government actions that may significantly chill the exercise of this right by forcing disclosure of individuals' associations to the government are subject to "exacting scrutiny."⁵¹¹ This is a high standard, but it is not an impossible test. As the Supreme Court explained in *John Doe No. 1 v. Reed*, this "standard requires a substantial relation between the disclosure requirement and a sufficiently important governmental interest. To withstand this scrutiny, the strength of the governmental interest must reflect the seriousness of the actual burden on First Amendment rights."⁵¹²

Thus, where there is a significant chilling effect, a court must assess the importance of the government's interest alongside the degree to which its action interferes with the freedom of association. In balancing these two considerations, the court will also evaluate whether the government may be able to achieve its purposes through means that are less intrusive on constitutionally protected liberties: "If the State has open to it a less drastic way of satisfying its legitimate interests, it may not choose a legislative scheme that broadly stifles the exercise of fundamental personal liberties."⁵¹³ In *John Doe No. 1*, the Court considered a Public Records Act requirement that to initiate any citizen referendum, proponents must file a petition disclosing the names of signers. The Court found that the disclosure requirement was closely tied to the state's important interest in preserving the integrity of the electoral process, and held that this interest was sufficient to justify the chilling effect of this disclosure requirement.⁵¹⁴

The Supreme Court stressed the element of overbreadth in holding that a conviction for failing to turn over the NAACP membership list to a legislative committee investigating the Communist Party's activities violated the First Amendment. The Court stressed that the state should demonstrate a nexus between the illegal conduct it is investigating and the organization whose members it seeks to identify. While noting that it did not deny "the existence of the underlying legislative right to investigate . . . subversive activities by Communists or anyone else," the Court instructed that "groups which themselves are neither engaged in subversive or other illegal or improper activities nor demonstrated to have any substantial connections with such activities are to be protected in their rights of free and private association."⁵¹⁵

⁵¹¹ *John Doe No. 1*, 130 S. Ct. at 2818.

⁵¹² *John Doe No. 1*, 130 S. Ct. at 2818 (internal citations and quotation marks omitted); see also *Buckley v. Valeo*, 424 U.S. at 25 (stating that even a "significant interference with protected rights of political association may be sustained if the State demonstrates a sufficiently important interest and employs means closely drawn to avoid unnecessary abridgment of associational freedoms") (internal citations omitted).

⁵¹³ *Kusper*, 414 U.S. at 58-59 (finding Illinois statute restricting voting in primaries infringes upon the right of free political association protected by the First and Fourteenth Amendments).

⁵¹⁴ *John Doe No. 1*, 130 S. Ct. at 2819.

⁵¹⁵ *Gibson v. Florida Legislative Investigation Committee*, 372 U.S. at 557-58.

A less stringent test applies if a court finds that the chilling effect of the government action is not significant. In the context of a minor political party's attempt to open its primary election to all voters contrary to the existing state voting system, the Supreme Court stated that while "severe burdens on associational rights" are subject to "strict scrutiny," a much lower standard of review applies when "regulations impose lesser burdens."⁵¹⁶ Where the burden on the freedom of association is minimal, the state's "important regulatory interests will usually be enough to justify reasonable, nondiscriminatory restrictions."⁵¹⁷ Thus, the rigor of the Court's inquiry will depend on the degree to which the government action is found to burden associational rights.

B. The NSA's Telephone Records Program Implicates the First Amendment

Although the NSA's telephone records program does not include an overt disclosure requirement of the type evaluated in such cases as *NAACP v. Alabama*, its operation similarly results in the compulsory disclosure of information about individuals' associations to the government. Like the government's collection of membership lists, its bulk collection of telephone records makes that information available for government analysis and can create a chilling effect on those whose records are being collected. As discussed in the next part of this Report, telephone metadata can be highly revealing of the patterns of individuals' connections and associations, including the frequency of all contacts among individuals and organizations. The networks revealed will necessarily include individuals' connections with advocacy groups and others whose political, social, religious, or cultural missions the individuals support — the type of associations at the core of the Constitution's protection for freedom of association.

The Supreme Court has acknowledged that government surveillance programs can implicate First Amendment rights in addition to Fourth Amendment rights.⁵¹⁸ Most

⁵¹⁶ *Clingman v. Beaver*, 544 U.S. 581, 586-87 (2005). The case involved a state primary election system that only permitted the Libertarian Party of Oklahoma to open its primary to its own members and registered independents. The Court found that the state's refusal to permit registered members of other political parties to vote in the Libertarian Party's primary did not limit the party's capacity to communicate with the public and its members or to recruit new members. The Court therefore found that the rule only "minimally" burdened the party's freedom of association. *Id.* at 587-90.

⁵¹⁷ *Id.* at 586-87.

⁵¹⁸ *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. at 313 ("National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech.") Some courts of appeals have concluded that government surveillance that complies with Fourth Amendment standards will also survive scrutiny under the First Amendment. *See, e.g., Reporters Committee for Freedom of the Press v. American Telephone and Telegraph Company*, 593 F.2d 1030, 1058 (D.C. Cir. 1978) (holding telephone companies' release of toll call records to law enforcement did not violate First or Fourth Amendment); *Gordon v. Warren Consol. Bd. Of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983) (holding surveillance by undercover officer did not violate First or Fourth Amendments).

recently, Justice Sonia Sotomayor noted in her concurring opinion in *United States v. Jones* that “[a]wareness that the Government may be watching chills associational and expressive freedoms.”⁵¹⁹ However, in the cases decided so far, the Court has not reached the underlying question of whether the First Amendment has been violated, because the Court has found that the individuals challenging the surveillance program are not legally entitled to do so because they are unable to show that they are directly affected by the monitoring.

In *Laird v. Tatum*, for instance, the Supreme Court considered a challenge to an Army program that gathered information on “public activities that were thought to have at least some potential for civil disorder” in order to enable contingency planning for how the government should respond in the event of such disorder.⁵²⁰ The Court found that the individuals who filed the lawsuit were not legally entitled to challenge the government program, because they could only point to their “knowledge that a governmental agency was engaged” in a “data-gathering” plan and their fear that “in the future” they might suffer from some detrimental action as a result.⁵²¹ Most recently, the Supreme Court held in *Clapper v. Amnesty International USA* that attorneys and advocacy groups could not challenge the FISA Amendments Act in court because they could not show that they themselves were imminently likely to be subject to surveillance.⁵²² The Court did not reach the question of whether the surveillance under that program would have a sufficient chilling effect to implicate First Amendment rights.⁵²³

Some federal courts of appeals have considered cases in which there was not a standing issue and have more explicitly recognized the impact of government surveillance

⁵¹⁹ *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

⁵²⁰ *Laird v. Tatum*, 408 U.S. 1, 6 (1972).

⁵²¹ *Laird*, 408 U.S. at 10-11. The Court held that the plaintiffs lacked legal standing to bring their challenge.

⁵²² *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). The question of whether an individual is entitled to bring such a legal challenge is separate from the question of whether a surveillance program actually infringes First Amendment rights. The chilling effect that a surveillance program may impose on speech and association may implicate the First Amendment and yet still not be sufficient to support an individual’s right to file a lawsuit. As the U.S. Court of Appeals for the District of Columbia Circuit has explained: “The harm of ‘chilling effect’ is to be distinguished from the immediate threat of concrete, harmful action. The former consists of present deterrence from First Amendment conduct because of the difficulty of determining the application of a regulatory provision to that conduct, and will not by itself support standing. The latter — imminence of concrete, harmful action such as threatened arrest for specifically contemplated First Amendment activity — does support standing.” *United Presbyterian Church in the U.S.A. v. Reagan*, 738 F.2d 1375, 1380 (D.C. Cir. 1984) (finding individuals lacked standing to challenge Executive Order 12333, which sets forth the framework for U.S. intelligence gathering).

⁵²³ The Court noted in passing that previous cases “had held that constitutional violations may arise from the chilling effect of regulations that fall short of a direct prohibition against the exercise of First Amendment rights,” but found that the attorneys and organizations lacked legal standing to bring the lawsuit since they did not show “specific present objective harm or a threat of specific future harm.” *Clapper v. Amnesty International USA*, 113 S. Ct. at 1151-53 (internal quotation marks and citations omitted).

upon First Amendment rights. For example, in a case challenging FBI electronic surveillance of an organization's headquarters, one court noted that the fear of electronic surveillance could chill "free and robust exercise of the First Amendment rights of speech and association,"⁵²⁴ citing in particular the harmful impact of permitting the government to review the names and addresses of the many individuals who called the organization.⁵²⁵ Similarly, another appeals court found that individuals were entitled to challenge a surveillance program of the City of Albuquerque Police Department where the individuals alleged that they were the targets of police surveillance, that the city maintained files on their activities, and that this caused a chilling effect on their First Amendment rights.⁵²⁶

Furthermore, Congress has recognized that collection of information under Section 215 can implicate the free exercise of speech and associational activities. In reauthorizing Section 215 in 2006, Congress added safeguards for government applications seeking records that directly implicate particular constitutional protections; specifically, Congress required that applications for 215 orders seeking such records be signed by high level officials and provided that this authority may not be delegated to lower level personnel.⁵²⁷ That requirement covers applications seeking records that are especially sensitive from the standpoint of the First Amendment right to free speech and association, such as library circulation records and patron lists and book sales records and customer lists.⁵²⁸

By indefinitely collecting information about all Americans' telephone calls, the NSA's telephone records program clearly implicates the First Amendment freedoms of speech and association. The connections revealed by the extensive database of telephone records gathered under the program will necessarily include relationships established among

⁵²⁴ *Zweibon v. Mitchell*, 516 F.2d 594, 633 (D.C. Cir. 1975) (holding warrant required for surveillance of organization even though conducted for foreign intelligence, and finding that "prior judicial review [of warrant process] can serve to safeguard both First and Fourth Amendment rights"). This case involved surveillance for foreign intelligence purposes and predates passage of the Foreign Intelligence Surveillance Act. However, its analysis of the First Amendment interests at stake is still relevant to our inquiry.

⁵²⁵ *Id.* at 634-35.

⁵²⁶ *Riggs v. City of Albuquerque*, 916 F.2d 582 (10th Cir. 1990) (reversing district court's dismissal for lack of standing in case challenging surveillance program as unconstitutional). The federal courts of appeals have also considered a variety of cases in which individuals alleged that government surveillance had chilled their First Amendment rights and the courts found a lack of standing to bring such claims. *See, e.g., ACLU v. NSA*, 493 F.3d 644 (6th Cir. 2007) (dismissing constitutional challenge to Terrorist Surveillance Program for lack of standing).

⁵²⁷ *See* 50 U.S.C. § 1861(a)(3).

⁵²⁸ The amendment to Section 215 also provided special treatment for records of firearms sales that are sensitive under the Second Amendment. *See* 50 U.S.C. § 1861(a)(3). In addition, Section 215 requires that if the government seeks to collect information about a U.S. person, the application for a 215 order may not be sought "solely upon the basis of activities protected by the first amendment to the Constitution." 50 U.S.C. § 1861(a)(1). While this latter requirement pertains to the evidence used to justify a Section 215 collection rather than the information obtained through an order, it nonetheless shows a recognition that collection of information about individuals can impact their freedom to engage in First Amendment activities.

individuals and groups for political, religious, and other expressive purposes. Compelled disclosure to the government of information revealing these associations can have a chilling effect on the exercise of First Amendment rights.

Any First Amendment inquiry must next ask whether the chilling effect of the program is significant or only minimal, since this will determine the applicable legal standard for review. If the chilling effect is found to be minimal, then the program is not subject to stringent review. If, however, the burden is found to be significant, then the “exacting scrutiny” test applies, and the question becomes whether the government possesses “a sufficiently important interest and employs means closely drawn to avoid unnecessary abridgment of associational freedoms.”⁵²⁹

As we explain in the next section of this Report, the NSA’s bulk collection of telephone records can be expected to exert a substantial chilling effect on the activities of journalists, protestors, whistleblowers, political activists, and ordinary individuals. This effect stems from the government’s collection of telephony metadata and the knowledge that the government has access to millions of individuals’ records — regardless of whether the individuals have any suspected connection to terrorist activity. More particularized methods of government access to data do not create the same broad impact, because individuals can expect that their records will not be collected unless they are connected to a specific criminal or terrorism investigation. We think the likely deterrence of these associational activities by the 215 bulk collection program rises to the level of a “significant interference” with the protected rights of political association, and thus the exacting scrutiny test should apply.

Combatting terrorism is a compelling government interest that may justify intrusions on First Amendment rights.⁵³⁰ However, we find it doubtful that the NSA’s program satisfies the requirement that the program be drawn narrowly to minimize the intrusion on associational rights.⁵³¹ As with the legislative investigation at issue in *Gibson*

⁵²⁹ *Buckley*, 424 U.S. at 25.

⁵³⁰ *See Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2730-31 (2010) (finding government’s compelling interest in counterterrorism overcame First Amendment speech and association interests of organization seeking to teach peaceful tactics to designated terrorist groups).

⁵³¹ *See Buckley*, 424 U.S. at 25; *Gibson*, 372 U.S. at 557-58 (in First Amendment challenge to law enforcement investigation by state legislature seeking disclosure of NAACP’s membership list, emphasizing that the state should demonstrate a nexus between the illegal conduct it is investigating and the organization whose members it seeks to identify, finding this nexus lacking, and instructed that “groups which themselves are neither engaged in subversive or other illegal or improper activities nor demonstrated to have any substantial connections with such activities are to be protected in their rights of free and private association”).

discussed above, the NSA program gathers information about individuals who have no demonstrated connection to illegal activities.

However, as with the Fourth Amendment questions described above, we note that the right of association questions are likely to be assessed in litigation that is already proceeding in the courts. However, we can say clearly that the 215 program implicates First Amendment rights — rights that must be considered in any policy assessment of the program. In the next section of this Report, we explore from a *policy* perspective the nature and strength of the chilling effect created by the telephone records program. We examine, as a matter of policy, whether the national security benefits provided by the calling records program outweigh its implications for privacy and civil liberties. In that assessment we consider the program's effectiveness and balance its value against its intrusions on privacy as well as on speech and association.

Part 7:
POLICY ANALYSIS AND RECOMMENDATIONS REGARDING
THE NSA SECTION 215 PROGRAM

I. Introduction

Even where measures taken to protect the nation from terrorism comply with the law and the Constitution, the question remains: do they strike the proper balance between security and liberty, between the need to safeguard the nation and to uphold the freedoms that define it? The 9/11 Commission, which first recommended the creation of our Board, expressed a firm belief that striking the proper balance is attainable and essential. As the Commission said in its report:

We must find ways of reconciling security with liberty, since the success of one helps protect the other. The choice between security and liberty is a false choice, as nothing is more likely to endanger American's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend.⁵³²

Consistent with the importance of reconciling security and liberty, the Board's statutory role includes the duty to "analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties."⁵³³

Below, we set forth the capabilities that the NSA's bulk collection of telephone records offers in the government's effort to safeguard the nation from terrorism. We then discuss the extent to which the program has contributed in a demonstrable way to that effort. Next, we explore the threats to privacy and civil liberties entailed by such a wide-scale assembly of communications records by the government. Finally, we provide our assessment of how the value of the NSA's program weighs against its implications for privacy and civil liberties and our assessment of how security and liberty concerns can best be reconciled with respect to this program.

⁵³² 9/11 Commission Report at 395; *see also* 42 U.S.C. § 2000ee(b)(3) (quoting 9/11 Commission Report).

⁵³³ 42 U.S.C. § 2000ee(c)(1).

II. The Terrorism Threat and the Challenges of Combating It

The threat of terrorism faced today by the United States is real. While the core group of Al Qaeda that planned the 9/11 attacks from Afghanistan largely has been decimated by military action, recent years have seen the rise of new al Qaeda affiliates in other nations plotting operations against the United States and Europe. President Obama described the emergence of these groups in a speech last May on the dangers currently posed by international terrorism: “From Yemen to Iraq, from Somalia to North Africa, the threat today is more diffuse, with Al Qaeda’s affiliates in the Arabian Peninsula — AQAP — the most active in plotting against our homeland.”⁵³⁴ Most of these affiliates presently are focused on executing attacks in their own regions, but such attacks can claim U.S. lives in addition to wreaking devastation on residents of the nations where they occur. Moreover, failed attacks against the United States, such as the attempted 2009 Christmas Day airplane bombing and the attempted 2010 Times Square bombing, serve as a reminder that foreign terrorist organizations continue to pose a danger to residents of this nation.

Political upheavals in the Middle East, meanwhile, threaten to create opportunities for safe havens where new terrorist affiliates can plan attacks. At the same time, the United States has seen evidence that radicalized individuals inside this country with connections to foreign extremists can carry out horrifying acts of violence, as appears to have been the case with the shooting at Fort Hood in Texas and the bombing of the Boston Marathon.⁵³⁵

Thus, while al Qaeda’s core group has not carried out a successful attack on U.S. soil since 2001 and is less capable of doing so, and while the violence now being attempted by emergent terrorist affiliates has not yet approached the scope of the 9/11 attacks, the danger posed to the United States by international terrorism is by no means over.⁵³⁶

Communications are essential to the facilitation of a terrorist attack against the United States, but awareness of those same communications can permit the United States to discover and thwart the attack. A key challenge — and a key opportunity — facing those who are tasked with preventing terrorism is that would-be terrorists utilize the same communications networks as the rest of the world. Identifying the communications of individuals plotting terrorism within those networks, without intruding on the communications of law-abiding individuals, is a formidable task. This challenge is compounded by the fact that terrorists, aware that attempts are being made to uncover

⁵³⁴ Remarks by the President at the National Defense University, Fort McNair, Washington, D.C. (May 23, 2013), available at <http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university>.

⁵³⁵ *See id.*

⁵³⁶ *See id.*

their communications, may employ a range of measures to evade those efforts and keep their plans secret.

III. Capabilities Provided by the NSA's Bulk Collection of Telephone Records

Because communication by telephone is useful, if not indispensable, in the coordination of terrorist efforts, would-be terrorists can be expected to employ this method of communication in planning and carrying out their violent attacks. Records of telephone calls therefore can serve as a trail helping counterterrorism investigators piece together the networks of terrorist groups and the patterns of their communications. Ultimately, such analysis can support the intelligence community's efforts to identify and locate individuals planning terrorist attacks and to discover and disrupt those attacks before they come to fruition.

The NSA's wholesale collection of the nation's telephone records, under the authority granted by the FISA court pursuant to Section 215, is but one method of gathering and analyzing telephone records for counterterrorism purposes. As described below, this method offers certain logistical advantages that may not be available through other means of gathering calling records. The broad scale of this collection, however, even when combined with strict rules on the use of the records obtained, carries serious implications for privacy and civil liberties.

A. Alternative Means of Collecting Telephone Records

Apart from the NSA's bulk collection program, the government has several means at its disposal to obtain telephone calling records for use in counterterrorism or criminal investigations.

Under the Electronic Communications Privacy Act ("ECPA"), which governs communications records, a governmental entity can use an administrative, grand jury or trial subpoena to require a telephone company to provide calling records to the government.⁵³⁷ The government can also use a judicial warrant or court order issued under ECPA or the Federal Rules of Criminal Procedure to compel disclosure of calling records,⁵³⁸ though it primarily relies on subpoenas.

When utilizing a grand jury subpoena, the government is entitled to whatever records it seeks unless there is "no reasonable possibility" that its request "will produce information relevant to the general subject of the grand jury's investigation."⁵³⁹ Under a

⁵³⁷ See 18 U.S.C. § 2703(c)(2).

⁵³⁸ See 18 U.S.C. § 2703(c)(1)(B); FED. R. CRIM. P. 41.

⁵³⁹ *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).

provision of ECPA dealing with counterterrorism and counterintelligence investigations, the government also can issue a national security letter (“NSL”) to a telephone company directing it to provide calling records to the government.⁵⁴⁰ These NSLs, which are a form of administrative subpoena, do not require permission from a court. To issue an NSL, a government official must certify in writing to the company that the records being sought are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.”⁵⁴¹

In order to obtain telephone records using either subpoenas or NSLs, the government must specify the phone numbers or other identifiers for which it is seeking records and it must reasonably believe that those records have some connection to a criminal or counterterrorism investigation. The government cannot use these authorities preemptively to collect records concerning numbers that it has no reason to believe are connected to such an investigation, with the intent of looking at them later when it develops some particularized suspicion.

Court orders, subpoenas, and NSLs can all entail a delay between the point at which the government becomes suspicious about a particular number and the point at which it obtains the calling records of that number. Even though judicial approval is not required when the government issues a subpoena or NSL, it takes some time for governmental personnel to assure themselves that the proper conditions for the use of the subpoena or NSL have been met, obtain the necessary supervisory approval, deliver the request to the telephone company, and receive the records back from the company. The government does have means available, however, to streamline this process and eliminate delays. It has been reported, for instance, that one telephone company has placed its employees in offices of the Drug Enforcement Agency with access to the company’s call records database, to disclose records pursuant to administrative subpoenas.⁵⁴² Under a similar arrangement, from April 2003 through January 2008, employees of certain communications providers were located at the FBI’s Communications Assistance Unit, where they accessed call records databases in response to NSLs.⁵⁴³ The on-site providers’ employees would deliver

⁵⁴⁰ See 18 U.S.C. § 2709(a), (b).

⁵⁴¹ 18 U.S.C. § 2709(b)(1). If the investigation is of a U.S. person, it cannot be conducted solely on the basis of activities protected by the First Amendment to the Constitution. *Id.*

⁵⁴² See Scott Shane and Colin Moynihan, Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.’s, *The New York Times* (Sept. 1, 2013) (“The government pays AT&T to place its employees in drug-fighting units around the country. Those employees sit alongside Drug Enforcement Administration agents and local detectives and supply them with the phone data from as far back as 1987.”).

⁵⁴³ See A Review of the Federal Bureau of Investigation’s Use of Exigent Letters and Other Informal Requests for Telephone Records, Oversight Review Division, Office of the Inspector General, at 24 (January 2010), available at <http://www.justice.gov/oig/reports/FBI/index.htm>.

records to the FBI in an electronic format compatible with FBI databases, using compact disks and email.⁵⁴⁴

Normally, obtaining records with a subpoena or NSL only provides the government with the telephone contacts of the original number about which information is sought. However, at least in the past, NSLs and grand jury subpoenas have requested of at least one telephone company, which had this capacity, a “community of interest” for specified telephone numbers — going beyond the direct contacts of the target number.⁵⁴⁵ It could therefore be possible for the government to seek contacts out to two hops in the contact chain through such alternate tools, although an individual request would only cover a single provider’s records.

When using court orders, subpoenas, or NSLs, the government is able to obtain only those records that the telephone company has retained on file. Data retention practices vary among providers. Telephone service providers currently are required by regulation to maintain records of the calls made by each telephone number only for eighteen months.⁵⁴⁶ Even during that limited period, some providers switch the format in which calling records are stored from digital formats — which enable quick searching and analysis — to less accessible formats such as back-up tapes. On the other hand, it has been reported that one provider’s database includes calls dating back twenty-six years.⁵⁴⁷

B. Logistical Advantages of Collecting Telephone Records in Bulk

Under Section 215, the NSA does not limit its collection of telephone records to those with a suspected terrorism connection. Instead, orders of the FISA court permit the agency to collect potentially all of the calling records generated by United States telephone companies on a daily basis. Those records are maintained for five years in the NSA’s databases. When the agency develops a “reasonable articulable suspicion” that a particular telephone number is associated with terrorism, the agency may view and analyze the complete calling records of that number, along with the complete calling records of all the numbers it has been in contact with, and the complete calling records of all the numbers that those numbers have been in contact with.⁵⁴⁸

⁵⁴⁴ *Id.* at 52.

⁵⁴⁵ *Id.* at 54-64. The IG stated that one company had particular capabilities to conduct community of interest searches, which it made available to the FBI under contract.

⁵⁴⁶ *See* 47 C.F.R. § 42.6.

⁵⁴⁷ Scott Shane and Colin Moynihan, Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.’s, *The New York Times* (Sept. 1, 2013).

⁵⁴⁸ *See* Part 3 of this Report for a more detailed description of the NSA’s collection and analysis of telephone calling records.

This arrangement provides the government with three main logistical advantages: greater speed, greater historical depth, and greater breadth of records available for analysis.

1. Speed

Under the NSA's bulk telephone records collection program, at the point when the agency learns that a particular telephone number may be associated with terrorism and worth investigating, the agency's database already contains the calling records of numbers that have been in contact with the number to be investigated. The only significant delay comes from the time required for agency personnel to assure themselves that the "reasonable articulable suspicion" standard for that number has been met — and, with respect to a number believed to be used by a U.S. person, that the agency's suspicions are not based solely on activity protected by the First Amendment. Once the necessary reviews have been conducted, the calling records associated with a telephone number — up to three "hops" away from that number — can be retrieved nearly instantaneously.

In contrast, obtaining the calling records of a particular number by subpoena or NSL might take days or longer. And this process would normally reveal only the direct contacts of the target number, although as noted, it could be possible to acquire contacts out to two hops. This alternative process would require separate subpoenas or NSLs to be directed to each provider; the NSA would then need to compile the results and check for connections among them.

2. Historical Depth

By collecting telephone records soon after they are created and storing them for five years, the NSA guarantees their continued availability during that period. Thus when the agency searches for the records of a telephone number of interest, it will have at its disposal calling records extending back five years.

In contrast, if the NSA waited to collect the records of a particular number until it came under suspicion, much of the older calling history of that number may not be available. As noted, telephone companies are required to maintain the records of an individual telephone call for eighteen months only. Beyond that, retention periods vary widely. A company receiving a government request for the records of a particular number might be able to furnish only a year and a half of records.

The farther back a telephone number's calling records stretch, the more telephone calls they will reveal. The NSA asserts that a greater historical depth of records therefore is more likely to show connections with numbers of interest. A larger historical repository of a suspect's calling records also may permit the NSA to better understand the typical

communications pattern of that suspect, alerting the agency to unusual or aberrational activity.

3. Breadth

Once the NSA develops reasonable suspicion about a particular telephone number, the agency is able to view and analyze all the telephone contacts made by that number (a first “hop”), all the contacts made by every number identified at the first tier (a second “hop”), and all the contacts made by every number identified at the second tier (a third “hop”). In contrast, obtaining telephone records through alternative means — absent the community of interest approach described above — would normally provide the agency with only the first tier: the immediate contacts of the original number. Although investigators could then pursue the full calling records of any of those contacts, based upon the information discernable at the first tier, automatic access to additional tiers provides insight that might not be gained any other way.

For instance, if target A is in contact with another number, B, that is unknown to the NSA, and if the timing, frequency, and pattern of their calls suggest nothing out of the ordinary, the agency might have no articulable reason to obtain the full calling records of B. Those records, however, might show that B is in contact with C, a number that is of high interest to the agency. Notwithstanding the agency’s lack of information about B, the calling records thus would have shown a “two hop” link between A and C. Such information could help analysts piece together a connection between suspects who were not previously known to be connected. The same information might also suggest that B is a number of potential interest to the agency — something that would not be fully apparent from the mere fact that B had been in contact with A.

In another hypothetical example, the same calling records might show that target A frequently contacts numbers D, E, and F. Viewing the full calling records of those three numbers might reveal that E and F also frequently communicate with each other, and always around the same time that one of them has been in touch with A. Number D, on the other hand, might have no evident connection to any of A’s other contacts. This information might lead investigators to prioritize E and F in their inquiry, while deemphasizing D. The relationship between E and F would not have been apparent by looking only at A’s first-tier contacts, and as a result investigators might not have explored those two numbers further.

Thus, immediate access to a second tier of contacts offers the promise of fleshing out networks of linked individuals in a way that working step-by-step, one tier of contacts at a time, may not. The difference is not merely that additional time is saved because the agency does not have to make a new request for each number. Rather, as a matter of practical reality, that new number might never be pursued at all. Simply put, the pressures of limited time and resources may deter investigators from further examining some important first-

tier contacts whose significance becomes apparent only when a second tier of calling records is automatically available. Losing that automatic access may translate into losing some degree of analytic insight.

IV. Demonstrated Efficacy of the NSA's Bulk Collection of Telephone Records

Clearly, the NSA's bulk acquisition of telephone records provides the government with certain capabilities that would otherwise be lacking in the endeavor to combat terrorism. But the question remains whether those capabilities have demonstrably enhanced the government's efforts to safeguard the nation. Answering this question requires examining the instances in which telephone records obtained by the NSA under Section 215 of the Patriot Act were used in counterterrorism investigations. That examination in turn must seek to ascertain whether similar results could have been achieved using telephone records obtained through other means.

Any attempt to assess the value of the NSA's telephone records program must be cognizant of a few considerations. First, the information that the NSA obtains through Section 215 is not utilized in a vacuum. Rather, it is combined with information obtained under different legal authorities, including the Signals Intelligence that the NSA captures under Executive Order 12333, traditional wiretaps and other electronic surveillance of suspects conducted under FISA court authority, the interception of telephone calls and emails authorized by the FISA Amendments Act of 2008, the collection of communications metadata through FISA's pen register and trap and trace provision, physical surveillance, and the development of informants. The intelligence community views the NSA's Section 215 program as complementing and working in tandem with these and other intelligence sources, enabling analysts to paint a more comprehensive picture when examining potential national security threats.

Moreover, what the Section 215 program yields is the identification of telephone numbers of potential interest, or the revelation of connections between telephone numbers of interest, which must be passed on to the FBI or other agencies as leads for further investigation. Any assessment of the program's value, and any expectations about what it can be expected to accomplish, must bear this consideration in mind.

Finally, an intelligence-gathering tool like the NSA's Section 215 program can provide value that materially enhances the safety of the nation even if it never provides the single critical piece of insight enabling the government to thwart an imminent terrorist attack. Because the work of intelligence gathering and analysis is cumulative, it is rare that any particular technique or legal authority can be identified as the key component without which a terrorist plot would have succeeded. Intelligence-gathering tools can provide value

in more indirect ways, by helping to advance investigations and focus efforts in ways that are sometimes more difficult to measure.

That being said, in the Board's view, an intelligence-gathering tool with significant ramifications for privacy and civil liberties cannot be regarded as justified merely because it provides *some* value in protecting the nation from terrorism. Particularly when an intelligence program reaches as broadly as the NSA's bulk collection of telephone records — potentially touching the lives of nearly every American, and in the process investing considerable power in the hands of the government to monitor the communication patterns of its citizens — we believe it is necessary to measure the value provided by the program by considering whether comparable results could be achieved through less intrusive means and whether any unique value offered by the program outweighs its implications for privacy and civil liberties.

In our effort to carry out this balancing task with respect to the NSA's Section 215 program, we have examined a wealth of classified materials regarding the operation of the program. As we have reviewed such materials, the intelligence community has provided us with follow-up information responding to specific questions or concerns we have posed to them. We have taken public testimony from government officials and have received a series of classified briefings with a range of personnel from the NSA and other elements of the intelligence community. We have spoken with representatives of private companies who have received and complied with court orders under the NSA's surveillance program. We have heard from academics, technology experts, civil liberties advocates, and former government officials through written submissions provided to us and through commentary at public workshops that we have conducted.

In particular, we have closely scrutinized the specific cases cited by the government as instances in which telephone records obtained under Section 215 were useful in counterterrorism investigations. In the wake of the unauthorized disclosures during the summer of 2013, the intelligence community compiled a list of fifty-four counterterrorism events in which Section 215 or Section 702 of the FISA Amendments Act of 2008 "contributed to a success story." Twelve of those incidents involved the use of Section 215. We have examined those incidents in depth, attempting to discern precisely what was accomplished in each case through the use of Section 215 records and whether similar results could have been achieved using more tailored means of gathering telephone records.

Our deliberations have led us to conceptualize seven broad ways in which an intelligence-gathering tool such as the NSA's bulk telephone records program can provide value in safeguarding the nation from terrorism. We explain these seven categories of success below and discuss how often the NSA's Section 215 program has achieved each of them.

Our analysis suggests that where the telephone records collected by the NSA under its Section 215 program have provided value, they have done so primarily in two ways. The first is by offering additional leads regarding the contacts of terrorism suspects already known to investigators, which can help investigators confirm suspicions about the target of an inquiry or about persons in contact with that target. But our review suggests that the Section 215 program offers little unique value here, instead largely duplicating the FBI's own information-gathering efforts. The second is by demonstrating that known foreign terrorism suspects do *not* have U.S. contacts or that known terrorist plots do *not* have a U.S. nexus. This can help the intelligence community focus its limited investigatory resources by avoiding false leads and channeling efforts where they are needed most. But the value of this benefit must be kept in perspective, as discussed below.

Based on the information provided to the Board, we have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. In that case, moreover, the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program.

Even in those instances where telephone records collected under Section 215 offered additional information about the contacts of a known terrorism suspect, in nearly all cases the benefits provided have been minimal — generally limited to corroborating information that was obtained independently by the FBI. And in those few cases where some information not already known to the government was generated through the use of Section 215 records, we have seen little indication that the same result could not have been obtained through traditional, targeted collection of telephone records. The classified briefings and materials the Board has received have not demonstrated that the increased speed, breadth, and historical depth of the Section 215 program have produced any concrete results that were otherwise unattainable. In other words, we see little evidence that the unique capabilities provided by the NSA's *bulk* collection of telephone records actually have yielded material counterterrorism results that could not have been achieved without the NSA's Section 215 program.

As noted, the Board has examined closely the twelve cases compiled by the intelligence community in which telephone records collected under Section 215 “contributed to a success story” in a counterterrorism investigation. We have assigned each of these cases to one or more of seven “categories of success” that we have devised to illustrate the different forms of value that a counterterrorism program like this one could

provide. We do not ascribe any talismanic significance or scientific precision to these broad, non-mutually exclusive categories. But we believe they help illustrate what the Section 215 program has and has not accomplished to date. These seven categories, and our analysis of how the government's twelve examples fit within them, are as follows:

1. Enabling "Negative Reporting." Analysis of telephone calling records can establish that a known terrorism suspect overseas has *not* been in telephone contact with anyone in the United States, suggesting that a known terrorist or terrorist plot in a foreign country does *not* have a U.S. nexus. Such information can help the government focus its limited investigative resources where they are needed most. We found five instances in which Section 215 records were used in this way.

2. Adding or Confirming Details. Analysis of telephone calling records can also help focus investigative efforts by providing additional information about terrorism suspects or plots already known to the government. The information obtained might confirm suspicions about a suspect, enable greater understanding about that suspect's connections, or establish links between known suspects. We found seven instances in which Section 215 telephone records served this function. The value provided by the records, however, was limited. In nearly every case, the information supplied by the NSA through Section 215 offered no unique value, but simply mirrored or corroborated information that the FBI obtained independently using other means. And in none of these cases did the rapid speed with which Section 215 records can be analyzed lead to any tangible benefits. In sum, we believe that the limited value provided by the Section 215 program in these cases could have been achieved without the NSA's bulk collection of telephone records.

3. "Triaging." In time-sensitive scenarios, where investigators have reason to believe that a terrorist attack may be imminent, or where they are otherwise conducting a fast-breaking investigation, prompt analysis of a suspect's telephone records may help the government prioritize leads based on their urgency. While this category is not fundamentally different from the previous one, as it also involves adding more information about plots or suspects already known to the government, its special value may lie in the potentially critical production of swift results. We identified four instances in which telephone numbers derived from the Section 215 program were disseminated quickly to the FBI in this type of scenario. In none of these cases, however, did the information contribute to the disruption of a terrorist attack.

4. Identifying Terrorism Suspects. Analysis of telephone records can contribute to the discovery of terrorism suspects previously unknown to the government. We found only one instance in which Section 215 telephone records arguably served this purpose and helped to identify a previously unknown suspect. In that case, however, the suspect was not involved in planning a terrorist attack — rather, he had sent money to support a foreign terrorist organization — and there is reason to believe that the FBI may have discovered him without the information it received from the NSA.

5. Discovering U.S. Presence of Known Terrorism Suspects. The use of Section 215 records theoretically could help alert the government that a known terrorism suspect has entered the United States from abroad. We are not aware of any instances in which this has occurred.

6. Identifying Terrorist Plots. The Board is not aware of any instances in which the use of Section 215 telephone records directly contributed to the discovery of a terrorist plot.

7. Disrupting Terrorist Plots. The Board is not aware of any instances in which the use of Section 215 telephone records directly contributed to the disruption of a terrorist plot.

To help illustrate the concrete benefits provided by the NSA's Section 215 program, we elaborate below on four counterterrorism investigations that members of the intelligence community have cited as demonstrating successful use of the program. These cases, which are among the twelve "success stories" referenced above, have been discussed by government officials in public statements, legal filings, and congressional testimony.⁵⁴⁹ We believe that scrutiny of these examples demonstrates the limited value provided by the NSA's Section 215 program.

⁵⁴⁹ Although the Board has benefitted from classified information obtained directly from members of the Intelligence Community, some information about these four cases has been made available to the public. *See, e.g.*, Declaration of Acting Assistant Director Robert J. Holley, Federal Bureau of Investigation, ¶¶ 24-26, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Oct. 1, 2013); Hearing of the Senate Appropriations Committee on Cybersecurity: Preparing for and Responding to the Enduring Threat, 113th Cong. (June 12, 2013); Hearing of the House Permanent Select Committee on Intelligence on How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries, 113th Cong. (June 18, 2013); Hearing of the House Judiciary Committee on Oversight of the Administration's Use of the Foreign Intelligence Surveillance Act (FISA) Authorities, 113th Cong. (July 17, 2013); Hearing of the Senate Judiciary Committee on Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs, 113th Cong. (July 31, 2013). Transcripts of much of this congressional hearing testimony are available at <http://icontherecord.tumblr.com/>.

A. New York City Subway Attack Plot

Since the disclosure of the NSA's Section 215 and Section 702 programs, one of the most frequently discussed cases in which these programs were utilized has been the thwarted 2009 plot to bomb the New York City subway. Section 215, however, played no role in disrupting this attack. It made a minor contribution by providing corroborating information about one of the plot's already known coconspirators, who was arrested months after the plot was disrupted. There is no reason to believe that bulk collection of telephone records was necessary for this minor contribution.

On September 6 and 7, 2009, the NSA intercepted emails sent from an unknown individual in the United States to an Al Qaeda courier in Pakistan whom it was monitoring. These emails sought advice on the correct mixture of ingredients to use for certain explosives, and the urgency of their tone suggested an imminent attack. The NSA passed this information on to the FBI, which used a national security letter to identify the unknown individual as Najibullah Zazi, located near Denver, Colorado. Beginning on September 7, the FBI set up 24-hour surveillance of Zazi's residence, began monitoring his Internet activity, and undertook other investigative efforts.

On September 8, Zazi conducted Internet searches suggesting that he was looking for home improvement stores in Queens, New York, where he could purchase acid that can be used in explosives. That same day, he rented a car. The next day, Zazi began driving from Colorado to New York City, arriving on September 10. His plan, he later said, was to meet up with associates, obtain and assemble the remaining components to build explosives, and detonate them on subway lines in Manhattan.

The FBI followed Zazi as he drove from Colorado to New York. By this time, over 100 agents from the Bureau's Denver field office were working on the investigation, and the Bureau's New York field office also became involved, along with local New York City law enforcement — by one account “every terrorism squad in New York City.”⁵⁵⁰

After arriving in New York, Zazi learned that law enforcement was monitoring him. His suspicions may have been triggered when he was pulled over by police on September 10 as he crossed the George Washington Bridge, for what he was told was a random drug search. After consenting to an inspection of his vehicle, he was allowed to proceed. Any suspicions Zazi might have had were confirmed when an associate of his tipped him off about the government's investigation. About the time of Zazi's arrival in New York, law enforcement agents working on the investigation interviewed Ahmad Wais Afzali, an imam whom the government allegedly had used in the past as an informant. These agents showed

⁵⁵⁰ Transcript of Jury Trial, *United States v. Mohammed Wali Zazi*, Crim. No. 10-0060 (E.D.N.Y. July 18, 2011) (Testimony of Eric Jurgenson, Special Agent, Federal Bureau of Investigations, Denver Field Office, National Security Squad 3).

Afzali photos of Zazi and asked questions about him. Thereafter, Afzali spoke by phone with Zazi and related to him what the authorities had asked about him.

Having been alerted about the government's investigation, Zazi purchased an airline ticket and returned to Colorado on September 12. He later stated that he and his associates abandoned their plans after learning that the government was monitoring him.

On September 14, two days after Zazi returned to Colorado, government agents searched three apartments in a Queens neighborhood. The agents found components that could be used to make bombs, along with evidence tying these materials to Zazi. The FBI first interviewed him on September 16 at the Bureau's Denver field office, where he appeared voluntarily with counsel, and he was arrested on September 19. Initially denying any involvement in terrorism, he later admitted his guilt and cooperated with investigators. Several other individuals were arrested in connection with the plot as well.

While Section 215 was used during the Zazi investigation, it played no role in thwarting the subway bombing plot. The plot was discovered through email monitoring, and its details were fleshed out through additional electronic surveillance, physical surveillance, and other traditional investigative measures. The plot was disrupted when law enforcement inadvertently tipped off Zazi that he was being monitored, leading him and his associates to abandon their plans and prompting him to return to Colorado. Although the NSA provided the FBI with a report early in the investigation showing calls made from Zazi's telephone, and later provided additional leads based on the Section 215 data, these reports did not identify Zazi's associates in New York City or the apartments where materials intended to support the bombing were found. Rather, other investigative techniques led to those discoveries.

The only concrete result obtained in the Zazi case through the use of Section 215 was to identify an unknown telephone number of one of Zazi's New York coconspirators, Adis Medunjanin. The FBI, however, already was aware of Medunjanin and his connection to Zazi's plot, having obtained that information independently using other means. And while the NSA's information may have further heightened the FBI's interest in Medunjanin, there is no indication that use of the NSA's bulk collection program was necessary for the government to identify the unknown telephone number, or that this information was not obtainable through more traditional law enforcement techniques. Despite being under suspicion from the outset of the plot's discovery in September 2009, Medunjanin was not arrested until January 2010, several months after Zazi returned to Colorado and was taken into custody. As far as we can tell, the particular speed associated with Section 215 queries offered no apparent benefit in corroborating the FBI's interest in Medunjanin. Nor did the ability to search through five years of records or to have immediate access to several "hops" of telephone calls.

The Zazi case shows how Section 215 is used to complement other investigative tools, as intelligence community officials have emphasized. In our view, it also illustrates the minimal added benefit provided by the program in light of those other tools.

B. Operation Wi-Fi

Our analysis of another 2009 case, which involved an early stage plot to attack the New York Stock Exchange, also fails to demonstrate that the Section 215 program has offered significant added value to the government's counterterrorism efforts.

While conducting Internet surveillance of an extremist based in Yemen, the NSA discovered a connection between that extremist and an unknown person in Kansas City, Missouri. The NSA provided information about this connection to the FBI. In the course of its investigation, the FBI subsequently identified the unknown person as an individual named Khalid Ouazzani, and it discovered that he was in communication with other individuals located in the United States who were in the very initial stages of devising a plan to bomb the New York Stock Exchange. All of these individuals eventually were convicted for their roles in the nascent plot.

After the FBI discovered the plot and identified the individuals involved, the NSA queried telephone numbers associated with those individuals using Section 215, providing additional telephone numbers as leads to the FBI. Those numbers simply mirrored information about telephone connections that the FBI developed independently using other authorities.

Thus, while Section 215 was used in the Operation Wi-Fi investigation, we are aware of no indication that bulk collection of telephone records was necessary to the investigation, or that the information produced by Section 215 provided any unique value.

C. David Coleman Headley Investigation

In October 2009, Chicago resident David Coleman Headley was arrested and charged for his role in plotting to attack the Danish newspaper that published inflammatory cartoons of the Prophet Mohammed. He was later charged with helping orchestrate the 2008 Mumbai hotel attack, in collaboration with the Pakistan-based militant group Lashkar-e-Taiba. He pled guilty and began cooperating with authorities.

Headley, who had previously served as an informant for the Drug Enforcement Agency, was identified by law enforcement as involved in terrorism through means that did not involve Section 215. Further investigation, also not involving Section 215, provided insight into the activities of his overseas associates. In addition, Section 215 records were queried by the NSA, which passed on telephone numbers to the FBI as leads. Those numbers, however, only corroborated data about telephone calls that the FBI obtained independently through other authorities.

Thus, we are aware of no indication that bulk collection of telephone records through Section 215 made any significant contribution to the David Coleman Headley investigation.

D. Basaaly Moalin Investigation

The investigation of Basaaly Moalin is the only case in which Section 215 records demonstrably contributed to the identification of an unknown terrorism suspect.

In 2007, the NSA provided the FBI with information showing an indirect connection between a telephone number in Somalia, which the NSA was tracking because of its association with the Al Shabaab terrorist organization, and an unknown telephone number in San Diego. The NSA reported this information to the FBI, which realized that the telephone number was linked to pending FBI investigations. Based on the NSA's report and the link between this telephone number and pending investigations, the FBI opened a preliminary investigation into the number.

Using a national security letter and database checks, the FBI identified the user of the San Diego telephone number as Basaaly Moalin, the subject of a previous FBI investigation that was closed several years earlier for lack of sufficient information. The FBI reopened the case, and through subsequent investigation it learned that Moalin and three others were providing material support to Al Shabaab. All four men were convicted in 2013 of providing funds to the terrorist organization.

The NSA's report was the catalyst that prompted the FBI to investigate Moalin's San Diego number. Even without the NSA's tip-off, however, FBI agents may well have discovered that the number was a common link among pending FBI investigations. Moreover, given that the NSA's tip came from monitoring a specific foreign number it was tracking, it is not clear to us that bulk collection of telephone records was necessary to discovering the connection between this number and Moalin's. Conventional techniques may have been less likely to discover it, or at least more time-consuming. But we know of no indication that speed or Section 215's five-year depth of records were important to the discovery.

In addition, we believe it worthy of note that Moalin and his associates were not charged or convicted of involvement in planning or executing any specific terrorist plots. Their crime was sending money to Al Shabaab. While there is a critical value in cutting off funds to deadly foreign terrorist organizations such as this one, we find it significant that in the seven-year history of the NSA's Section 215 program, this material-support prosecution remains the only time that the program has directly contributed to the identification of an unknown terrorism suspect. And even in this instance, as noted, Moalin was not entirely unknown to law enforcement, but rather was the subject of a previous FBI investigation and was the user of a telephone number already linked to pending FBI investigations.

In our view, therefore, it is telling that the Moalin case represents perhaps the strongest success story produced by the NSA's Section 215 program. Like the other three cases discussed above, the Moalin investigation shows that the program does provide some demonstrable value in supporting the government's counterterrorism efforts. But it also starkly illustrates the limits of what the program has accomplished, and perhaps what it is capable of accomplishing.

E. Remaining Success Stories

Three of the remaining cases included among the government's twelve "success stories" are similar to the narratives described above. In these three cases, the NSA queried Section 215 telephone records and passed information on to the FBI to be used as leads in its investigations. But in all three cases, that information simply mirrored or corroborated intelligence that the FBI obtained independently through other means. In none of these cases has the Board identified any unique value supplied to the FBI by the Section 215 program. Nor can the Board point to any concrete way in which the program altered the outcome of these investigations.

The last five success stories provided by the government are all examples of "negative reporting," as described above — situations in which the Section 215 data helped investigators eliminate the possibility of a U.S. connection to a foreign terrorist plot. While the value of such "peace of mind" is not to be discounted, especially in time-sensitive scenarios where it may permit investigators to better focus their attention on the true threats, it also must be kept in perspective. Particularly in light of the policy considerations discussed below, we question whether the government's routine collection of all Americans' telephone records is justified on the basis that it can be helpful to identify situations where there is *no threat* to the United States.

F. 9/11

Some have suggested that if the NSA's calling records program were in place before 9/11, it could have alerted the government that one of the future airplane hijackers was in the United States, and perhaps have led to the prevention of the attacks. For several years, beginning in the late 1990s, the NSA intercepted telephone calls to and from a prominent Al Qaeda safe house in Yemen. A number of calls were made in early 2000 between this safe house and a person named Khalid, who after 9/11 was identified as hijacker Khalid al-Mihdhar. Although the NSA was able to listen to these conversations, it did not have the telephone number that was calling the safe house, and thus it did not know that Mihdhar made the calls from San Diego, California. Had the NSA known this information, it is argued, the government could have identified Mihdhar as the caller and been aware of his presence

in the United States, perhaps leading to his apprehension and the identification and detention of other hijackers.⁵⁵¹

For two reasons, we do not believe the Mihdhar example supports continuance of the NSA's Section 215 program. First, the failure to identify Mihdhar's presence in the United States stemmed primarily from a lack of information sharing among federal agencies, not of a lack of surveillance capabilities. As documented by the 9/11 Commission and others, this was a failure to connect the dots, not a failure to collect enough dots. Second, in order to have identified the San Diego telephone number from which Mihdhar made his calls, it was not necessary to collect the entire nation's calling records.

As explained by the 9/11 Commission Report, the joint inquiry into the 9/11 attacks by the House and Senate intelligence committees, and a Department of Justice Inspector General report, the government had ample opportunity before 9/11 to pinpoint Mihdhar's location, track his activities, and prevent his 2001 reentry into the United States. By early 2000, the CIA was aware of Mihdhar and knew that he had a visa enabling him to travel to the United States. Yet despite having information that Mihdhar and fellow hijacker Nawaf al-Hazmi "were traveling to the United States," the CIA "missed repeated opportunities to act based on the information in its possession." The agency did not advise the FBI of what it knew or "add their names to watchlists."⁵⁵² Furthermore, at the time that Mihdhar and Hazmi were in San Diego in early 2000, when the calls to Yemen were made, they were living with "a long-time FBI asset."⁵⁵³ Mihdhar left the United States in June 2000, and he was able to return in 2001 because he still had not been placed on any watchlists. And "[o]n four occasions in 2001, the CIA, the FBI, or both had apparent opportunities to refocus on

⁵⁵¹ The executive branch has highlighted the Mihdhar case in its applications to the FISA court seeking authorization for the NSA's program, in litigation defending the program in other courts, and in briefing papers provided to the congressional intelligence committees urging the extension of Section 215's sunset date. Officials have also discussed the case in congressional testimony. *See, e.g.*, Testimony of General Keith Alexander, Commander, U.S. Cyber Command, Director of the National Security Agency and Chief of the Central Security Service, Hearing of the Senate Appropriations Committee on Cybersecurity: Preparing for and Responding to the Enduring Threat, 113th Cong. (June 12, 2013); Testimony of the Honorable Robert S. Mueller, III, Director, Federal Bureau of Investigation, Hearing before the Committee on the Judiciary, House of Representatives: Oversight of the Federal Bureau of Investigation, 113th Cong. (June 13, 2013); Testimony of Sean Joyce, Deputy Director, Federal Bureau of Investigation, Hearing of the House Permanent Select Committee on Intelligence on How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries, 113th Cong. (June 18, 2013).

⁵⁵² Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence: Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, S. Rep. No. 107-351, H.R. Rep. No. 107-792, at 12-16 (Dec. 2002).

⁵⁵³ Office of the Inspector General, Department of Justice, A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks, Chapter 5 (Nov. 2004), *available at* <http://www.justice.gov/oig/special/0506/chapter5.htm>.

the significance of Hazmi and Mihdhar and reinvigorate the search for them.”⁵⁵⁴ Yet these opportunities were missed.⁵⁵⁵

It is argued, however, the NSA’s bulk telephone records program could have made up for these intelligence lapses and failures of information sharing. Knowledge that the telephone calls from “Khalid” to the Yemen safe house were made from San Diego theoretically could have led the government to discover Mihdhar’s presence in the United States. But obtaining this knowledge did not require a bulk telephone records program. The NSA knew the telephone number of the Yemen safe house. If the telephone calls with Mihdhar were deemed suspicious at the time, the government could have used existing legal authorities to request from U.S. telephone companies the records of any calls made to or from that Yemen number. Doing so could have identified the San Diego number on the other end of the calls.⁵⁵⁶ Thus we do not believe that a program that collects all telephone records from U.S. telephone companies was necessary to identify Mihdhar’s location in early 2000, nor that such a program is necessary to make similar discoveries in the future.

Finally, in the absence of evidence that the NSA’s Section 215 program has made any significant contribution to counterterrorism efforts to date, some officials have suggested to us that the program should be preserved because it might do so in the future. Like a burglar alarm or a fire insurance policy, under this reasoning, the program is valuable even if it has not yet been triggered by a break-in or a fire. Yet, it is worth noting that the program supplied no advance notice of attempted attacks on the New York City subway, the failed Christmas Day airliner bombing, or the failed Times Square car bombing. Given the limited value this program has demonstrated to date, as outlined above, we find little reason to expect that it is likely to provide significant value, much less essential value, in safeguarding the nation in the future.

V. Privacy and Civil Liberties Implications of the NSA’s Bulk Collection of Telephone Records

Having described what we believe to be the value of the NSA’s telephone records program in combating terrorism, we now turn to the implications of that program for privacy and civil liberties. We believe those implications are serious. The design of the NSA’s program shows that the government recognizes the privacy concerns raised by the

⁵⁵⁴ THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, at 266 (2004).

⁵⁵⁵ See 9/11 Commission Report at 266-72.

⁵⁵⁶ The government could have sought this information through any of the alternative means of seeking telephone records described earlier, although the speed with which telephone companies could respond to such requests would likely vary by provider.

collection and analysis of telephone calling records. The government has responded to those concerns by imposing rules that limit the NSA's use of telephone records after their collection by the agency. These rules offer many valuable safeguards designed to curb the intrusiveness of the program. But in our view, they cannot fully ameliorate the implications for privacy, speech, and association that follow from the government's ongoing collection of virtually all telephone records of every American.

Because telephone calling records can reveal intimate details about a person's life, particularly when aggregated with other information and subjected to sophisticated computer analysis, the government's collection of a person's entire telephone calling history has a significant and detrimental effect on that person's privacy. Beyond such individual privacy intrusions, permitting the government to routinely collect the calling records of the entire nation fundamentally shifts the balance of power between the state and its citizens. Moreover, as outlined below, this practice can be expected to have a chilling effect on the free exercise of speech and association, because law-abiding individuals and groups engaged in sensitive or controversial work cannot trust in the confidentiality of their relationships as revealed by their calling patterns. Finally, for the reasons explained below, we do not believe that these concerns are eliminated by the detailed rules placed on the NSA's use of telephone calling records after their collection.⁵⁵⁷

A. The Revealing Nature of Telephone Calling Records

Telephone calling records, which indicate who called whom, at what time, and for how long, but do not include the contents of any conversations, are a form of "metadata."⁵⁵⁸ Like the address on the outside of an envelope, which announces the envelope's destination but does not reveal the content of the letter inside, telephone calling records provide information about the existence and details of a call without revealing what was said.

⁵⁵⁷ In assessing the privacy intrusions associated with the NSA's bulk collection of telephone records, the widely recognized Fair Information Practice Principles ("FIPPs") help inform our analysis. The FIPPs offer guidance for privacy safeguards that have formed the basis for the Privacy Act of 1974 and many federal agencies' approaches to privacy protection. See Federal Trade Commission, Fair Information Practice Principles, available at <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>. The Department of Homeland Security describes the FIPPs as a set of eight principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. Department of Homeland Security, Privacy Policy Guidance Memorandum, No. 2008-01, at 1 (Dec. 29, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (memorializing DHS adoption of the FIPPs).

⁵⁵⁸ Telephony metadata might also include cell site location information, but the NSA does not presently obtain location information as part of its collection efforts under Section 215. The technological infrastructure through which the NSA receives calling records from the telephone companies supports the collection of cell site location information but the information is filtered out. As recently as 2010 and 2011, the government has confirmed, the NSA conducted a pilot project to test the collection of cell site information about mobile telephones. See Charlie Savage, *In Test Project, N.S.A. Tracked Cellphone Locations*, N.Y. TIMES (Oct. 2, 2013). The information that is collected by the NSA under Section 215 does include telephone area codes, prefixes, and other data that allows the agency to locate callers geographically in a very broad sense.

But while telephone calling records are distinct from the spoken content of any conversation, they can be highly revealing nonetheless. As Justice Stewart noted over thirty years ago, the telephone numbers that a person dials “easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person’s life.”⁵⁵⁹ Because the circumstances of a particular call can be highly suggestive of its content, the mere record of a call potentially offers a window into the caller’s private affairs. Some illustrative examples cited by a privacy advocacy organization include the following: calling a suicide prevention hotline; calling a telephone sex service at 2:30 a.m.; calling an HIV testing service, then one’s doctor, then one’s health insurance company within the same hour; receiving a call from the local NRA office during a campaign against gun legislation, then calling one’s congressional representatives immediately afterward; and calling one’s gynecologist, speaking for half an hour, then calling the local Planned Parenthood number later that day.⁵⁶⁰

At bottom, telephone metadata is information about a person’s conduct. Just as it reveals something about a person to know that he or she visited the doctor’s office, likewise it reveals something about that person to know that he or she called the doctor’s office on the telephone. When the government collects metadata about its citizens, therefore, it is collecting information about its citizens’ activity.

Moreover, when the government collects *all* of a person’s telephone records, storing them for five years in a government database that is subject to high-speed digital searching and analysis, the privacy implications go far beyond what can be revealed by the metadata of a single telephone call. The frequency with which two numbers are in contact with each other, along with the timing and duration of their calls, provides insight into the nature of the relationship between the two callers. When both of those numbers are in contact with a third number, the pattern of calls among these three numbers adds to the story that can be gleaned from their communications records. Thus, aggregation of numerous calling records over an extended period of time can paint a clear picture of an individual’s personal relationships and patterns of behavior. This picture can be at least as revealing of those relationships and habits as the contents of individual conversations — if not more so.⁵⁶¹

⁵⁵⁹ *Smith*, 442 U.S. at 748 (Stewart, J., dissenting).

⁵⁶⁰ Kurt Opsahl, *Why Metadata Matters*, EFF.ORG (June 7, 2013), available at <https://www.eff.org/deeplinks/2013/06/why-metadata-matters>.

⁵⁶¹ All four expert technologists who testified at the Board’s July 2013 public workshop agreed on this point. See Privacy and Civil Liberties Oversight Board, Transcript of Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 140-41 (July 9, 2013) (statement of Ashkan Soltani, Independent Researcher and Consultant) (“The metadata is actually more sensitive at times than the content.”); *id.* at 184-85 (statement of Daniel Weitzner, MIT Computer Science and Artificial Intelligence Lab (“Metadata at scale is at least as revealing as content.”); *id.* at 189-90 (statement of Steven Bellovin, Columbia University Computer Science Department); *id.* at 137 (statement of Marc Rotenberg, Electronic Privacy Information Center),

The power of such communications metadata to illustrate a person's social connections with stark accuracy has been illustrated vividly by technology researchers.⁵⁶²

Based on our consideration of this issue, the Board is convinced that telephone calling records, when collected in bulk and subjected to powerful analytic tools, can reveal highly sensitive personal information. The government acknowledges as much, arguing that "sophisticated analytic tools" can reveal "chains of communication" and "connections between individuals."⁵⁶³ As one former general counsel of the NSA recently was quoted as saying: "Metadata absolutely tells you everything about somebody's life. . . . [It's] sort of embarrassing how predictable we are as human beings. . . . If you have enough metadata you don't really need content."⁵⁶⁴

There is a paradox here. We have concluded, based on the evidence provided by the government, that the NSA's Section 215 program has not proven useful in identifying unknown terrorists or terrorist plots, in part because the program often merely corroborates information about connections among individuals that have already been obtained independently through other means. Yet we also conclude that telephone calling records, if used in more expansive ways than the government currently employs them, can reveal a great deal about an innocent person's habits, private affairs, and network of social, familial, and professional connections. This capability is magnified when calling records are aggregated across customers and carriers and over a long period of time. The very power that inheres in the analysis of telephone calling records — a power that the government has emphasized in defending the intelligence value of the NSA's Section 215 program — illustrates the depth of the privacy implications entailed by the program without proving its effectiveness as a counterterrorism tool.⁵⁶⁵

available at <http://www.pclab.gov/>. See also Steven Bellovin, Submission to the Privacy and Civil Liberties Oversight Board: Technical Issues Raised by the Section 215 and Section 702 Programs, at 2-4 (July 31, 2013) ("Metadata is often far more revealing than content").

⁵⁶² For instance, researchers at the Massachusetts Institute of Technology have developed a program called "Immersion" that can generate a telling visual rendering of an individual's web of social connections simply through the use of email metadata — the record of who sent email messages to whom. See Immersion: A People-Centric View of Your Email Life, available at <https://immersion.media.mit.edu/>. See also Abraham Riesman, *What Your Metadata Says About You*, BOSTON GLOBE (June 29, 2013).

⁵⁶³ Administration White Paper, Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act, at 13-14 (Aug. 9, 2013).

⁵⁶⁴ Alan Rusbridger, *The Snowden Leaks and the Public*, N.Y. REVIEW OF BOOKS (Nov. 21, 2013) (quoting former NSA general counsel Stewart Baker).

⁵⁶⁵ While the apparent lack of a case in which the 215 program actually detected terrorist activity may be a paradox in light of the revealing nature of call detail records, it should not be a surprise. In 2008, the National Research Council of the Academies of Science published a report in which a committee comprised of some of the nation's leading experts on computer science, data mining, behavioral science, terrorism and law concluded, after two years of study, the same thing we find here: "Modern data collection and analysis techniques have had remarkable success in solving information-related problems in the commercial sector;

B. Privacy Implications of Bulk Collection of Telephone Calling Records

Given the ability of telephone calling records to reveal intimate details of a person's life, significant privacy interests are at stake when the government collects all of a person's calling records, particularly when it retains this information for years in a database that enables swift mapping of one's pattern of communications and network of contacts.

At the most basic level, routine government collection of telephone records defeats the core concept of information privacy — the ability of individuals to control information about themselves. This loss of control is heightened when it is *the government* collecting personal records. With its powers of compulsion and criminal prosecution, the government poses unique threats to privacy when it collects data on its own citizens.⁵⁶⁶ Allowing it to gather vast quantities of information about the conduct of individuals as a routine matter where those individuals are not suspected of any crimes affects the balance of power between the state and its people.⁵⁶⁷

Collection and analysis of information on the scale of the NSA's Section 215 program also heightens the risk of the types of mistakes that often accompany the implementation of large information systems. Indeed, privacy violations, including the inadvertent collection of unauthorized personal data, improper use of the data collected, or dissemination of that data to persons or entities not approved to receive it, may be inevitable.⁵⁶⁸ As discussed in detail in Part 4 above, since the NSA began collecting telephone and Internet metadata

for example, they have been successfully applied to detect consumer fraud. But such highly automated tools and techniques cannot be easily applied to the much more difficult problem of detecting and preempting a terrorist attack, and *success in doing so may not be possible at all.*" National Research Council, Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment, at 2 (National Academies Press, 2008) (emphasis added). See also Constitution Project, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* at 10 (2010) (examining data mining programs and finding the value of programs to identify potential terrorists "is unclear due to the particular difficulties of developing a predictive model to identify plans for terrorist acts."). These studies only focus on the power to detect terrorist activity and do not address other potential benefits from the 215 program discussed above.

⁵⁶⁶ See, e.g., Jim Harper, *Understanding Privacy — and the Real Threats to It* (Cato Policy Analysis No. 520) (Aug. 4, 2004).

⁵⁶⁷ See Neil Richards, *The Dangers of Surveillance*, 126 Harvard Law Review 1934, 1952-53 (2013) ("the gathering of information affects the power dynamic between the watcher and the watched, giving the watcher greater power to influence or direct the subject of surveillance.").

⁵⁶⁸ As Professor Steven Bellovin explained: "It is a truism in the computer security business that data that does not exist cannot be compromised. This includes both organizational misuse and misuse by individuals. Conversely, databases that do exist can be and are misused. . . . I am by no means suggesting that intelligence agencies should not collect or store information. That said, any form of collection does pose additional risks to personal privacy and security; an evaluation of the desirability of creating new databases of this type should take potential misuse into account as well. Put bluntly, it *will* happen; technical and personnel precautions will at best limit the extent." Steven Bellovin, Submission to the Privacy and Civil Liberties Oversight Board: Technical Issues Raised by the Section 215 and Section 702 Programs, at 8 (July 31, 2013) (emphasis in original).

under the supervision of the FISA court, there have been repeated instances of precisely these sorts of violations.⁵⁶⁹

Government collection of personal information on such a massive scale also courts the ever-present danger of “mission creep.” At the moment, telephone records obtained by the NSA under Section 215 may exclusively be used in furtherance of clearly defined counterterrorism efforts, and only in the manner prescribed by the FISA court’s orders. Once collected, however, information is always at risk of being appropriated for new purposes. Thus, when the government assembles a database containing the calling histories of millions of individuals, proposals to make this information available for other important governmental functions may be inevitable.⁵⁷⁰ Already, it has been reported in the press, officials from numerous federal agencies have exerted pressure on the NSA to share its data and surveillance tools for investigations into “drug trafficking, cyberattacks, money laundering, counterfeiting and even copyright infringement.”⁵⁷¹

An even more compelling danger is that personal information collected by the government will be misused to harass, blackmail, or intimidate, or to single out for scrutiny individuals or groups adhering to minority religions or holding unpopular views. To be clear, the Board has seen no evidence suggesting that anything of the sort is occurring at the NSA. But while the danger of such abuse may seem remote, it is more than merely theoretical. The government’s rampant misuse of its surveillance authority during the twentieth century to squelch domestic dissent in the name of national security was amply documented by the reports of the Church Committee, and was in fact the impetus for passage of the Foreign Intelligence Surveillance Act. In recent months, allegations have emerged at the national and local level involving the targeting of particular groups based on their ideology or religion — whether it be the Internal Revenue Service’s reported singling out of Tea Party–affiliated organizations or the New York Police Department’s alleged secret labeling of entire mosques as terrorist organizations. Prudence cautions

⁵⁶⁹ See pages 46 to 56 of this Report for a discussion of compliance issues in the NSA’s bulk telephone records program.

⁵⁷⁰ See Privacy and Civil Liberties Oversight Board, Transcript of Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 127 (July 9, 2013) (Bellovin statement) (“One of the things that’s the biggest problem in privacy is not the primary uses of data collected for a legitimate reason but the secondary uses that are often found later on for some particular database.”); *id.* at 137-38 (Rotenberg statement) (“Once you have information collected and stored in a database, you will not surprisingly find new uses for it. In fact, it would be surprising if you didn’t find new uses”). See also Ashkan Soltani, Watching the Watchers: Increased Transparency and Accountability for NSA Surveillance Programs, Submission to the PCLoB, at 9-10 (July 9, 2013).

⁵⁷¹ Eric Lichtblau & Michael S. Schmidt, *Other Agencies Clamor for Data N.S.A. Compiles*, N.Y. TIMES (Aug. 3, 2013). According to this report, the NSA generally has fended off these requests, but not without reportedly generating complaints from other agencies that its stance has “undermined their own investigations into security matters.” *Id.*

against assuming that abuse of surveillance powers is a problem that will never reoccur, and any decision to invest the government with a broad surveillance power must duly take into account the abuse that this power could enable, whether or not such abuse is evident today. Regardless of the good faith with which it may be wielded today, the immense power afforded the government by routine collection of all telephone records enables significant abuse and intrusion into Americans' privacy.

C. Chilling of Free Speech and Association

The NSA's bulk collection of telephone records also directly implicates freedom of speech and association. The readiness with which individuals engage in certain political and social activities understandably may be chilled by knowledge that the government collects a record of virtually every telephone call made by every American. Inability to expect privacy vis-à-vis the government in one's telephone communications means that people engaged in wholly lawful activities — but who for various reasons justifiably do not wish the government to know about their communications — must either forgo such activities, reduce their frequency, or take costly measures to hide them from government surveillance. Among the important freedoms that may be threatened by this chilling effect are the rights to participate in political activism, communicate with and benefit from the press, and promote novel or unpopular ideas.

“Awareness that the Government may be watching chills associational and expressive freedoms,” as Justice Sonia Sotomayor noted in a 2012 concurring opinion.⁵⁷² Her predecessors on the Supreme Court observed decades ago that national security cases “often reflect a convergence of First and Fourth Amendment values not present in cases of ‘ordinary’ crime” and that “[h]istory abundantly documents the tendency of Government — however benevolent and benign its motives — to view with suspicion those who most fervently dispute its policies.”⁵⁷³ Years earlier, the Court recognized the “vital relationship between freedom to associate and privacy in one's associations,” explaining: “Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.”⁵⁷⁴ More recently, in discussing NSA surveillance, President Obama has acknowledged that privacy in communications is part of “our First Amendment rights and expectations in this country.”⁵⁷⁵

⁵⁷² *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

⁵⁷³ *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 313 (1972).

⁵⁷⁴ *Nat'l Ass'n for Advancement of Colored People v. State of Ala. ex rel. Patterson*, 357 U.S. 449, 462 (1958).

⁵⁷⁵ Josh Gernstein, *Obama plans new limits on NSA surveillance*, POLITICO.COM (Dec. 5, 2013).

Following public disclosure of the NSA's bulk telephone records program, numerous advocacy organizations from across the political spectrum have joined legal challenges to the program, asserting that it hinders their ability to communicate confidentially with members, donors, legislators, whistleblowers, members of the public, and others.⁵⁷⁶

For instance, the NRA has asserted in a legal filing that, as an organization advancing often-controversial political stances, it "has jealously guarded information about its members and supporters" who have expressed concern about "repercussions either at work or in their community" if their NRA membership were disclosed.⁵⁷⁷ The organization likens the government's bulk telephone records program to a compelled disclosure of its membership list, because the program supplies the government with the calling records of "everyone who might communicate with the NRA or its affiliates by phone."⁵⁷⁸ In a different lawsuit, organizations ranging from environmentalists to gun-rights activists to religious and political advocacy groups have filed affidavits declaring that they have been chilled in their ability to associate with their supporters.⁵⁷⁹ For example, Greenpeace has declared that it "cannot reassure those who contact Greenpeace" or "those we actively seek out for collaboration that their communications with Greenpeace will be confidential" — frustrating the organization's advocacy mission, which depends on "free and open communication with colleagues, members, experts, and leaders of government and industry," as well as the ability to receive confidential tips about threats to the organization's protest activities.⁵⁸⁰

Knowledge that the government continuously gathers a comprehensive record of the nation's telephone calls may also deter whistleblowers from calling attention to corporate or government wrongdoing, for fear of reprisals if their identities become known.⁵⁸¹ More broadly, these considerations may constrain the work of anyone who seeks

⁵⁷⁶ See Complaint ¶¶ 3, 24-27, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. June 11, 2013); Complaint ¶¶ 2, 17-39, *First Unitarian Church of Los Angeles v. NSA*, No. 13-3287 (N.D. Cal. Oct. 30, 2013).

⁵⁷⁷ Brief of Amicus Curiae, National Rifle Association of America, Inc., in Support of Plaintiff, at 7, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Sept. 4, 2013).

⁵⁷⁸ *Id.*

⁵⁷⁹ In the lawsuit, *First Unitarian Church of Los Angeles v. NSA*, No. 13-3287 (N.D. Cal.), twenty-two organizations have filed affidavits making such assertions.

⁵⁸⁰ Declaration of Deepa Padmanabha for Greenpeace, Inc., in Support of Plaintiffs' Motion for Partial Summary Judgment, ¶¶ 11, 14-15, *First Unitarian Church of Los Angeles v. NSA*, No. 13-3287 (N.D. Cal. Oct. 30, 2013).

⁵⁸¹ In support of a legal challenges to the NSA's calling records program, the Patient Privacy Rights Foundation, which seeks to "protect citizens' rights to health information privacy," claims that "phone calls are essential for discussion of sensitive matters concerning hidden use, disclosure, and sale of the nation's personal health information." Declaration of Deborah C. Peel, MD, for Patient Privacy Rights Foundation, ¶¶ 3-6, 9, *First Unitarian Church of Los Angeles v. NSA*, No. 13-3287 (N.D. Cal. Oct. 29, 2013). The organization reports in its declaration that following public disclosure of the NSA's program it experienced a significant

to communicate with activists, dissidents, and others involved in sensitive work as part of his or her research and writing. Stunting the unimpeded exchange of ideas on which such writers thrive carries implications for freedom of information as well as freedom of expression. As argued in a legal filing by the PEN American Center, a nonprofit association of writers, “[t]he prospect that telephone metadata can reveal the entire web of a writer’s associations and interactions — and the contacts of all the writer’s contacts, and their contacts — will inevitably limit and deter valuable interactions.”

Writers in the United States who support human rights or who communicate with human rights activists, for instance, are acutely aware of the dangers that comprehensive telephone metadata may create. The government’s records of calling activity may permit reprisals or sanctions to be visited on writers, or on people with whom they speak, or on those people’s families and friends, here and in other countries where they may be more vulnerable.⁵⁸²

Awareness that complete connection data on all telephone communications is stored in a government database may have debilitating consequences for journalism as well. Sources in a position to offer crucial information about newsworthy topics may remain silent out of fear that their telephone records could be used to trace their contacts with journalists — or they may be deterred by the onerous measures required to avoid leaving such a record.

Reporters and news organizations recently have warned about the danger of “self-censorship from sources and harm to the public discourse.”⁵⁸³ Pointing out that many significant pieces of American journalism have relied heavily on confidential sources, the Reporters Committee for Freedom of the Press, joined by thirteen other news organizations, has asserted: “When the risk of prosecution reaches such sources, quality reporting is diminished. Since the public has become aware of the call tracking, many reporters at major news outlets have said that this program and other NSA surveillance efforts have made sources less willing to talk with them, even about matters not related to national security.”⁵⁸⁴

decrease in telephone calls from whistleblowers and others who would have reason to communicate anonymously. *Id.*

⁵⁸² Brief of Amici Curiae PEN American Center in Support of Plaintiffs’ Motion for a Preliminary Injunction and in Opposition to Defendants’ Motion to Dismiss, at 20, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Sept. 4, 2013).

⁵⁸³ Brief Amici Curiae of Reporters Committee for Freedom of the Press and 13 Other News Organizations in Support Plaintiffs’ Motion for Partial Summary Judgment, at 3, *First Unitarian Church of Los Angeles v. NSA*, No. 13-3287 (N.D. Cal. Nov. 18, 2013).

⁵⁸⁴ Brief Amici Curiae of Reporters Committee for Freedom of the Press and 13 Other News Organizations in Support Plaintiffs’ Motion for Partial Summary Judgment, at 1-2, *First Unitarian Church of*

These accounts describe changes in behavior on the part of journalists, sources, whistleblowers, activists, dissidents, and others upon learning that the government maintains a comprehensive and daily updated repository of call detail records on their telephone calls. The Board believes that such a shift in behavior is entirely predictable and rational. Although we cannot quantify the full extent of the chilling effect, we believe that these results — among them greater hindrances to political activism and a less robust press — are real and will be detrimental to the nation.

All of these accounts cited above refer to a chilling effect created by the *collection* of telephone calling records. The journalists, members of political organizations, and ordinary Americans discussed above assert that they are inhibited in their associations by the knowledge that the government is compiling a comprehensive record of phone calls that are then available for government review and analysis. While the government urges that the odds of any particular telephone record being reviewed by analysts is very small — noting that the NSA only queried the database for fewer than 300 “selectors” in 2012 — the government acknowledges that the number of individuals whose phone records are returned through this query process is substantially larger than 300 per year.⁵⁸⁵ Under the automated system approved by the FISC, the results of all queries may be compiled in the “corporate store” database. As explained elsewhere in this Report, the compiled records that may be aggregated in the corporate store could contain the complete calling records of 1.5 million telephone numbers — which could encompass records of telephone calls made between these numbers and over 100 million other numbers.⁵⁸⁶ Once contained in the corporate store, analysts may further examine these records without the need for any new reasonable articulable suspicion determination. With such vast numbers of telephone records readily subject to review, it would not be speculative for these individuals to fear that their own records may be culled from the NSA’s collection repository and subject to review by government analysts.

Los Angeles v. NSA, No. 13-3287 (N.D. Cal. Nov. 18, 2013). In addition, a report by the Committee to Protect Journalists spearheaded by the former Executive Editor of the *Washington Post* examined the combined impact of the Section 215 and 702 programs on journalism. It quoted one journalist as noting that “I worry now about calling somebody because the contact can be found out through a check of phone records or e-mails. . . . It leaves a digital trail that makes it easier for the government to monitor those contacts.” Leonard Downie Jr. & Sara Rafsky, Committee to Protect Journalists, *The Obama Administration and the Press: Leak Investigations and Surveillance in Post-9/11 America* (Oct. 10, 2013), <http://cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php>.

⁵⁸⁵ Declaration of Teresa H. Shea, Signals Intelligence Director, National Security Agency, ¶ 24, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Oct. 1, 2013). While fewer than 300 identifiers were used to query the NSA’s call detail records in 2012, that number “has varied over the years.” *Id.* ¶ 24.

⁵⁸⁶ See pages 29 to 31 of this Report.

D. Significance of Rules Limiting the NSA's Use of Telephone Records

In the government's view, concerns about the privacy and civil liberties implications of the NSA's bulk acquisition of calling records should be allayed by the detailed rules that limit the agency's use of those records after collection. We disagree.

To begin with, the current rules governing the NSA's Section 215 program permit analysts to view the complete calling records of individuals who have no suspected connections to terrorist activity. In defense of the program, the government emphasizes that NSA analysts may access telephone records collected under Section 215 only through a "query" that begins with a telephone number reasonably suspected of being associated with terrorism. As described earlier in this Report, when designated agency personnel develop "reasonable articulable suspicion" or "RAS" that a number is "associated" with terrorism, they are permitted to enter that number (the "seed") into the NSA's database of Section 215 records and identify all numbers (say, seventy-five) that have been in contact with the seed over the course of five years (the "first hop"). Most if not all of the individuals behind those seventy-five numbers will have no connection with terrorism. Yet the program rules allow the system to search those seventy-five numbers against the full database with no RAS determination (the "second hop") and acquire all of the numbers (say, seventy-five) that have been in touch with each of the first seventy-five numbers over the course of five years (amounting now to 5,625 numbers). Again, the vast majority of the individuals behind those 5,625 numbers would have no connection with terrorism and quite likely none would, yet the rules allow all 5,625 to be searched against the database (the "third hop") with no RAS determination, yielding possibly over 400,000 phone numbers of individuals called or receiving calls from the 5,625.

Moreover, under the new technical system that has received FISA court approval,⁵⁸⁷ the results of those queries (the full calling records of over 5,000 numbers generated by a three hop analysis of one seed) are placed into a central repository termed the "corporate store."⁵⁸⁸ The NSA has estimated that in the year 2012 approximately 300 numbers were approved as reasonably suspicious and used as seeds to query its database. If that figure holds true, then during the course of one year the corporate store could acquire the complete calling records of 1.5 million telephone persons (5,625 times 300, since the third hop produces full calling records on the 5,625 numbers yielded by the second hop) — which could encompass records of telephone calls made between these numbers and over 100 million other numbers (1.5 million persons, each calling or receiving a call from seventy-five other numbers). The rules of the FISA court for the 215 program impose no

⁵⁸⁷ See Primary Order at 11 & n.11, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-158 (FISA Ct. Oct. 11, 2013).

⁵⁸⁸ See *id.*

limits on how long data can be held in the corporate store, in contrast to the five-year retention limit on collection store data.

Furthermore, under the rules approved by the FISA court, NSA personnel may then search any phone number, including the phone number of a U.S. person, against the corporate store — as long as the agency has a valid foreign intelligence purpose in doing so — without regard to whether there is “reasonable articulable suspicion” about that number.⁵⁸⁹ Unlike with respect to the initial RAS query, the FISA court’s orders specifically exempt the NSA from maintaining an audit trail when analysts access records in the corporate store.⁵⁹⁰ The Board does not believe that this system adequately protects individual privacy, particularly as to those who are not reasonably suspected of any involvement in terrorism.

Not only do we find the existing rules inadequate in light of the depth and breadth of the data collected by the government, but we also must note again the difficulties that the NSA has had in following those rules, as described earlier in this Report. The complexity of a system like the NSA’s Section 215 program may unavoidably entail inadvertent violations of the rules that govern the handling of individuals’ calling records. From the beginning of the Section 215 program, the government assured the FISA court that software measures would prevent analysts from viewing calling records of telephone numbers that had not been approved for searching. Yet those assurances turned out to be wrong, leading the FISA court to conclude in 2009 that, from the inception of the program, “the NSA’s data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures.”⁵⁹¹ Since then, a range of inadvertent violations resulting from the complexity of the program and the NSA’s technological systems has continued up to the present day. And beyond the government’s self-reported compliance failures (the reporting of which is laudable), the FISA court has acknowledged that it has little independent means of verifying whether the NSA’s program is being implemented according to the court’s orders and in a manner that protects privacy interests.⁵⁹²

Finally, we note the risk that rules could be changed. The government could, in the future, be permitted to use the NSA’s Section 215 records for purposes other than the narrow counterterrorism efforts for which they are authorized now. It might be permitted to store the records for longer than five years, or to disseminate them more broadly among federal agencies and personnel than current standards permit. The “reasonable articulable suspicion” standard could be loosened or eliminated.

⁵⁸⁹ See Primary Order at 11 & n.11, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-158 (FISA Ct. Oct. 11, 2013).

⁵⁹⁰ See *id.* at 7 n.6. All records in the corporate store will be the results of RAS-approved queries.

⁵⁹¹ Order at 14-15, *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Mar. 2, 2009).

⁵⁹² See, e.g., *id.* at 12.

The rules could also be impacted by changes in technology. That is in evidence right now, as the NSA moves to an updated system of handling its Section 215 records that involves a new system of automated queries (described above) that places substantial information outside the database controlled by the court-imposed rules. Technology upgrades also present opportunities for mistakes and miscommunication regarding the manner in which individuals' calling records are being treated, a problem that has occurred in the past with the Section 215 data.

In sum, even under the rules that are in place today, the permissibility of three-hop querying makes a huge number of telephone records pertaining to innocent Americans subject to viewing by intelligence analysts. Moreover, under the new automated query process approved by the FISA court, all of those records may be retained indefinitely and analyzed through a variety of means without auditing. Even if the data were subject to stricter rules, the record casts doubt on whether those outside the government could reasonably be assured that those rules were being complied with. Thus, even if such stricter rules, consistently followed, were adequate to prevent invasions of privacy, they could not fully ameliorate the legitimate concerns raised by the government's possession of such a comprehensive dataset. Under the Section 215 program, individuals and groups who desire privacy in their activities and associations must contend with a novel and troubling dynamic: all of their calling records must be presumed to be in the hands of the government, under circumstances that give them no ability to know whether the government is scrutinizing their records or disseminating them to other agencies. That scenario threatens to impose a unique chilling effect on speech and association.

VI. Conclusion

The 9/11 Commission, noting that the Patriot Act "vested substantial new powers in the investigative agencies of the government" and acknowledging "concerns regarding the shifting balance of power to the government," made the following recommendation: "The burden of proof for retaining a particular governmental power should be on the executive, to explain," among other things, "that the power actually materially enhances security."⁵⁹³ Based on our study of the NSA's bulk telephone records program, which has included access to classified material and numerous briefings with intelligence officials, we do not believe the government has demonstrated that the program materially enhances security to a degree that justifies its effects on privacy, free speech, and free association.

If the program's implications for privacy and civil liberties were minor, then the showing made by the government might perhaps warrant retention of the program on the

⁵⁹³ 9/11 Commission Report at 394-95.

chance that it may offer critical counterterrorism insights in the future, even if it has not yet done so. As we have explained above, however, in our view the daily governmental collection of the telephone calling records of nearly every American has deep privacy ramifications, fundamentally alters the relationship between citizens and the state, and threatens to substantially chill the speech and associational freedoms that are essential to our democracy. Any governmental program that entails such costs requires a strong showing of efficacy. We do not believe the NSA's telephone records program conducted under Section 215 meets that standard.

VII. Recommendations for Section 215 Program

Recommendation 1. The government should end its Section 215 bulk telephone records program.

The Section 215 bulk telephone records program is not sustainable from a legal or policy perspective. As outlined in this Report, the program lacks a viable legal foundation under Section 215, implicates constitutional concerns under the First and Fourth Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value. For these reasons, the government should end the program.

As intelligence community officials have emphasized, the Section 215 program is but one tool used in the government's counterterrorism efforts. Without the program, the government would still be able to seek telephone calling records directly from communications providers for records held in their own databases, through national security letters or, in investigations of potential criminal conduct, with grand jury subpoenas, court orders or warrants.⁵⁹⁴ And the government would still be able to use pen registers and trap and trace devices under FISA and, in criminal investigations, under Title 18 for the prospective collection of new calling records as they are generated. The Board believes that the Section 215 program has contributed only minimal value in combating terrorism beyond what the government already achieves through these and other alternative means. Cessation of the program would eliminate the privacy and civil liberties concerns associated with bulk collection without unduly hampering the government's efforts, while ensuring that any governmental requests for telephone calling records are tailored to the needs of specific investigations.

⁵⁹⁴ We recognize that the use of national security letters, which are issued without judicial approval, present its own privacy and civil liberties concerns and has been the subject of extensive debate. In this study, we did not examine the government's use of NSLs. We merely recognize here that they remain a tool available to the government for the acquisition of telephone calling records on a particularized basis.

The Board does not recommend that the government impose data retention requirements on communications providers in order to facilitate any system of seeking records directly from private databases. The Board also does not recommend creating a third party to hold the data; such an approach would pose difficult questions of liability, accountability, oversight, mission creep, and data security, among others.

Once the Section 215 bulk collection program has ended, the government should purge the database of telephone records that have been collected and stored during the program's operation, subject to limits on purging data that may arise under the federal records laws or as a result of any pending litigation. This should include purging both the "collection store," which contains all records obtained under the program over the past five years, and the "corporate store," which contains the results of all automated contact chaining queries. NSA and other agencies could retain copies of data already disseminated in reports.

The Board also recommends against the enactment of legislation that would merely codify the existing program or any other program that collected bulk data on such a massive scale regarding individuals with no suspected ties to terrorism or criminal activity. While new legislation could provide clear statutory authorization for a program that currently lacks a sound statutory footing, any new bulk collection program would still pose grave threats to privacy and civil liberties. If the government and Congress seek to develop a new program to replace the Section 215 program, any such new program should be crafted far more narrowly, and the government should demonstrate that its effectiveness will clearly outweigh any intrusions on privacy and civil liberties interests.⁵⁹⁵

Moreover, the Board's constitutional analysis above should provide a message of caution to policymakers. As Fourth Amendment doctrine continues to evolve in order to address powerful new electronic surveillance technologies, the Supreme Court may be on the cusp of modifying the third-party doctrine on which the Section 215 program rests. Freedoms under the First Amendment, such as free speech, religion, and association, are clearly implicated by bulk collection of information on telephone communications. It is not necessary to find constitutional violations in order to urge — as a policy matter — that Congress should exercise restraint to respect the important individual interests involved. Given the significant privacy and civil liberties interests at stake, Congress should seek the least intrusive alternative and should not legislate to the outer bounds of its authority.

⁵⁹⁵ In theory the government could seek authorization from Congress for a new and significantly more targeted program, limited, for example, to telephone numbers that are more likely to be associated with potential terrorists, if such a program could be developed. The government might seek the private sector's assistance in developing a methodology for targeting this narrower, more relevant pool of information.

The Board recognizes that immediate shutdown of the 215 program could be disruptive, and the government may need a short period of time to explore and institutionalize alternative approaches, and believes it would be appropriate for the government to wind down the 215 program over a short interim period. If the government does find the need for a short wind-down period, the Board urges that it should follow the procedures under Recommendation 2 below.

Recommendation 2. The government should immediately implement additional privacy safeguards in operating the Section 215 bulk collection program.

The Board recommends that the government immediately implement several additional privacy safeguards to mitigate the privacy impact of the present Section 215 program. The recommended changes can be implemented without any need for congressional or FISC authorization. Specifically, the government should:

- (a) reduce the retention period for the bulk telephone records program from five years to three years;
- (b) reduce the number of “hops” used in contact chaining from three to two;
- (c) submit the NSA’s “reasonable articulable suspicion” determinations to the FISC for review after they have been approved by NSA and used to query the database; and
- (d) require a “reasonable articulable suspicion” determination before analysts may submit queries to, or otherwise analyze, the “corporate store,” which contains the results of contact chaining queries to the full “collection store.”

At present, the NSA retains all collected call detail records for five years, but this retention period can and should be limited to three years. Over time, people change their telephone numbers as well as their patterns of contacts and communications. Government officials have already said that reducing the retention period from five years to three would preserve the greatest value that the program offers.⁵⁹⁶

Similarly, changing program rules to limit contact chaining to two hops — that is, permitting each query to return only records of calls from the selector number out to the telephone numbers it calls, and from those “first hop” telephone numbers out to the numbers they have called — would not unduly diminish the value of the telephony

⁵⁹⁶ Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing, Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 118 (Nov. 4, 2013) (testimony of Rajesh De, General Counsel, NSA) (“[T]hree years probably would be where the knee of the curve is in terms of the greatest value”), available at <http://www.pclob.gov/>.

metadata program. No third hops (the telephone numbers called by the second hop numbers) should be permitted based on a single RAS determination. If the government wishes to search for connections from identifiers it obtained at the second hop, it should be required to obtain a new RAS approval for each such telephone number. Each additional hop from the original “selector” makes the connection more remote and adds exponentially greater numbers of “false positives” to the query results. The value of connections becomes more limited as the contact chain is extended and it becomes more difficult to sift through the results.

The third immediate change that the Board recommends is that the NSA should submit its RAS determinations to the FISC for review after queries have been run. NSA officials would still make the RAS determinations under existing minimization rules and this would provide sufficient authorization to run a query. The NSA would submit these RAS determinations to the FISC periodically over the coming months or as part of the next renewal application for the program. Submission of RAS determinations would allow the FISC to assess whether the RAS standard has properly been met as part of the evaluation of whether to renew the program and potentially modify its terms and protections.

The Board notes that review of RAS determinations will increase the workload of the FISC, and urges Congress to take into account the growing responsibilities of the FISC overall as it considers the judiciary’s budget, but the Board does not believe that the burden will be excessive. The government has stated that in 2012 there were fewer than 300 RAS-approved selectors over the course of the entire year, so the number of RAS determinations submitted to the FISC for any quarterly renewal application should be manageable. Further, this after the fact procedure would not present the time pressure of individualized FISC review prior to querying the database.

The fourth immediate change is to extend privacy safeguards to the database that contains all of the metadata generated by queries run on RAS-approved selectors. As described above, NSA uses RAS-approved selectors to run queries on the full database of calling records termed the “collection store.” Under the automated query process approved by the FISC, the results of all queries, containing millions of call detail records retrieved through contact chaining, are compiled in a database called the “corporate store.” The vast majority of the call detail records transferred will concern U.S. persons as to whom there is no suspicion of any connection to terrorism. In essence, the corporate store will contain an ever-growing subset of telephone calling records. Under the current minimization procedures approved by the FISC, analysts may query the corporate store database with any selector, without prior RAS approval — so long as they have a valid foreign intelligence purpose — and seemingly may engage in data mining or other forms of analysis besides querying. The Board recommends that this rule be changed. Telephony metadata on

presumptively innocent Americans, whether in the large database or a subset, should be subject to query only based on the same reasonable articulable suspicion standard.

Part 8:
DISCUSSION AND RECOMMENDATIONS REGARDING THE
FOREIGN INTELLIGENCE SURVEILLANCE COURT

I. Overview of the Foreign Intelligence Surveillance Court

The Foreign Intelligence Surveillance Court (“FISC” or “FISA court”) is a critical component of the system of checks and balances that our nation has created around the exercise of national security powers. When Congress created the court in 1978 in response to concerns about the abuse of electronic surveillance,⁵⁹⁷ it represented a major restructuring of the domestic conduct of foreign intelligence surveillance, with constitutional implications. Until then, successive Presidents of both parties had authorized national security wiretaps and other searches solely on the basis of their powers under Article II of the Constitution. The Foreign Intelligence Surveillance Act (“FISA”) of 1978 provided a procedure under which the Attorney General could obtain a judicial warrant authorizing the use of electronic surveillance in the United States for foreign intelligence purposes.⁵⁹⁸ As the House Permanent Select Committee on Intelligence explained in its 1978 report recommending adoption of FISA:

The history and law relating to electronic surveillance for "national security" purposes have revolved around the competing demands of the President’s constitutional powers to gather intelligence deemed necessary to the security of the nation and the requirements of the fourth amendment. The U.S. Supreme Court has never expressly decided the issue of whether the President has the constitutional authority to authorize warrantless electronic surveillance for foreign intelligence purposes. Whether or not the President has an “inherent power” to engage in or authorize warrantless electronic surveillance and, if such power exists, what limitations, if any, restrict the scope of that power, are issues that have troubled constitutional scholars for decades.⁵⁹⁹

⁵⁹⁷ See S. Rep. No. 95-604(I), at 7 (1978) (“Senate Judiciary Committee Report”) (“The legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused.”); H.R. Rep. No. 95-1283(I), at 111 (1978) (“HPSCI Report”) (dissenting views of Reps. Wilson, McClory, Robinson and Ashbrook) (“No one can deny that abuses of electronic surveillance have taken place in the past under the claim of ‘national security.’”).

⁵⁹⁸ Senate Judiciary Committee Report at 5. When enacted, FISA did not cover activities occurring outside the United States. By and large, that remains true today, the only exception being acquisitions of foreign intelligence that intentionally target a U.S. person reasonably believed to be outside the United States, which were brought within the jurisdiction of the FISC under the FISA Amendments Act of 2008. See 50 U.S.C. § 1881c.

⁵⁹⁹ HPSCI Report at 15.

In essence, FISA represented an agreement between the executive and legislative branches to leave that debate aside⁶⁰⁰ and establish a special court to oversee foreign intelligence collection. While the statute has required periodic updates, national security officials have agreed that it created an appropriate balance among the interests at stake, and that judicial review provides an important mechanism regulating the use of very powerful and effective techniques vital to the protection of the country.⁶⁰¹

Currently, the FISA court is comprised of eleven judges. The Chief Justice of the United States appoints these judges from among sitting U.S. district court judges, who previously have been appointed by the President and confirmed by the Senate. The Chief Justice also appoints one of the FISC judges to serve as presiding judge. These judges serve on the FISC for staggered seven-year terms while continuing to maintain a full docket of cases in their home districts. FISA requires that the judges be drawn from at least seven different U.S. judicial circuits. At least three of the eleven must reside within twenty miles of Washington, D.C.,⁶⁰² to ensure that there will be a judge available to hear emergency matters.

Over time, the scope of FISA and the jurisdiction of the FISA court have evolved. When FISA was first enacted, the jurisdiction of the court was limited to reviewing applications for “electronic surveillance.” That term has its own unique and complex definition under the statute but largely it concerns the acquisition of the contents of electronic communications.⁶⁰³ In 1994, Congress amended FISA to permit applications for and orders authorizing physical searches.⁶⁰⁴ In 1998, Congress further amended the statute

⁶⁰⁰ “[T]he bill does not recognize, ratify, or deny the existence of any Presidential power to authorize warrantless surveillance in the United States in the absence of the legislation. It would, rather, moot the debate over the existence or non-existence of this power[.]” HPSCI Report at 24. This agreement between Congress and the executive branch to involve the judiciary in the regulation of intelligence collection activities did not and could not resolve constitutional questions regarding the relationship between legislative and presidential powers in the area of national security. *See In re: Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002) (“We take for granted that the President does have that authority [inherent authority to conduct warrantless searches to obtain foreign intelligence information] and, assuming that is so, FISA could not encroach on the President’s constitutional power.”).

⁶⁰¹ *See, e.g., FISA Hearing: Hearing before the Permanent Select Committee on Intelligence*, 110th Cong. (2007) (statement of Michael McConnell, Director of National Intelligence) (“It is my steadfast belief that the balance struck by the Congress in 1978 was not only elegant, it was the right balance to allow my Community to conduct foreign intelligence while protecting Americans.”); Joint Statement for the Record of James R. Clapper, Director of National Intelligence, and General Keith B. Alexander, Director, National Security Agency, before the Senate Committee on the Judiciary, at 9 (Oct. 2, 2013) (“On the issue of FISC reform, we believe that the *ex parte* nature of proceedings before the FISC is fundamentally sound and has worked well for decades in adjudicating the Government’s applications for authority to conduct electronic surveillance or physical searches in the national security context under FISA.”).

⁶⁰² 50 U.S.C. § 1803(a). The Patriot Act expanded the number of judges on the FISC from seven to eleven and added the requirement that three of the judges must reside within twenty miles of Washington, D.C.

⁶⁰³ 50 U.S.C. § 1801(f).

⁶⁰⁴ Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443 (1994) (codified at 50 U.S.C. §§ 1821 to 1829).

to add authority for the FISC to review and approve applications for the installation and use of pen registers and trap and trace devices to collect foreign intelligence.⁶⁰⁵ Also in 1998, Congress amended the statute to create a “business records” provision, which authorized the FISA court, at the government’s request, to order a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession pertaining to a foreign power or agent of a foreign power.⁶⁰⁶ That authority was substantially amended by Section 215 of the Patriot Act.⁶⁰⁷

However, despite these changes, the main business of the Court prior to 2004 remained the consideration of government applications relating to a specific person, a specific place, or a specific communications account or device. Numerically, consideration of such particularized applications still constitutes the vast majority of the court’s workload. In considering these applications, judges sitting on the FISC perform a role very similar to that performed by judges and magistrates in ordinary criminal cases. Proceedings are conducted *ex parte*; that is, with only government attorneys appearing before the court, which is the same way that applications for a search warrant or a wiretap are considered in criminal proceedings. Such individualized applications tend to be very fact-specific; often the only question is whether the application meets the express standard set forth in FISA. As a former judge of the FISA court recently explained, “approving search warrants and wiretap orders and trap and trace orders and foreign intelligence surveillance warrants one at a time is familiar ground for judges.”⁶⁰⁸

There is one major difference between these individualized FISC and criminal proceedings. FISA applications and the proceedings associated with them are not only *ex parte*, they are also secret, to a degree that makes it very difficult for a target of surveillance to ever challenge the legality of the government’s actions.⁶⁰⁹ As Judge James G. Carr, a senior district court judge and former member of the FISA court, has pointed out “[T]he subject of a conventional Fourth Amendment search warrant knows of its execution, can challenge its lawfulness if indicted, and can, even if not indicted, seek to recover seized property or possibly sue for damages. In contrast, except in very, very rare instances,

⁶⁰⁵ Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2404 (1998) (codified at 50 U.S.C. §§ 1841 to 1846).

⁶⁰⁶ Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2410 (1998) (codified at 50 U.S.C. §§ 1861 to 1863).

⁶⁰⁷ Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified at 50 U.S.C. § 1861). See pages 40 to 41 of this Report for a discussion of this expanded authority.

⁶⁰⁸ Privacy and Civil Liberties Oversight Board, Transcript of Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 35 (July 9, 2013) (statement of Judge James Robertson), *available at* <http://www.pclob.gov/>.

⁶⁰⁹ FISA directs that the “record of proceedings under this Act, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.” 50 U.S.C. § 1803(c).

suppression or other means of challenging the lawfulness of a FISA order is simply not available to the subject of a FISA order.”⁶¹⁰ Although criminal defendants must be notified if the government intends to enter into evidence or otherwise use against them evidence derived from FISA surveillance, special procedures under the statute limit what can be disclosed to defendants, and proceedings on a motion to suppress must be held *ex parte* if the Attorney General files an affidavit that disclosure or an adversary hearing would harm the national security of the United States.⁶¹¹ In practice, the government always files such an affidavit, and it appears that no defendant has ever obtained a copy of the government’s statement of probable cause or other documents that served as the basis for FISA surveillance.⁶¹²

II. The FISC’s Role after 9/11

Beginning in 2004, the role of the FISA court changed as a result of two significant developments. First, in 2004, the government approached the court with a request to approve a program involving what is now referred to as “bulk collection.” Specifically, the government requested that the court approve, under the FISA provisions for pen registers and trap and trace devices, the bulk collection of “to and from” data concerning the Internet communications of many unspecified persons. Both the government and the court recognized that the application raised novel legal issues not presented in the individualized applications that had characterized the court’s work until then. The government submitted a lengthy memorandum of law supporting its request, and the court, when it approved the request, issued a lengthy opinion addressing the legal issues presented. That request for collection of Internet metadata was followed by one in 2006 concerning telephony metadata, filed under a different provision of FISA and thus presenting further unique questions.

⁶¹⁰ Prepared Remarks of James G. Carr, Senior U.S. District Judge, N.D. Ohio, *Senate Judiciary Committee Hearing: Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs* (July 31, 2013), available at <http://www.judiciary.senate.gov/pdf/7-31-13CarrTestimony.pdf>.

⁶¹¹ 50 U.S.C. § 1806(f).

⁶¹² Jimmy Gurulé, *FISA and the Battle Between National Security and Privacy*, JURIST (Feb. 17, 2012) (noting that no court has ever disclosed FISA documents to a defendant and concluding that defendants face “insurmountable legal hurdles” to suppress evidence derived from electronic surveillance or physical searches authorized under FISA). It is our understanding that these practices will not be affected by the DOJ’s recent decision to notify defendants when surveillance under FISA leads to other evidence that the government intends to introduce against them. See Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES (Oct. 16, 2013) (reporting that the DOJ had been taking a narrow view of “derived from” and had not been notifying defendants if they had been targeted under FISA but the information obtained was not itself introduced but had led to other evidence that was introduced).

A second major development occurred when Congress enacted the FISA Amendments Act of 2008 (“FAA”), which authorized the Attorney General and the Director of National Intelligence (“DNI”) to target the electronic communications of persons reasonably believed to be located outside the United States, for the purpose of acquiring foreign intelligence information. The FAA authorized the Attorney General and the DNI to issue directives requiring electronic communications service providers to assist the government in collecting these communications. In contrast to other acquisitions of content authorized under FISA, the FAA did not require the government to seek the FISA court’s approval of its decisions about which individuals to target; instead, the Act authorized the court to review annual “certifications” by the government and to review the targeting and minimization procedures adopted by the government for this program. The required certifications must include an affidavit by an appropriate official attesting that there are targeting and minimization procedures in place that meet statutory requirements and stating that a significant purpose of the acquisition is to obtain foreign intelligence information.⁶¹³ The FAA required the government to assess its compliance with the targeting and minimization procedures and to report its assessment to the court on a semi-annual basis and to report other implementation details to the court on an annual basis. From time to time, in response to compliance lapses brought to the FISA court’s attention by the government⁶¹⁴ the FISC has conducted detailed inquiries into specific technical and constitutional issues arising in the implementation of the government’s authority.

III. Process for FISC Review of Government Applications

Whether the FISA court is considering a particularized request or a programmatic one such as the bulk metadata collection program under Section 215, even before an application reaches the court, it undergoes extensive review in the executive branch. It is first reviewed by lawyers at the FBI, the NSA, or other agencies, and then by lawyers at the National Security Division of the Department of Justice (“NSD”), who present the government’s applications to the court. Review by the NSD frequently involves substantial back and forth between the agency seeking authorization and the DOJ lawyers, as the lawyers seek additional factual details about the target of the surveillance, technical information about the surveillance methodology, or assurances about how the information acquired will be used and disseminated. Agency personnel would say that at times these interactions are quasi-adversarial. At the conclusion of the process, the application will generally be quite lengthy and may have extensive supporting documentation, and it must

⁶¹³ 50 U.S.C. § 1881a(g).

⁶¹⁴ See pages 46 to 56 of this Report for a discussion of these compliance incidents.

be approved by the Attorney General, the Deputy Attorney General, or upon designation, the Assistant Attorney General for National Security.⁶¹⁵

At the FISC, each week one of the eleven judges who comprise the court is on duty in Washington.⁶¹⁶ Normally, a proposed application must be submitted to the duty judge by the DOJ at least seven days before the government seeks to have the matter entertained. Upon the court's receipt of a proposed application, a member of the FISA court's legal staff will review the application and evaluate whether it meets the legal requirements under FISA. The FISC's legal staff are career employees who have developed substantial expertise in FISA. They are much more senior and experienced than typical judicial law clerks in federal courts, who are often recent law school graduates. However, the legal staff's job responsibilities and role are analogous to those of most judicial law clerks in that they serve as staff to the judges rather than as advocates.⁶¹⁷ They conduct research to probe whether the government's application should be granted. While their role includes identifying any flaws in the government's statutory or constitutional analysis, it does not reach to contesting the government's arguments in the manner of an opposing party. As part of their evaluation of a proposed application, the court attorneys will often have one or more telephone conversations with the DOJ lawyers to seek additional information and/or raise concerns about the application.⁶¹⁸ The legal staff will prepare a written analysis of the application for the duty judge, which includes an identification of any weaknesses, flaws or other concerns. For example, the court attorney may recommend that the judge consider requiring the addition of information to the application; imposing special reporting requirements; or shortening the requested duration of an application.

The duty judge will then review the proposed application along with the legal staff's analysis and will make a preliminary determination about how to proceed. The judge's

⁶¹⁵ 50 U.S.C. § 1801(g) (defining Attorney General to include delegation to other specified officials); *id.* § 1804(g) (Attorney General approval required).

⁶¹⁶ The description of the FISC's procedures in this section is based on its published Rules of Procedure and on two detailed letters from FISC presiding judge Reggie B. Walton to the chairman of the Senate Judiciary Committee. *See* United States Foreign Intelligence Surveillance Court, Rules of Procedure (Nov. 1, 2010); Letter from the Honorable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to the Honorable Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate (July 29, 2013) ("Walton Letter of July 29, 2013"); Letter from the Honorable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to the Honorable Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate (Oct. 11, 2013) ("Walton Letter of Oct. 11, 2013").

⁶¹⁷ *See*, David Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RESEARCH PAPER SERIES, at 38-39 (Sept. 29, 2013), available at <http://www.lawfareblog.com/>. Kris notes that Congress could expand the number of FISC legal advisers and "allow and encourage" FISC judges to designate one or more to draft briefs opposing the DOJ attorneys' legal arguments.

⁶¹⁸ The legal staff interact with the government by telephone on a daily basis; they meet in person with the government as often as two to three times a week, or as few as one to two times a month, in connection with the various matters pending before the court. *See* Walton Letter of July 29, 2013, at 6.

responses might include indicating to the court staff that he or she is prepared to approve the application without a hearing; indicating an inclination to impose conditions on the approval of the application; determining that additional information is needed about the application; determining that a hearing would be appropriate before deciding whether to grant the application; or indicating an inclination to deny the application. The staff attorney will then relay the judge's inclination to the government, and the government will then submit a final application, which may include additional information in response to the court's feedback. The government may seek a hearing, for example, to challenge the judge's proposed conditions. In some cases, the government may decide not to submit a final application or to withdraw one that has been submitted, after learning that the judge does not intend to approve it. Unless the government withdraws the application, the FISC judge, either with or without a hearing, will decide whether to approve or deny it or to approve it with conditions.

When a FISA court judge holds a hearing, it will be attended, at a minimum, by the Department of Justice attorney who prepared the application and a fact witness from the agency seeking the Court's authorization. FISC judges have the authority to take testimony, for example, from government employees familiar with the technical issues associated with a particular technique or program or from personnel responsible for the operation of a program. Although it is an open question, in theory, at least, the court could also hear from outside experts on technical questions.⁶¹⁹

It is frequently reported that the FISA court approves a very large percentage of government applications. In fact, however, the approval rate for wiretap applications in ordinary criminal cases is higher than the approval rate for FISA applications.⁶²⁰ Moreover, the FISA statistics do not take into account the changes to the final applications that are ultimately submitted, made as a result of the back and forth between the FISC legal staff and government attorneys. Nor does the percentage of approvals take into account the applications that are withdrawn or never submitted in final form due to concerns raised by the court or its legal staff. The FISA court has recently kept track of such actions and has found that, during the three month period from July through September 2013, 24.4% of matters submitted to the FISA court ultimately involved substantive changes to the

⁶¹⁹ Judge James Carr, former FISC judge, and James Baker, who previously practiced before the FISC, both testified at the PCLOB's hearing on November 4, 2013, about the role of in-house legal counsel and the court's ability to consult outside technologists. *See* Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing, Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 175-77, 204-08 (Nov. 4, 2013), available at <http://www.pclob.gov/>.

⁶²⁰ Walton Letter of July 29, 2013, at 3 n.6.

information provided by the government or to the authorities granted as a result of court inquiry or action.⁶²¹

Applications that are novel or more complex, such as applications under Section 702 and applications for renewal of bulk phone call metadata collection under Section 215, are handled using a process that is similar to the one described above, but more exacting. The government typically submits a proposed application of this type more than one week in advance; in the case of Section 702, proposed applications are typically filed approximately one month before filing a final application. Programmatic applications are accompanied by even more detailed information than an individualized application, and the court attorney who reviews that application spends more time reviewing it, as does the judge. In addition, under the court's rules, if an application involves an issue not previously presented to the court, including novel issues of technology or law, the government must advise the FISC in writing of the nature and significance of the issue and submit a memorandum explaining the novel technique, novel implementation of an existing technique, or legal issue not previously considered by the court.⁶²²

FISA does not provide a mechanism for the FISC to invite non-governmental parties to provide views on pending government applications or otherwise participate in FISA court proceedings prior to approval of an application. After an order has been issued, the statute and the FISC rules provide opportunities for recipients of such orders (or of government directives issued under Section 702) to challenge those orders or directives.⁶²³ Such challenges are very rare. There has been one instance in which the court heard arguments from a non-governmental party that sought to substantively contest a directive from the government.⁶²⁴ In another case that did not address the legality of a particular order but concerned service providers' ability to disclose information about the number of orders they had received, the court heard from outside lawyers, but even though those outside attorneys had security clearances, they were not granted full access to the

⁶²¹ See Walton Letter of Oct. 11, 2013, at 1-2.

⁶²² FISC Rule of Procedure 11.

⁶²³ In the case of particularized orders issued under Title I of FISA, a recipient of an order can refuse to comply, in which case the government may seek to compel, setting up the opportunity for the recipient to challenge the order. The FAA provides that an electronic communication service provider receiving a directive issued under Section 702 may file a petition to modify or set aside such directive with the FISC, which shall have jurisdiction to review such petition. See 50 U.S.C. § 1881a(h)(4). Likewise, a person receiving a production order under Section 215 may challenge the legality of that order or of the nondisclosure provision that accompanies Section 215 orders by filing a petition with FISC. See 50 U.S.C. § 1861(f).

⁶²⁴ Specifically, in 2007, the government issued directives to Yahoo!, Inc., pursuant to the Protect America Act of 2007. Yahoo! refused to comply, and the government filed a motion with the FISC to compel compliance. The court ordered and received briefing from both parties. See *In Re Directives*, 551 F.3d 1004 (FISA Ct. Rev. 2008).

information that DOJ attorneys submitted to the FISC.⁶²⁵ Outside parties have participated as an amicus or friend of the court in several matters before the FISA court, but to date, those have involved proceedings seeking the release of various records and not an assessment of the government's legal authorization to conduct surveillance.⁶²⁶

FISA also established a Foreign Intelligence Court of Review ("FISCR"), comprised of three judges drawn from U.S. district courts or courts of appeals. These judges are also appointed by the Chief Justice of the United States and also serve staggered seven-year terms. The appellate jurisdiction of the FISCR was originally limited to reviewing the denial of applications.⁶²⁷ Since 2006, when recipients of FISC orders under Section 215 were permitted to challenge those orders, the statute was amended to allow appeal to the FISCR whenever the FISA court denies a challenge to a Section 215 order.⁶²⁸ Likewise, the FISA Amendments Act of 2008 granted electronic communication service providers the right to appeal FISC decisions denying challenges to directives issued under the FAA.⁶²⁹ Appeals to the FISCR have been rare.⁶³⁰ FISA does not provide a way for the FISCR to receive the views of other non-governmental parties on appeals pending before it. However, the court has in one case accepted amicus curiae or friend of the court briefs on a significant legal question pending before it.⁶³¹ FISA also provides that the Supreme Court of the United

⁶²⁵ At the PCLOB's November 4, 2013, hearing, Marc Zwillinger, of ZwillGen PLLC, testified regarding his experience representing Internet service providers before the FISC, including a challenge by five Internet service providers seeking the right to disclose information about the number of FISA orders they receive. He noted that the outside counsel in the case with security clearances were denied access to certain government filings. See Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing, Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 156-59 (Nov. 4, 2013), available at <http://www.pclob.gov/>. The litigation in this matter is ongoing.

⁶²⁶ See Walton Letter of July 29, 2013. Recently, the Center for National Security Studies sought permission to file an amicus brief urging that Section 215 does not permit bulk collection of telephone records in connection with the renewal of the Section 215 program. The FISC granted permission for CNSS to file such an amicus brief, but only in a miscellaneous docket where it can be accessed by any FISC judge. See Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things* No. BR 13-158 (FISA Ct. Dec. 18, 2013).

⁶²⁷ 50 U.S.C. § 1803(b).

⁶²⁸ See 50 U.S.C. § 1861(f)(2). This provision was added as part of the modifications to Section 215 by the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 191 (2006).

⁶²⁹ Electronic communications service providers may also appeal an adverse decision when the DOJ has moved to compel their compliance with such a directive. See 50 U.S.C. § 1881a(h)(6).

⁶³⁰ Only two opinions from the FISCR have been released. These are *In Re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002) (an appeal by the government), and *In Re Directives*, 551 F.3d 1004 (FISA Ct. Rev. 2008) (an appeal by Yahoo! in the case described above). Based upon the best information available to the Board, these are the only two cases decided by the FISCR to date.

⁶³¹ See *In Re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002).

States has jurisdiction to review FISC decisions,⁶³² but to date, no FISC decision has come before the Supreme Court for review.⁶³³

IV. Proposals for Reform of the FISC Process

In recent months, numerous proposals have been offered to modify the process by which the FISA court considers government applications, especially in cases involving novel legal or technical issues. These proposals have arisen in part from a concern that the FISC's *ex parte*, classified proceedings do not take adequate account of positions other than those of the government. In considering these proposals, the Board gives great weight to two points: that the FISC, its judges, their staff, and the government lawyers who appear before the court operate with integrity and give fastidious attention and review to surveillance applications; but also that it is critical to the integrity of the process that the public have confidence in its impartiality and rigor.⁶³⁴

Proposals to change the FISA court process must take into account the imperative of secrecy in the application of some of the nation's most sensitive intelligence collection techniques; the importance of speed in responding to often fast-breaking events posing severe risk to the national security; the resource limits faced by the court and its judges (who carry an ordinary civil and criminal caseload in their "home" districts); and constitutional issues.

With those considerations in mind, we believe that some reforms are appropriate and would help bolster public confidence in the operation of the court. The most important reforms concern three sets of issues: (1) providing a greater range of views and legal arguments to the FISC as it considers novel and significant issues; (2) facilitating appellate review of such decisions; and (3) providing increased opportunity for the FISC to receive technical assistance and legal input from outside parties. In addition, in the next section of this Report, we discuss and make recommendations regarding the need for greater public transparency for the legal opinions adopted by the court.

⁶³² 50 U.S.C. § 1803(b), § 1861a(f), § 1881a(h)(6), § 1881a(i)(4).

⁶³³ The Supreme Court has not heard any appeals of FISC orders, nor has it ever considered the merits of a FISA order or ruled on the constitutionality of the statute. In *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), the Court held that the petitioners lacked standing to bring a constitutional challenge to the FAA, and on November 18, 2013, the Court denied a mandamus petition filed by the Electronic Privacy Information Center that had sought to challenge the FISC's order approving the Section 215 telephony metadata program. See *In Re Electronic Privacy Information Center*, No. 13-58 (U.S. Nov. 18, 2013).

⁶³⁴ The PCLOB heard from three judges who formerly served on the FISC. Judge James Robertson, who served on the FISC from 2002 through 2005, participated in the Board's July 9, 2013, public workshop; Judge James Carr, who served on the FISC from 2002 through 2008, participated in our November 4, 2013, public hearing; Judge John Bates, who served on the Court from 2006 to February, 2013 and as its presiding judge from 2009 to 2013, met with the Board on October 16, 2013.

V. Recommendations Regarding FISC Operations

Recommendation 3. Congress should enact legislation enabling the FISC to hear independent views, in addition to the government's views, on novel and significant applications and in other matters in which a FISC judge determines that consideration of the issues would merit such additional views.

Although the FISC continues to review applications for individualized FISA warrants, in the past decade it has also been called upon to evaluate requests for broader collection programs, such as the 215 telephony metadata program, and to review extensive compliance reports regarding the implementation of the surveillance authorized under Section 702. This expansion of the FISC's jurisdiction has presented it with complex and novel issues of law and technology. Currently, these issues are adjudicated by the court based only on filings by the government, supplemented by the research and analysis of the judges and their experienced legal staff.

Our judicial system thrives on the adversarial presentation of views. As Judge Robertson noted:

[A]nybody who has been a judge will tell you that a judge needs to hear both sides of a case before deciding. It's quite common, in fact it's the norm to read one side's brief or hear one side's argument and think, hmm, that sounds right, until we read the other side.⁶³⁵

Nonetheless, the *ex parte* process works well when the FISC is considering individualized applications presenting no novel legal or technical questions. The inquiry there is fact-based, and the legal standard is familiar and explicit in the statute. Consideration of individualized surveillance applications is a function that judges in other courts all over the country routinely perform on an *ex parte* basis, and it is no less appropriate in the national security context.

However, there is a growing consensus that the *ex parte* approach is not the right model for review of novel legal questions or applications involving broad surveillance programs that collect information about the communications of many people who have no

⁶³⁵ Privacy and Civil Liberties Oversight Board, Transcript of Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 34 (July 9, 2013) (statement of Judge James Robertson); *see also* Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing, Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 151 (Nov. 4, 2013) (testimony of Judge James Carr) (“[I]t’s how we [judges] work, through the adversary process.”), available at <http://www.pclomb.gov/>.

apparent connection to terrorism.⁶³⁶ The Board believes that, when FISC judges are considering requests for programmatic surveillance affecting numerous individuals or applications presenting novel issues, they should have the opportunity to call for third-party briefing on the legal issues involved. In addition to assisting the court, a mechanism allowing FISC judges to call upon independent expert advocates for a broader range of legal views could bolster the public's trust in its operations and in the integrity of the FISA system overall.

Accordingly, the Board recommends that Congress amend FISA to authorize the FISC to create a pool of "Special Advocates" who would be called upon to present independent views to the court in important cases. Even in the absence of such legislative authority, the Board believes the court has discretion to call upon outside lawyers, if they have the necessary national security clearances, to offer analysis of legal or technical issues, and the Board would urge the court to amend its rules to allow for such advocacy. However, it would be preferable to have a statutory basis for such a system.

The Board has examined the myriad bills introduced in Congress and proposals offered by advocates, scholars and others. The Board does not attempt to draft legislative language or to express views on which program details should be expressed in statute and which may be left to court rules of procedure. However, the Board has identified key elements of an advocacy process that should offer the court the benefit of outside expert participation without unduly disturbing the structure or functioning of the vast majority of the court's proceedings.

To serve this purpose, Congress should authorize the establishment of a panel of outside lawyers to serve as Special Advocates before the FISC in appropriate cases. These lawyers would not become permanent government employees, but would be available to be called upon to participate in particular FISC proceedings. The presiding judge of the FISC should select the attorneys to serve on the panel. The attorneys should be drawn from the private sector, and the Board expects that they would possess expertise in national security, privacy and civil liberties issues and be capable of obtaining appropriate security clearances. The attorneys would need office space with appropriate secure facilities, ideally within the FISA court. Congress should ensure that the FISC has adequate appropriations to

⁶³⁶ See Transcript of July 9, 2013 Public Workshop, *supra*, at 34-37 (statement of Judge James Robertson); Transcript of November 4, 2013 Hearing, *supra*, at 148-52 (testimony of Judge James Carr). Judge Carr also presented his views in a *New York Times* op-ed, see James G. Carr, *A Better Secret Court*, N.Y. TIMES (July 22, 2013), and in testimony before the Senate Judiciary Committee. See Prepared Remarks of James G. Carr, Senior U.S. District Judge, N.D. Ohio, *Senate Judiciary Committee Hearing: Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs* (July 31, 2013), available at <http://www.judiciary.senate.gov/pdf/7-31-13CarrTestimony.pdf>.

implement and operate the Special Advocate program. The Board is confident that such a system would not raise any serious constitutional issues.⁶³⁷

In the Board's view, the FISC should have discretion to choose the applications or other matters on which it would seek the Special Advocate's views. In such cases, the FISC judge assigned to the matter would call upon one of the lawyers on the Special Advocate panel to participate in it. The FISC can establish specific rules for inviting a Special Advocate's participation, including whether the lawyers on the panel would be invited on a rotating basis. The Board expects that the court would invite the Special Advocate to participate in matters involving interpretation of the scope of surveillance authorities, other matters presenting novel legal or technical questions, or matters involving broad programs of collection, but would not mandate the participation of the Special Advocate in any particular case. In addition, the Board would leave flexibility for a FISC judge to identify other matters that merit Special Advocate participation. The Board does not believe it is necessary or appropriate for Special Advocates to participate in all applications for individualized FISA orders, but the court should have the option of seeking input when such applications present novel legal or technical questions.

The role of the Special Advocate, when invited by the court to participate, would be to make legal arguments addressing privacy, civil rights, and civil liberties interests. The Board does not propose requiring the Special Advocate to serve as the government's adversary, as opposing lawyers would do in traditional litigation. The Special Advocate should not be expected to oppose every argument made by the government. Rather, the Special Advocate would review the government's application and exercise his or her judgment about whether the proposed surveillance or collection is consistent with law or unduly affects privacy and civil liberties interests. The Special Advocate would rely on both statutory and constitutional arguments as appropriate. The Special Advocate would have discretion to make legal arguments opposing the application in its entirety, advocating modifications to the application that would address privacy and civil liberties-related legal concerns, or to conclude that the application was lawful and did not unduly burden privacy or civil liberties.

As noted above, current FISC Rule of Procedure 11 requires that if an application involves any novel issues, including novel issues of technology or law, the government must advise the FISC in writing of the nature and significance of the issue and submit a memorandum explaining the novel technique or legal interpretation. This existing

⁶³⁷ For example, the Appointments Clause would not be implicated because the role we suggest would not provide the Special Advocate with the requisite legal authority to qualify as an officer under this clause. See Andrew Nolan, Richard M. Thompson II, & Vivian S. Chu, *Introducing a Public Advocate into the Foreign Intelligence Surveillance Act's Courts: Select Legal Issues*, CONGRESSIONAL RESEARCH SERVICE, at 8-13 (Oct. 25, 2013) (outlining circumstances under which a public advocate role might cause an Appointments Clause problem).

requirement provides a useful mechanism to trigger consideration of whether Special Advocate participation would be beneficial. If the presiding judge determined that Special Advocate participation would be helpful based on the government's Rule 11 submission, the judge could immediately invite Special Advocate participation. Otherwise, FISC rules could require that, upon receiving such a notification, the presiding judge should seek a Special Advocate's preliminary views on whether the matter poses privacy or civil rights issues and whether the judge's resolution of these issues would benefit from Special Advocate participation. Upon reviewing the Special Advocate's submission, the judge would determine whether to invite his or her full participation.

However, the circumstances prescribed in FISC Rule 11 are not the only circumstances where participation by the Special Advocate might be appropriate. FISC judges should also consider inviting Special Advocate participation for applications to *renew* already approved programs or implementations of techniques. This may be appropriate in matters that raised issues that were novel or significant at the time the *original* application was filed but were not fully considered at that time; matters in which intervening circumstances have raised issues that did not exist at the time of the original application; or in other matters where the judge concludes that it would be helpful to have a more thorough briefing with a diversity of views presented.

Once a Special Advocate has been invited to participate with respect to an application or other matter, the Special Advocate should be permitted to participate in all proceedings related to that application or matter and should have access to all government filings.

The procedures for participation by a Special Advocate should recognize that Special Advocate participation might not be possible in emergency circumstances before electronic surveillance begins. Tracking the existing rules for emergency employment of electronic surveillance under FISA, the procedures should permit the Special Advocate to participate when the court subsequently reviews the application after commencement of the emergency surveillance.

The Board does not intend this proposal to confer on the Special Advocate any absolute right to participate in any matter. Instead, the Board intends that Special Advocate participation would be at the discretion of the court. Based on statements by former FISC judges, the Board believes that the FISC judges themselves will find value in hearing the views of independent advocates in difficult cases. Their experience with and dedication to the more expansive proceedings in their regular district court roles will insure that the Special Advocate will be invited to participate in the type of novel and difficult cases that have inspired the current debate.

One of the policy underpinnings of the Board’s recommendation is that providing an independent voice in FISC proceedings will increase public confidence in the integrity of those proceedings. Toward this end, the Board recommends that the rules for the Special Advocate program be made public and that the Attorney General provide regular and public reports on the program’s operation. Those recommendations are discussed in detail in the next section of this Report concerning transparency.

Recommendation 4. Congress should enact legislation to expand the opportunities for appellate review of FISC decisions by the FISCR and for review of FISCR decisions by the Supreme Court of the United States.

Over the past decade, the FISC has generated a significant body of law interpreting FISA authorities and other potentially applicable statutes, and analyzing related constitutional questions. However, FISC opinions have been much less likely to be subject to appellate review than the opinions of ordinary federal courts. Virtually all proponents of FISC reform, including judges who have served on the court, agree that there should be a greater opportunity for appellate review of FISC decisions by the FISCR and for review of the FISCR’s decisions by the Supreme Court of the United States.⁶³⁸ Providing for greater appellate review of FISC and FISCR rulings will strengthen the integrity of judicial review under FISA. Providing a role for the Special Advocate in seeking that appellate review will further increase public confidence in the integrity of the process.

Identifying the precise mechanism by which the Special Advocate could seek appellate review of a FISC decision that has rejected arguments based on alleged infringements of privacy or civil liberties is a hard task, but such a mechanism should not be impossible to design.

There are two basic ways in which the Special Advocate could seek judicial review of a FISC order: by directly filing a petition for review with the FISCR of orders that the Special Advocate believes are inconsistent with FISA or the Constitution; or by requesting that the FISC certify an appeal of its order. Under either approach, the Board would expect the Special Advocate, in deciding whether to seek an appeal, to exercise his or her judgment about the importance of the legal questions at stake and the severity of the implications for

⁶³⁸ See, e.g., Transcript of November 4, 2013 Hearing, *supra*, at 148-52 (testimony of Judge James Carr) (“[C]ertainly, in my day-to-day functions as an ordinary Article III judge, it [appellate review] is very important.”). See also Angela Canterbury (Project On Government Oversight), Kel McClanahan (National Security Counselors), & Patrice McDermott (OpenTheGovernment.org), Submission to the Privacy and Civil Liberties Oversight Board, at 4 (Aug. 1, 2013) (recommending that attorney representing the public “have the opportunity to appeal adverse decisions”), available at <http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0029>; Gregory T. Nojeim (Center for Democracy and Technology), Submission to the Privacy and Civil Liberties Oversight Board, at 6-7 (Aug. 1, 2013) (recommending that ombudsman representing civil liberties interests be able to address “whether an order that is granted should be appealed to the FISA Court of Review”), available at <http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0034>.

privacy or civil liberties. The Special Advocate would not be considered an adversary in the traditional sense, and would not be required to seek an appeal of every order that did not adopt the position he or she took before the FISC.

If Congress were to adopt the first approach, the Board would recommend a structure allowing the Special Advocate to file a petition with the FISCR seeking review of a FISC order and giving the FISCR discretionary review of the petition. This would be similar to the process of seeking certiorari in the Supreme Court of the United States. Congress or the FISCR could enact or adopt standards by which the FISCR would decide which petitions to grant, similar to the standards by which the Supreme Court decides when to grant a petition for certiorari.⁶³⁹ If the FISCR granted review, the Special Advocate would be permitted to participate in the matter, just as in the FISC. Similarly, Congress could authorize the Special Advocate to file a petition for certiorari seeking the Supreme Court's review of a FISCR decision in which the Special Advocate had participated. This approach would be consistent with the Board's recommendation above, which grants the court some discretion to manage the Special Advocate's role in proceedings. It also would have the benefit of allowing the Special Advocate to appeal without the permission of the court that issued the order in question.

Under the second approach, Congress would enact legislation authorizing FISC judges to certify their decisions to the FISCR for review. The Special Advocate would be eligible to file a motion with the FISC requesting the court to certify its decision to the FISCR and, if it were denied by the FISC, to appeal that denial. The Special Advocate could participate in any appellate proceedings that followed. In addition, Congress could amend 28 U.S.C. § 1254(2) to add the FISCR as a court authorized to certify a question of law to the Supreme Court for review,⁶⁴⁰ and the Special Advocate could be authorized to petition the FISCR to certify its decision to the Supreme Court for review. Under this approach, the decision whether to certify a case for review to the FISCR would be left to the discretion of the FISC or the FISCR, and the decision whether to certify a case for review to the Supreme Court would be left to the discretion of the FISCR.

Both approaches avoid concerns by some commentators that a Special Advocate lacks Article III standing to directly appeal a FISC decision.⁶⁴¹

⁶³⁹ See Rules of the Supreme Court of the United States, Rule 10 (July 1, 2013), available at <http://www.supremecourt.gov/ctrules/2013RulesoftheCourt.pdf>.

⁶⁴⁰ This statute currently provides that one of the methods by which cases in the courts of appeals may be reviewed by the U.S. Supreme Court is as follows: "By certification at any time by a court of appeals of any question of law in any civil or criminal case as to which instructions are desired, and upon such certification the Supreme Court may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy." 28 U.S.C. § 1254(2).

⁶⁴¹ See *e.g.*, Andrew Nolan, Richard M. Thompson II, & Vivian S. Chu, *Introducing a Public Advocate into the Foreign Intelligence Surveillance Act's Courts: Select Legal Issues*, CONGRESSIONAL RESEARCH SERVICE, at 20-24

Our recommendations for enhancing appellate review are based on the assumption that, as with traditional litigation in federal court, a FISC order would take effect immediately unless the court granted a stay of its order. Thus, when a Special Advocate appeals or seeks certification of an appeal of a FISC order, the surveillance approved by the FISC should generally be permitted to proceed pending any further review. The Special Advocate should be permitted to file a motion for a stay pending appeal that, if granted, would prohibit the government from immediately undertaking the approved surveillance. The government should be allowed to oppose this order and, as with similar stay motions in U.S. District Court, the FISC judge should determine whether to grant the stay. If the motion is denied, the Special Advocate should also be permitted to file similar motions in the FISCR and Supreme Court. FISA Section 103(f) already makes clear that judges of the FISC and FISCR and justices of the Supreme Court have the authority to order such stays pending review.

Recommendation 5. The FISC should take full advantage of existing authorities to obtain technical assistance and expand opportunities for legal input from outside parties.

FISC judges should take advantage of their ability to appoint Special Masters or other technical experts to assist them in reviewing voluminous or technical materials, either in connection with initial applications or in compliance reviews.

In addition, the FISC and the FISCR should develop procedures to facilitate amicus participation by third parties in cases involving questions that are of broad public interest, where it is feasible to do so consistent with national security. The Board recognizes that it will be difficult to take advantage of amicus participation by parties who lack national security clearances and cannot be privy to the facts of the case. Nevertheless, the fact that there has already been a case in which the FISCR has accepted input from amici and the FISC's recent order granting permission for the filing of an amicus brief⁶⁴² demonstrate that it is sometimes possible. The Special Advocate could advise the FISC or FISCR that amicus participation would be helpful in a particular case and ask the court to provide appropriate public notice of the opportunity for amicus participation.

(Oct. 25, 2013); Marty Lederman & Steve Vladeck, *The Constitutionality of a FISA "Special Advocate,"* JUST SECURITY (Nov. 4, 2013), <http://justsecurity.org/2013/11/04/fisa-special-advocate-constitution/>. The Board does not take a position on whether these concerns about lack of standing would ultimately prevail in litigation.

⁶⁴² See Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things* No. BR 13-158 (FISA Ct. Dec. 18, 2013).

Part 9:

DISCUSSION AND RECOMMENDATIONS REGARDING TRANSPARENCY

I. Introduction

In a representative democracy, the tension between openness and secrecy is inevitable and complex. The challenges are especially acute in the area of intelligence collection, where the powers exercised by the government implicate fundamental rights and our enemies are constantly trying to understand our capabilities in order to avoid detection. In this context, both openness and secrecy are vital to our survival, and we must strive to develop and implement intelligence programs in ways that serve both values.⁶⁴³

Transparency is one of the foundations of democratic governance.⁶⁴⁴ Our constitutional system of government relies upon the participation of an informed electorate. This in turn requires public access to information about the activities of the government. Transparency supports accountability. It is especially important with regard to activities of the government that affect the rights of individuals, where it is closely interlinked with redress for violations of rights.

There are also instrumental benefits to openness, as summarized by the Moynihan Commission:

Broad access to information promotes better decisions. It permits public understanding of the activities of government and promotes more informed debate and accountability. It increases the Government's ability to respond to criticism and justify its actions to the public. It makes possible the free exchange of scientific information and encourages new discoveries that foster economic growth. By allowing a better understanding of our history, it provides opportunities to learn lessons from the past, and it makes it easier to quash unfounded speculation about the Government's past actions. Reducing the amount of information in the classification system allows for better management and cost controls of that system and increases respect for the information that needs to stay protected. Greater access thus provides ground in which the public's faith in its government can flourish.⁶⁴⁵

⁶⁴³ "Protecting information critical to our Nation's security and demonstrating our commitment to open Government . . . are equally important priorities." Exec. Order No. 13,526 (Dec. 29, 2009).

⁶⁴⁴ See Exec. Order No. 13,292 (Mar. 25, 2003) ("Our democratic principles require that the American people be informed of the activities of their Government").

⁶⁴⁵ Report of the Commission on Protecting and Reducing Government Secrecy ("Moynihan Commission Report"), S. Doc. No. 105-2 at 49-50 (1997), *available at* <http://www.fas.org/sgp/library/moynihan/index.html>. The Moynihan Commission report remains one of

In the intelligence context, transparency regarding collection authorities and their exercise can increase public confidence in the intelligence process and in the monumental decisions that our leaders make based on intelligence products.⁶⁴⁶ With respect to electronic surveillance in particular, where the government depends on the cooperation of service providers and those service providers in turn depend for their commercial success on the trust of their customers, transparency, if coupled with a system of appropriate controls, can help boost public confidence in the security and confidentiality of communications services. Public disclosure showing that certain techniques are applied with more precision and under stricter controls than many fear can help allay concerns, benefiting U.S.-based companies in the global marketplace. Transparency also works in tandem with other forms of oversight and control, alerting Congress, courts, inspectors general and others, including this Board, to issues that merit deeper scrutiny in public and classified settings. As the 9/11 Commission noted, “[s]ecrecy, while necessary, can also harm oversight.”⁶⁴⁷

However, we must also recognize the critical functions served by government secrecy. To quote again from the Moynihan Commission:

Effective secrecy has proven indispensable to the functioning of government, serving the interests not only of the officials in power but of the governed as well. . . . The primary objective of government secrecy in the national security realm . . . is to protect U.S. interests by controlling information that provides an advantage (including the element of surprise) over an adversary or prevents that adversary from gaining an advantage that could damage the United States. . . . The maintenance of secrecy has proven essential to the successful development, implementation, and completion (or, conversely, the abandonment) of plans and missions. . . . The successful conduct of plans and missions in turn may depend on protecting key technologies. . . . Secrecy also is essential to the effective conduct of diplomatic negotiations. . . . Closely linked to [these] is the protection of internal policy deliberations: the negotiations among government officials that precede and accompany the development of the plans, missions, and external negotiations cited above. . . . Thus, drafts and memoranda used in negotiations often remain classified

the best sources on both the importance of protecting secrets and the costs of secrecy. *See id.* at 6-10 (discussing both principles).

⁶⁴⁶ *See* Nick Hopkins, *Former NSA Chief: Western Intelligence Agencies must be more Transparent*, THE GUARDIAN (Sept. 30, 2013) (quoting former NSA Director Michael Hayden: “It’s clear to me now that in liberal democracies the security services don’t get to do what they do without broad public understanding and support. And although the public cannot be briefed on everything, there has to be enough out there so that the majority of the population believe what they are doing is acceptable.”).

⁶⁴⁷ 9/11 Commission Report, *supra*, at 103.

even when the final positions and statements do not. . . . Finally, secrecy is essential in protecting confidential relationships with individuals.⁶⁴⁸

Despite widespread support for balancing openness and secrecy, there has been equally widespread consensus within and without the government that the system tilts too far in the direction of secrecy.⁶⁴⁹ Even officials who themselves have implemented the classification system have long been saying that the government has far too many secrets.⁶⁵⁰

Undoubtedly, “we can, and must, be more transparent.”⁶⁵¹ The question is how. Generalities about the value of transparency do not go far in answering the hard questions of what can be disclosed and what must remain secret. Instead, progress may best be achieved by considering specific problems.⁶⁵² In that spirit, our focus here will be on transparency with regard to the Section 215 program, the opinions of the FISC, and statistical reporting on the government’s use of FISA authorities. Insights garnered with respect to those three concrete matters may have broader value regarding transparency about other legal authorities of the government that affect the rights of individuals and about the scope of the exercise of those powers.

⁶⁴⁸ Moynihan Commission Report, *supra*, at 6-7.

⁶⁴⁹ There is a long history of official studies finding that too much information is classified. In 1956, the Defense Department Committee on Classified Information found that “overclassification has reached serious proportions.” DEF. DEP’T COMM. ON CLASSIFIED INFO., REPORT TO THE SECRETARY OF DEFENSE BY THE COMMITTEE ON CLASSIFIED INFORMATION 6 (1956). Forty years later, the Moynihan Commission found that the information classification system sought to protect far too much information while not effectively protecting the most important secrets. *See* Moynihan Commission Report, *supra*. Fifteen years after that, the Public Interest Declassification Board (“PIDB”), an advisory committee established by Congress, concluded that the current classification system “keeps too many secrets, and keeps them too long.” Public Interest Declassification Board, *Transforming the Security Classification System*, at 2 (Nov. 2012), available at <http://www.archives.gov/declassification/pidb/recommendations/transforming-classification.html>. For summaries of other official condemnations of overclassification, *see* Steven Aftergood, *Reducing Government Secrecy: Finding What Works*, 27 YALE L. & POL’Y. REV. 399, 404-07 (2009).

⁶⁵⁰ *See, e.g.*, IC21: The Intelligence Community in the 21st Century: Hearing before H. Permanent Select Comm. on Intelligence, 104th Cong., at 204 (July 27, 1995) (testimony of former National Security Advisor Brent Scowcroft) (“I think there is no question that we classify too much.”). Former Deputy Under Secretary of Defense for Intelligence and Security Carol Haave told a House subcommittee in 2004 that the amount of defense information that is overclassified or unnecessarily classified could be as much as fifty percent. Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing: Hearing before the Subcomm. on National Security, Emerging Threats and International Relations before H. Comm. on Gov’t Reform, 108th Cong., at 82 (Aug. 24, 2004) (testimony of Carol Haave).

⁶⁵¹ President Barack Obama, Remarks by the President in a Press Conference at the White House (Aug. 9, 2013), available at <http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference>.

⁶⁵² *See* Steven Aftergood, *Reducing Government Secrecy: Finding What Works*, *supra*, at 407-14.

We expect to return to transparency in our future work.⁶⁵³ In our first semi-annual report, issued before the Snowden leaks, the Board identified transparency as a cross-cutting issue that it intended to pursue. In part, this Report contributes to that goal, as we seek to describe the Section 215 telephone metadata program in a more comprehensive and accurate way than has been done anywhere else so far.⁶⁵⁴ We plan to provide a similarly detailed picture of the Section 702 program in a subsequent report.

II. Recent Developments

In the aftermath of the Snowden disclosures, the government has released a substantial amount of information on the leaked government surveillance programs. These official disclosures have helped foster greater public understanding of government surveillance programs, although there remains a deep well of distrust.

In August 2013, following the President's directive, the Office of the Director of National Intelligence ("ODNI") created a new public website, "IC on the Record." Through this website, the ODNI has released thousands of pages of documents related to the Section 215 and 702 programs as well as other material regarding FISA and the operation of the FISC more generally. The site also compiles a variety of public statements by government officials on these topics, including press statements and congressional testimony.

The FISA court has also newly created a website where it posts pleadings, orders and other materials.⁶⁵⁵ Recently, public interest groups have initiated proceedings in the

⁶⁵³ Promoting appropriate transparency in counterterrorism programs is an express part of the PCLOB's statutory mandate. Our authorizing statute charges the Board with making our reports public, holding public hearings, and otherwise informing the public of our activities, as appropriate and in a manner consistent with the protection of classified information and applicable law. *See* 42 U.S.C. § 2000ee(f).

⁶⁵⁴ A group of 53 non-governmental organizations joined in a letter to the PCLOB on July 9, 2013, asking that the PCLOB seek disclosure "of sufficient information to enable the public to understand the existing legal authorities for national security surveillance of Americans and the administration's interpretation of their scope, and to permit an informed public debate on government surveillance."

⁶⁵⁵ U.S. Foreign Intelligence Surveillance Court Public Filings (Beginning June 2013), *available at* <http://www.uscourts.gov/uscourts/courts/fisc/index.html>.

FISC seeking release of FISC decisions⁶⁵⁶ and seeking the ability to participate in proceedings on future government applications for renewal of FISA programs.⁶⁵⁷

There have also been increased disclosures under the Freedom of Information Act, a cornerstone of our system of transparency whose limitations in the national security arena are well known. Some of the documents newly released to the public by the government have been released in lawsuits filed under FOIA years before the Snowden leaks.⁶⁵⁸ After the Snowden leaks, the government has confirmed the existence of these programs, defined the scope of documents discoverable in the litigation relatively broadly, and moved expeditiously to create redacted versions of classified documents for release.

However, to date the official disclosures relate almost exclusively to specific programs that had already been the subject of leaks, and we must be careful in citing these disclosures as object lessons for what additional transparency might be appropriate in the future. Any harm to national security was already done with Snowden's illegal disclosures. Additional material has been officially disclosed to correct misperceptions caused by fragmentary leaks, but in part such disclosures were considered appropriate because it was judged that the marginal additional harm to national security would be minimal.

The reactive nature of the government's disclosures gives little insight into what principles should guide transparency in any programs not yet disclosed or still on the drawing board. Nor do we yet have insights into what in retrospect the intelligence

⁶⁵⁶ In one case pending before the FISC where public interest groups sought disclosure of a FISC opinion issued on February 19, 2013 interpreting Section 215, Judge Saylor ordered the government to submit a detailed explanation of its conclusion that it was unable to create a redacted version of that opinion. *In re: Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (FISA Ct. Nov. 20, 2013), available at <http://www.uscourts.gov/uscourts/courts/fisc/misc-13-02-order-131120.pdf>. The government responded on December 20, 2013, indicating that it had created a proposed redacted opinion for the court's review. See Submission of the United States in Response to the Court's November 20, 2013 Order. *Id.* (FISA Ct. December 20, 2013), available at <http://www.uscourts.gov/uscourts/courts/fisc/br13-02-order-131230.pdf>.

⁶⁵⁷ In addition to seeking permission to file an amicus brief, as described earlier, the Center for National Security Studies' petition sought to require the government to file a public application and have the FISC sit en banc when the FISC considered renewal of Section 215 orders in January 2014. Although the FISC granted permission for CNSS to file an amicus brief, it denied the other requests. See *In re: Application of the FBI for an Order Requiring the Production of Tangible Things*, No. BR 13-158 (FISA Ct. December 18, 2013), available at <http://www.uscourts.gov/uscourts/courts/fisc/br13-158-Memorandum-131218.pdf>.

⁶⁵⁸ Years before the Snowden leaks, the American Civil Liberties Union and the Electronic Frontier Foundation had filed FOIA lawsuits seeking information on the government's interpretation and application of Sections 215 and 702. See *American Civil Liberties Union v. Federal Bureau of Investigation*, No. 11-7562 (S.D.N.Y. 2011) (FOIA suit seeking records concerning the FBI's use and interpretation of Section 215); *Electronic Frontier Foundation v. U.S. Department of Justice*, No. 11-5221 (N.D. Cal. 2011) (Section 215 FOIA); see also *Electronic Frontier Foundation v. U.S. Department of Justice*, No. 12-1441 (D.D.C. 2012) (Section 702 FOIA).

community believes might have been disclosed earlier in the case of the leaked programs without unreasonable risk to national security.

The Board believes that the government must take the initiative and formulate long-term solutions that promote greater transparency for government surveillance policies more generally, in order to inform public debate on technology, national security, and civil liberties going beyond the current controversy over the Section 215 and 702 programs. In this effort, all three branches have a role.

There are some guideposts for how to draw the lines that need to be drawn to actually implement transparency in a responsible way. Some recent examples suggest possible criteria for transparency.

III. Transparency by the Executive Branch

On March 22, 2012, the Office of the Director of National Intelligence and the Department of Justice announced that they had adopted revised guidelines on the access, retention, use, and dissemination by the National Counterterrorism Center (“NCTC”) of information in databases of other agencies containing non-terrorism information. The ODNI and DOJ issued a press release about the guidelines⁶⁵⁹ and posted the guidelines themselves on the Internet.⁶⁶⁰ The announcement attracted immediate media attention.⁶⁶¹ Public interest organizations published analyses of the guidelines.⁶⁶² The ACLU produced a redline comparing the revised guidelines to the prior version.⁶⁶³ *The Wall Street Journal* further investigated the background of the guidelines’ development and published a major

⁶⁵⁹ Office of the Director of National Intelligence and U.S. Department of Justice Joint Statement, “Revised Guidelines Issued to Allow the NCTC to Access and Analyze Certain Federal Data More Effectively to Combat Terrorist Threats” (Mar. 22, 2012), available at <http://www.dni.gov/index.php/newsroom/press-releases/96-press-releases-2012/528-odni-and-doj-update-guidelines-for-nctc-access,-retention,-use,-and-dissemination-of-information-in-datasets-containing-non-terrorism-information>.

⁶⁶⁰ Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information (March 2012), available at <http://www.nctc.gov/docs/NCTC%20Guidelines.pdf>.

⁶⁶¹ See Charlie Savage, *U.S. Relaxes Limits on Use of Data in Terror Analysis*, N.Y. TIMES (Mar. 22, 2012).

⁶⁶² John Malcom, Jessica Zuckerman and Andrew Kloster, *New National Counterterrorism Center Guidelines Require Strong Oversight*, HERITAGE FOUNDATION (Feb. 21, 2013), available at <http://www.heritage.org/research/reports/2013/02/new-national-counterterrorism-center-guidelines-require-strong-oversight>; Chris Calabrese, *The Biggest New Spying Program You’ve Probably Never Heard Of*, ACLU (July 30, 2012), available at <https://www.aclu.org/blog/national-security-technology-and-liberty/biggest-new-spying-program-youve-probably-never-heard>; Rachel Levinson-Waldman, *What the Government Does with Americans’ Data*, BRENNAN CENTER FOR JUSTICE, at 19-22 (Oct. 2013), available at <http://www.brennancenter.org/publication/what-government-does-americans-data>.

⁶⁶³ 2008 National Counterterrorism Center Guidelines Redlined with 2012 Changes, ACLU (July 27, 2012), available at <https://www.aclu.org/national-security/2008-national-counterterrorism-center-guidelines-redlined-2012-changes>.

story in December 2012.⁶⁶⁴ Later, the ODNI's privacy office issued an information paper describing the civil liberties and privacy protections in the updated guidelines.⁶⁶⁵

The government's decision to write the guidelines in unclassified form not only supported press and advocacy inquiry, but also served to bring the guidelines to the attention of oversight entities, which could then pursue further classified oversight. In fact, soon after PCLOB members began substantive work, in December 2012, we sought and received one of several in-depth briefings on the guidelines from the NCTC, followed by a briefing from the Department of Homeland Security.

The release of the NCTC guidelines is only one example of the preparation and release of key policy documents in unclassified form. The Attorney General Guidelines on FBI investigations, which govern not only criminal investigations but also investigations for foreign intelligence purposes, are unclassified. The FBI's massive manual of investigative procedures is largely public, covering not only criminal investigations, but also national security matters, and describing in great detail the situations in which various investigative techniques are used.⁶⁶⁶ Key criteria for operation of the nation's airline passenger screening system were publicly developed through a notice and comment proceeding,⁶⁶⁷ and substantial information about the program, including a Privacy Impact Assessment, is published online.⁶⁶⁸

These and other disclosures about key national security programs that involve the collection, storage and dissemination of personal information show that it is possible to describe practices and policies publicly, even those that have not been otherwise leaked, without damage to national security or operational effectiveness. Of course, the targets of investigation are secret, and may remain so indefinitely in the case of national security investigations. But a very wide range of legal authorities is laid out, along with the criteria for exercising them.

⁶⁶⁴ Julia Angwin, *U.S. Terrorism Agency to Tap a Vast Database of Citizens*, WALL STREET JOURNAL (Dec. 13, 2012).

⁶⁶⁵ Office of the Director of National Intelligence, Civil Liberties and Privacy Office, "Description of Civil Liberties and Privacy Protections Incorporated in the Updated NCTC Guidelines" (January 2013), *available at* http://www.nctc.gov/docs/CLPO_Information_Paper_on_NCTC_AG_Guidelines_-_1-22-13.pdf.

⁶⁶⁶ FBI Domestic Investigations and Operations Guide (DIOG) (2011 Version), *available at* <http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%209/fbi-domestic-investigations-and-operations-guide-diog-2011-version/>.

⁶⁶⁷ Department of Homeland Security, Transportation Security Administration, Secure Flight Program Final Rule, 73 Fed. Reg. 64018 (Oct. 28, 2008), *available at* <http://www.gpo.gov/fdsys/pkg/FR-2008-10-28/html/E8-25432.htm>.

⁶⁶⁸ Transportation Security Administration, Secure Flight Program, <http://www.tsa.gov/stakeholders/secure-flight-program>.

IV. Transparency in the Legislative Process

When Section 215 was adopted in 2001 to authorize applications for FISA court orders requiring production of “any tangible things,” there was no mention in the public record that it was intended to provide legal justification for the bulk collection of business records. (There is also no indication that there was any non-public discussion of using the statute in that way, as the bulk collection programs were just beginning when Section 215 was adopted and those nascent bulk programs were proceeding under different legal theories not involving approval of the FISA court). When the statute was revised and reauthorized in 2005–2006, there was no also indication on the public record that it would provide the legal justification for bulk collection, although by then the existence of bulk collection programs was known to some members of Congress. During the 2005-2006 reauthorization debate, critics of Section 215 speculated that it could be used to acquire entire data sets, although none speculated that it could be used to justify ongoing collection, and the government’s public statements did not address bulk collection. By the time Section 215 was up for renewal in 2011, it was known to some members of Congress that the statute was being used to support bulk collection, and the DOJ provided Congress with a classified description of the NSA’s telephone and Internet bulk collection programs.⁶⁶⁹ But public references by Senators familiar with the program to “sensitive sources and collection methods” and “secret legal interpretations”⁶⁷⁰ were so guarded that there was no public discussion of bulk collection.⁶⁷¹

With full respect for the pressure confronting Congress and the executive branch in the years after 9/11 and up until this very day, we do not believe that the process surrounding the application of Section 215 to bulk collection comported with the kind of public debate that best serves the development of policy affecting the rights of Americans.⁶⁷² Even where classified intelligence operations are involved, the “purposes

⁶⁶⁹ See pages 97 to 99 of this Report.

⁶⁷⁰ Statement of Senator Ron Wyden re: Patriot Act Reauthorization (May 26, 2011) (“[W]hen the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry. . . . Members of the public have no access to the executive branch’s secret legal interpretations, so they have no idea what their government thinks this law means.”) available at <http://www.wyden.senate.gov/news/press-releases/in-speech-wyden-says-official-interpretations-of-patriot-act-must-be-made-public>.

⁶⁷¹ In an indication of how little information was made available to the public, one close observer of the surveillance debates mistakenly concluded in 2011 that there was “fairly persuasive” evidence that Senator Wyden was referring to the collection of geolocation data — the one piece of metadata that the government was in fact *not* collecting under the 215 program. See Julian Sanchez, *Atlas Bugged: Why the “Secret Law” of the Patriot Act is Probably About Location Tracking*, CATO AT LIBERTY (May 27, 2011), <http://www.cato.org/blog/atlas-bugged-why-secret-law-patriot-act-probably-about-location-tracking>.

⁶⁷² Referring generally to the “many legal novelties and legal hurdles that the administration faced after 9/11,” former Assistant Attorney General Jack Goldsmith concluded, “The administration’s failure to engage Congress deprived the country of national debates about the nature of the threat and its proper response that

and framework” of a program for domestic intelligence collection should be debated in public.⁶⁷³ Here we are talking specifically about the legislative process and programs that are intended to be ongoing; different considerations may apply, for example, when a statute is being applied case-by-case to unique fact situations. Also, during the process of developing legislation, some hearings and briefings may need to be conducted in secret to ensure that policymakers fully understand the intended use of a particular authority. But the government should not base an ongoing program affecting the rights of Americans on an interpretation of a statute that is not apparent from a natural reading of the text. Either the statute should be amended or, if the statute is subject to periodic reauthorization, the legal interpretation extending the statute to a new program should be made public before the statute is reauthorized.

In the case of Section 215, the government should have made it publicly clear in the reauthorization process that it intended for Section 215 to serve as legal authority to collect data in bulk on an ongoing basis. It should have been possible for the government to describe criteria for selecting categories of data for acquisition as well as procedures around storage and use of such data. It may have been appropriate to withhold the specific categories of data (telephony metadata) that the government intended to collect. Certainly, once the program was statutorily authorized, it would be appropriate to keep secret the names of the telephone carriers subject to the FISC orders. A description of the power sought would have avoided the many legal questions now being raised about the government’s interpretation of Section 215, such as the scope of the “relevance” standard, the use of the statute for ongoing disclosures, and the extent to which bulk collection under Section 215 may conflict with other statutes.

would have served an educative and legitimating function regardless of what emerged from the process. The go-it-alone strategy minimized the short-term discomforts to the Executive branch of public debate, but at the expense of medium-term Executive Branch mistakes. When the Executive Branch forces Congress to deliberate, argue, and take a stand, it spreads accountability and minimizes the recriminations and other bad effects of the risk taking that the President’s job demands.” *See* Preserving the Rule of Law in the Fight Against Terrorism, Hearing before the Senate Judiciary Committee (Oct. 2, 2007) (statement of Jack Landman Goldsmith), *available at*

http://www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da12ecadc&wit_id=e655f9e2809e5476862f735da12ecadc-1-1.

⁶⁷³ Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing, Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, 290-93 (Nov. 4, 2013) (testimony of Jane Harmon, former Member of Congress and Member of House Armed Services, Homeland Security, and Intelligence Committees), *available at* <http://www.pclob.gov/>.

V. Release of FISC and FISCR Opinions

Since 9/11, and especially since 2004, the FISA court has confronted novel and significant legal questions, as the government has brought various programs under the FISA system, as the statute itself has been amended, including to add new authorities, and as technology and the government's capabilities have evolved. Consequently, in the past ten years the court has issued a substantial body of opinions on statutory and constitutional questions.⁶⁷⁴ These opinions discuss and approve the underlying legal rationale for government activities and address the implications of compliance issues and other matters raised by the sometimes unique conditions judges are imposing on the operation of approved programs. In short, these opinions describe (often in very accessible language) the scope of the government's authority and the ways in which that authority is implemented in contexts affecting the rights of Americans. There is thus public interest in the disclosure of these opinions.

FISA requires that "The record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence."⁶⁷⁵ Until recently, with two exceptions from 1981 and 2002, FISC opinions were written in a totally classified fashion, without an eye to publication in any form, with facts and law tightly interwoven. The recent release of opinions regarding already leaked programs offers, in itself, little insight into how to maximize disclosure of legal opinions.

Nevertheless, there is precedent for public disclosure of opinions on sensitive intelligence matters. Early in the history of FISA, a FISC opinion was written in unclassified form on a question of law (whether the court had the authority to issue orders approving physical searches).⁶⁷⁶ Since 9/11, two opinions of the FISCR were released at the time they were issued, with relatively few redactions.⁶⁷⁷ Regular Article III courts have been

⁶⁷⁴ If our recommendations on creation of a Special Advocate are implemented, the number of opinions may increase at an even greater rate. And while the FISCR has heard relatively few cases, that too would change if our recommendations are implemented for creating a path for appellate review of FISC decisions.

⁶⁷⁵ 50 U.S.C. § 1803(c).

⁶⁷⁶ *In re Application of the United States for an Order Authorizing the Physical Search of Nonresidential Premises and Personal Property*, slip op. (FISA Ct. June 11, 1981) (in case preceding enactment of amendment to FISA providing explicit authority for physical searches, court found that it lacked such authority). *See also In Re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp.2d 611 (FISA Ct. 2002) (addresses government request to permit greater sharing of information between law enforcement and intelligence personnel in the aftermath of September 11th), *rev'd sub nom. In Re Sealed Case 310 F.3d 717* (FISA Ct. Rev. 2002).

⁶⁷⁷ *In Re Sealed Case 310 F.3d 717* (FISA Ct. Rev. 2002), and *In Re Directives*, 551 F.3d 1004 (FISA Ct. Rev. 2008). Based upon the best information available to the Board, these are the only two cases decided by the FISCR to date.

grappling with secrecy issues in opinions on habeas petitions by Guantanamo detainees and in other matters. Combining the best of the methods applied by judges so far, redactions can be grouped together so that the rest of the text remains uninterrupted and comprehensible, the significance of the redacted information to the holding could be explained, and unclassified summaries of the redacted paragraphs could be added.⁶⁷⁸

In recent months, we are told that the FISC judges have begun drafting their opinions with the expectation that they may be declassified and released in redacted form.⁶⁷⁹ We believe that, as a general rule, FISA court judges can write their opinions in such a way as to separate specific facts peculiar to the case at hand from broader legal analyses. This trend is one that we view as a significant step toward greater transparency not only with regard to already disclosed programs, but also with respect to other matters that may arise. Prospectively, we encourage the FISA court to write opinions with an eye to declassification. We also believe that there is significant value in producing declassified versions of earlier opinions. We realize that the process of redacting opinions written during a period of presumed secrecy will be more difficult and will burden individuals with other pressing duties, but we believe that it is appropriate to make the effort where those opinions and orders complete the historical picture of the development of legal doctrine regarding matters within the jurisdiction of the FISC.

We therefore recommend that the government undertake a classification review of all significant FISC opinions and orders involving novel interpretations of law, beginning with opinions describing the legal theories relied upon for widespread collection of metadata from Americans not suspected of terrorist affiliations, to be followed by opinions involving serious compliance issues.

We note one other transparency matter concerning the FISC. Should the government adopt our recommendation for a Special Advocate in the FISC, the nature of that advocate's role must be transparent to be effective. The FISC should publicly disclose any rules the court adopts governing the advocate's participation in proceedings. In addition, the Attorney General should regularly and publicly report statistics on the frequency of Special Advocate participation including the number of times Special Advocates have sought review of FISC decisions in the FISCR and the U.S. Supreme Court.

⁶⁷⁸ Michael A. Sall, *Classified Opinions: Habeas at Guantanamo and the Creation of Secret Law*, 101 GEO. L.J. 1147, 1167 (citing, *inter alia*, *Parhat v. Gates*, 532 F.3d 834, 844 (D.C. Cir. 2008)).

⁶⁷⁹ For example, Judge Eagan's August 29, 2013 opinion and order reauthorizing the Section 215 bulk telephony metadata program were released in redacted form less than one month after issuance. The declassified version of the opinion as well as the accompanying order containing Judge Eagan's legal analysis includes very few redactions. See Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

VI. Increased Public Reporting

One important way to understand and assess any government program is numerically — to categorize its critical elements and count them. Periodic public reporting on surveillance programs is a valuable tool promoting accountability and public understanding. When the government was seeking reauthorization of the Patriot Act, it publicly released detailed numerical information about the use of sunseting authorities as a way of reassuring Congress and the public that the authorities were being used in a targeted and limited fashion.⁶⁸⁰ When FISA was first adopted in 1978, it included a provision requiring the Attorney General every year to transmit to Congress a report setting forth the total number of applications made for FISA surveillance and the total number of such orders either granted, modified, or denied.⁶⁸¹ The reports, while skeletal, have never been classified.⁶⁸² Since 1978, Congress amended FISA to require the government to provide to Congress additional information, including a breakdown of the number of persons targeted under the statute's various authorities.⁶⁸³ These more detailed reports, however, are classified and the granularity of public reporting remains very limited.

We recommend that the government should also increase the level of detail in its unclassified reporting to Congress and the public regarding surveillance programs. It is important to ensure that any public reporting does not aid our adversaries. However, we believe that publication of additional numerical information on the frequency with which various surveillance authorities are being used would be possible without allowing terrorists to improve their tradecraft. To ensure that such information is meaningful, the government would have to distinguish between particularized programs and those involving bulk collection. In the case of targeted programs, the government should disclose how many orders have been issued and how many individuals have been targeted.

⁶⁸⁰ See, e.g., Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee, 109th Cong. at 8-9 (April 28, 2005) (statement of Kenneth Wainstein) (“As of March 30, 2005, federal judges have reviewed and granted the Department’s request for a section 215 order 35 times. To date, the provision has only been used to obtain driver’s license records, public accommodations records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen registers and trap-and-trace orders (a pen register records the numbers a telephone dials and a trap-and-trace device records the numbers from which it receives calls). The Department has not requested a section 215 order to obtain library or bookstore records, medical records, or gun sale records.”), available at <http://www.justice.gov/archive/ll/subs/testimony/042805-usa-wainstein.pdf>.

⁶⁸¹ Pub. L. 95-511, 92 Stat. 1783, 1795 (1978) (codified at 50 U.S.C. § 1807).

⁶⁸² For a collection of these reports, see the Federation of American Scientists’ website: <https://www.fas.org/irp/agency/doj/fisa/#rept>.

⁶⁸³ See 50 U.S.C. §§ 1862, 1871.

In recent years, U.S. companies have begun publishing reports showing, country by country, how many government demands they receive for disclosure of user data (and how often they receive demands for takedown of content.) The companies find these reports useful in building and maintaining customer trust. However, the secrecy of FISA orders and National Security Letters limits the ability of private sector entities to disclose to their customers the scope of government surveillance or data disclosure demands. The United States is one of few countries that permit any publication of figures on government surveillance, but the unique position of the United States in the global communications infrastructure puts unique pressure on companies headquartered here. Some Internet service providers have sought permission to voluntarily disclose statistics regarding the number of government FISA requests they have received and the number of their customers affected.⁶⁸⁴ Government officials have opposed these requests in part on the grounds that such statistics would reveal government capabilities and could indicate to would-be terrorists which providers to favor and which to avoid. The government has indicated, however, that it may be possible to provide aggregate statistics in a way that does not jeopardize national security in this fashion. We urge the government to work with the companies to reach agreement on standards allowing reasonable disclosures of aggregate statistics that would be meaningful without revealing sensitive government capabilities or tactics.

Beyond public reporting, FISA requires the Attorney General to “fully inform” the Senate and House Intelligence and Judiciary Committees regarding the government’s activities under certain sections of FISA including Section 215.⁶⁸⁵ FISA also requires the government to provide the congressional committees with copies of “all decisions, orders, or opinions of the FISC or FISC that include significant construction or interpretation” of the provisions of FISA. These two reporting requirements facilitate congressional oversight. The Board urges the government to extend this complete reporting to the PCLOB as well, to facilitate the Board’s oversight role.

⁶⁸⁴ Google, Inc., Microsoft Corporation, Yahoo! Inc., Facebook, Inc., and LinkedIn Corporation have filed declaratory judgment actions in the FISC seeking permission to disclose such statistics, and additional providers have filed motions seeking permission to participate in the cases as friends of the court. The FISC has created a public docket of these filings. *See* FISA Ct., Nos. Misc. 13-03, Misc. 13-04, Misc. 13-05, Misc. 13-06, & Misc. 13-07, *available at* <http://www.uscourts.gov/uscourts/courts/fisc/index.html>.

⁶⁸⁵ *See* 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f. Reporting requirements under Sections 1808 and 1862 do not include the House Judiciary Committee, but the other sections include all four committees.

VII. Recommendations to Promote Transparency

Recommendation 6. To the maximum extent consistent with national security, the government should create and release with minimal redactions declassified versions of new decisions, orders and opinions by the FISC and FISCR in cases involving novel interpretations of FISA or other significant questions of law, technology or compliance.

FISC judges should continue their recent practice of drafting opinions in cases involving novel issues and other significant decisions in the expectation that declassified versions will be released to the public. This practice has facilitated declassification review. The government should promptly create and release declassified versions of these FISC opinions.

Recommendation 7. Regarding previously written opinions, the government should perform a declassification review of decisions, orders and opinions by the FISC and FISCR that have not yet been released to the public and that involve novel interpretations of FISA or other significant questions of law, technology or compliance.

Although it may be more difficult to declassify older FISC opinions drafted without expectation of public release, the release of such older opinions is still important to facilitate public understanding of the development of the law under FISA. The government should create and release declassified versions of older opinions in novel or significant cases to the greatest extent possible consistent with protection of national security. This should cover programs that have been discontinued, where the legal interpretations justifying such programs have ongoing relevance. The Board acknowledges the cumulative burden of these transparency recommendations, especially as the burden of review for declassification may fall on the same individuals who are responsible for preparing new FISA applications, overseeing compliance with existing orders, and carrying out other duties. The Board urges the government to develop and announce some prioritization plan or approach. We recommend beginning with opinions describing the legal theories relied upon for widespread collection of metadata from Americans not suspected of terrorist affiliations, to be followed by opinions involving serious compliance issues.

Recommendation 8. The Attorney General should regularly and publicly report information regarding the operation of the Special Advocate program recommended by the Board. This should include statistics on the frequency and nature of Special Advocate participation in FISC and FISCR proceedings.

These reports should include statistics showing the number of cases in which a Special Advocate participated, as well as the number of cases identified by the government as raising a novel or significant issue, but in which the judge declined to invite Special

Advocate participation. The reports should also indicate the extent to which FISC decisions have been subject to review in the FISCR and the frequency with which Special Advocate requests for FISCR review have been granted. The Attorney General can make such reports without the need for a congressional directive. However, Congress might amend FISA's reporting requirement to require the Attorney General to report in unclassified form on the number of matters in which the government notified the court of a novel issue under Rule 11 and, in such cases, the number of times the FISC invited Special Advocate participation.⁶⁸⁶ In addition to providing such regular public reports, the Attorney General should include statistics and information on operation of the Special Advocate as part of the Attorney General's obligation under 50 U.S.C. § 1871(a)(5) to submit to congressional committees copies of all decisions or opinions of the FISC that include significant construction or interpretation of the provisions of FISA.

The FISC should also make public any rules adopted by the FISC governing the Special Advocate's participation in court proceedings.

Recommendation 9. The government should work with Internet service providers and other companies that regularly receive FISA production orders to develop rules permitting the companies to voluntarily disclose certain statistical information. In addition, the government should publicly disclose more detailed statistics to provide a more complete picture of government surveillance operations.

The Board understands that the government has engaged in discussions with certain communications service providers that are seeking permission to publish statistics about the number of government surveillance and data disclosure requests they receive per year. The Board urges the government to pursue these discussions to determine the maximum amount of information that could be published in a way that is consistent with protection of national security. In addition, the government should itself release annual reports showing in more detail the nature and scope of FISA surveillance for each year. The government disclosures showing the number of orders or demands directed to private entities could be provided in numerical ranges and aggregated for all providers, but they should be separated by the type of FISA authority involved. Thus, for example, all Section

⁶⁸⁶ Since FISA first came into effect, the government has filed in unclassified form the report required under Section 107 of the Act covering certain annual statistics regarding the number of FISA applications and orders. 50 U.S.C. § 1807. Over the years, those reports have become somewhat longer with the addition of further reporting requirements. Compare the report for 1979, <https://www.fas.org/irp/agency/doj/fisa/1979rept.html>, with the report for 2012, <https://www.fas.org/irp/agency/doj/fisa/2012rept.pdf>. Section 502 of the Act, 18 U.S.C. § 1862, regarding business records, specifically requires unclassified reporting of these statistics, and Section 118 of the USA PATRIOT Improvement and Reauthorization Act, Pub. L. 109-177, 120 Stat. 192, 217 (2006), requires unclassified reports on use of National Security Letter authorities.

215 requests for all companies could be aggregated, but Section 215 statistics would be reported separately from requests under other FISA authorities.

The Board recognizes that company-by-company reporting presents certain difficulties, as does reporting of the number of customers affected. On the one hand, so long as one FISA order can encompass multiple accounts, a simple statement of the number of demands received will not indicate how many accounts or customers are affected. On the other hand, if a company is allowed to report the number of customers affected (even in ranges), if its numbers suddenly jump from the range of hundreds or thousands of customers affected to millions or hundreds of millions, that would immediately signal that that particular company has received a bulk collection demand, a fact that may be operationally sensitive. At the very least, both government and companies need to agree on the rules for reporting numbers of customers affected. Perhaps, the content versus non-content distinction is relevant: Companies could be permitted to disclose the number of customers or accounts affected by FISA acquisitions of content, but not by bulk collections of metadata.⁶⁸⁷

The problem could be further mitigated if the Board's recommendation regarding transparency of bulk collection authorities is adopted. The government could indicate how many orders for bulk collection it has obtained, and under which legal authority, without disclosing which companies have received bulk collection orders. Otherwise, if a statute such as Section 215 continues to be used as the basis both for individualized collection and bulk collection, the mere number of Section 215 orders could be misleading. Despite the attention that has been given to numerical reporting, mere numbers can be misleading. A key thrust of the Board's recommendations is that the government should first and foremost explain, to the extent possible, what it is doing and should contextualize the numbers that it issues.

Recommendation 10. The Attorney General should fully inform the PCLOB of the government's activities under FISA and provide the PCLOB with copies of the detailed reports submitted under FISA to the specified committees of Congress. This should include providing the PCLOB with copies of the FISC decisions required to be produced under Section 601(a)(5).

Recommendation 11. The Board urges the government to begin developing principles and criteria for transparency.

⁶⁸⁷ Our suggestions here focus on FISA authorities and are also relevant to National Security Letters. Our recommendations do not address reporting of activities under Executive Order 12333. It has become clear in recent months that E.O. 12333 collection poses important new questions in the age of globalized communications networks, but the Board has not yet attempted to address those issues.

The Board has offered some initial suggestions about how lines can be drawn in the future around the disclosure of legal authorities. The Board urges the Administration to commence the process of articulating principles and criteria for deciding what must be kept secret and what can be released as to existing and future programs that affect the American public.

Recommendation 12. The scope of surveillance authorities affecting Americans should be public.

In particular, the Administration should develop principles and criteria for the public articulation of the legal authorities under which it conducts surveillance affecting Americans. If the text of the statute itself is not sufficient to inform the public of the scope of asserted government authority, then the key elements of the legal opinion or other document describing the government's legal analysis should be made public so there can be a free and open debate regarding the law's scope. This includes both original enactments such as 215's revisions and subsequent reauthorizations.

The Board's recommendation distinguishes between "the purposes and framework" of surveillance authorities and factual information specific to individual persons or operations. While sensitive operational details regarding the conduct of government surveillance programs should remain classified, and while legal interpretations of the application of a statute in a particular case may also be secret so long as the use of that technique in a particular case is secret, the government's interpretations of statutes that provide the basis for ongoing surveillance programs affecting Americans can and should be made public. This includes intended uses of broadly worded authorities at the time of enactment as well as post-enactment novel interpretations of laws already on the books.

**Part 10:
CONCLUSION**

Our nation is protected by men and women devoted to the rule of law. In talking to dozens of career employees throughout the intelligence agencies, we found widespread dedication to the Constitution and eagerness to comply with whatever rules are laid down by Congress and the judiciary. We are grateful to the employees of the intelligence community for their cooperation with this study, and for working tirelessly to keep us safe. None of the comments in this Report should be read in any way as a criticism of their integrity. We hope that this Report is viewed as a contribution to our shared mission of protecting America from terrorism while also preserving “the precious liberties that are vital to our way of life.”⁶⁸⁸

⁶⁸⁸ National Security Intelligence Reform Act, § 1061(b)(1), as amended by Pub. L. 110-53, section 801 (2007) (codified at 42 U.S.C. § 2000ee(b)).

ANNEX A

Separate Statement by Board Member Rachel Brand

I commend the Board and our tiny staff for putting together this comprehensive Report while simultaneously struggling to establish our still-infant agency. Although I disagree with much of the Report's discussion and some of its recommendations, this may be the most thorough description and analysis of the Section 215 bulk telephony metadata collection program ("Section 215 program") that has been published to date.

I concur in most of the Board's recommendations, and I am pleased that we were able to achieve unanimity on so many of them. However, I write separately to briefly note several points on which I disagree with the Report. Most importantly, I dissent from the Board's recommendation to shut down the Section 215 program without establishing an adequate alternative.

Where I agree with the Board's Report

I join the Board's proposal to create a process for appointing an independent advocate to provide views to the Foreign Intelligence Surveillance Court ("FISC") in important or novel matters. (Recommendations 3-5.) Although I believe the FISC already operates with the same integrity and independence as other federal courts, I agree with the Board that some involvement by an independent third party will bolster public confidence in the FISC's integrity and strengthen its important role.

Of course, the devil is in the details. Meddling in a system that already works well is risky. Any proposal to change the FISC's operations must, among other things, ensure that the FISC can continue to operate very quickly; not jeopardize the security of the sensitive materials reviewed by the court; provide adequate resources to account for an increased burden on the court; and allow the FISC's judges to retain discretion and control over the participation of an independent advocate in any given case. I believe this Board's recommendations account for all of these considerations better than any of the other proposals that have been offered.

I also sign on to most of the Board's recommendations to provide greater transparency about the government's counterterrorism programs. (Recommendations 6-11.) I agree with the Board that additional transparency, where possible, promotes public confidence in our national security agencies. However, it is important to note that the Board recommends that transparency measures be adopted *to the extent consistent with national security*. It is this qualification that enables me to sign on to the core of those recommendations. I suspect I have a different view than some of my colleagues about how

to implement each of the recommendations, but those details will be worked out in the future.

I do not sign on to the Board's discussion concerning Recommendation 12, because I do not believe that an intelligence program or legal justification for it must necessarily be known to the public to be legitimate or lawful.

Finally, I join the Board's recommendations for immediately modifying the Section 215 program (Recommendation 2) because I believe these changes will ameliorate privacy concerns while preserving the operational value of the program.

Where I disagree with the Board's Report

I cannot sign on to the substance of much of the Board's analysis. I am concerned that the Report gives insufficient weight to the need for a proactive approach to combating terrorism, and I hope that the Report will not contribute to what has aptly been described as cycles of "timidity and aggression" in the government's approach to national security.⁶⁸⁹ After September 11, 2001, the public demanded to know why the government had not stopped those attacks. Fingers were pointed in every direction, and civil liberties and privacy considerations took a backseat in the public debate immediately following the attacks. Of course, the legal structure under which the agencies operated prior to 9/11 had been put into place in the 1970s as a reaction to the Church Committee's revelations of prior excesses and abuses by the Intelligence Community. Since the recent leaks of classified programs, the pendulum seems to be swinging sharply back in that direction. But I have no doubt that if there is another large-scale terrorist attack against the United States, the public will engage in recriminations against the Intelligence Community for failure to prevent it. These swings of the pendulum, though they may be an inevitable result of human nature, are an unfortunate way to craft national security policy, and they do a disservice to the men and women dedicated to keeping us safe from terrorism.

The primary value that this bipartisan, independent Board can provide is a reasoned, balanced approach, taking into account (as our statute requires) *both* civil liberties and national security interests. We should not overreact to the crisis or unauthorized disclosure du jour, but take a longer view.

With these background considerations in mind, I turn to my reasons for dissenting from the Board's recommendation to shut down the Section 215 program.

The Board concludes that the Section 215 program is not legally authorized. I cannot join the Board's analysis or conclusion on this point.

⁶⁸⁹ See, e.g., JACK GOLDSMITH, *THE TERROR PRESIDENCY, LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION* 163-64 (2007).

The statutory question—whether the language of Section 215 authorizes the telephony bulk metadata program—is a difficult one. But the government’s interpretation of the statute is at least a reasonable reading, made in good faith by numerous officials in two Administrations of different parties who take seriously their responsibility to protect the American people from terrorism consistent with the rule of law. Moreover, it has been upheld by many Article III judges, including over a dozen FISC judges and Judge Pauley in a thorough opinion in a regular, public proceeding in U.S. District Court.⁶⁹⁰

In light of this history, I do not believe this is a legal question on which the Board can meaningfully contribute. If we were addressing this as a matter of first impression, advising the government on whether to launch the program in the first place, we would need to grapple with this question of statutory construction. But we do not approach this question as a matter of first impression. It has been extensively briefed and considered by multiple courts over the course of several years. Some of those cases are ongoing. This *legal* question will be resolved by the courts, not by this Board, which does not have the benefit of traditional adversarial legal briefing and is not particularly well-suited to conducting *de novo* review of long-standing statutory interpretations. We are much better equipped to assess whether this program is sound as a *policy* matter and whether changes could be made to better protect Americans’ privacy and civil liberties while also protecting national security.

Because the Board also concludes that the program should be shut down as a policy matter, it seems to me unnecessary and gratuitous for the Board to effectively declare that government officials and others have been operating this program unlawfully for years. I am concerned about the detrimental effect this superfluous second-guessing can have on our national security agencies and their staff. It not only undermines national security by contributing to the unfortunate “cycles of timidity and aggression” that I mentioned earlier, but is also unfair, demoralizing, and potentially legally harmful to the individuals who carry out these programs.

Turning to the constitutionality of the Section 215 program, I agree with the Board’s ultimate conclusion that the program is constitutional under existing Supreme Court caselaw.⁶⁹¹ The Board appropriately states that government officials are entitled to rely on current law when taking action. But in speculating at great length about what might be the future trajectory of Fourth Amendment caselaw, it implicitly criticizes the government for not predicting those possible changes when deciding whether to operate the program.

⁶⁹⁰ See Memorandum & Order, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013).

⁶⁹¹ One federal judge recently reached the opposite conclusion, holding that the Section 215 program is likely unconstitutional. See Memorandum Opinion, *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013). This demonstrates that these are difficult legal questions that ultimately will be resolved by the courts.

Perhaps the Supreme Court will amend its views on the third-party doctrine or other aspects of Fourth Amendment jurisprudence in future cases. But that is beside the point in a Report addressing whether the government's actions were legal at the time they were taken and now. Surely government officials should be able to rely on valid Supreme Court precedent without being second-guessed years later by a Board musing on what legal developments might happen in the future.

Of course, the government must seriously consider whether it *should* take actions that intrude on privacy even if it *can* take them as a legal matter. Whether the Section 215 program should continue as a matter of good policy is a question squarely within the Board's core mandate and one that courts have not addressed and cannot resolve. However, I do not agree with the Board's conclusion that the program should be shut down.

Whether the program should continue boils down to whether its potential intrusion on privacy interests is outweighed by its importance to protecting national security.

Starting with the privacy question, on the one hand, any collection program on this scale gives me pause. As the Board discusses, metadata can be revealing, especially in the aggregate (though I do not agree with the Board's statement that metadata may be even "more" revealing than contents). Whenever the government possesses large amounts of information, it could theoretically be used for dangerous purposes in the wrong hands without adequate oversight. Even if there is no actual privacy violation when information is collected but never viewed, accessed, analyzed, or disseminated in any way, as is true of the overwhelming majority of data collected under the Section 215 program, collection and retention of this much data about American citizens' communications creates at least a *risk* of a serious privacy intrusion.

This is why I join the Board's recommendations for immediate modifications to the program (Recommendation 2), including eliminating the third "hop" and reducing the length of time the data is held. Based in part on the Board's lengthy discussions with government officials, I believe these changes would increase privacy protections without sacrificing the operational value of the program.

On the other hand, the government does not collect the content of any communication under this program. It does not collect any personally identifying information associated with the calls. And it does not collect cell site information that could closely pinpoint the location from which a cell phone call was made. The program is literally a system of numbers with no names attached to any of them. As such, it does not sweep in the most sensitive and revealing information about telephone communications. This seems to have gotten lost in the public debate.

In addition, the program operates within strict safeguards and limitations. The Board's Report describes these procedures, but it bears repeating just how hard it is for the government to make any use of the data collected under this program. For example, before even looking at what the database holds on a particular phone number, an NSA analyst must first be able to produce some evidence—enough to establish “reasonable, articulable suspicion” or “RAS”—that that particular phone number is connected to a specific terrorist group listed in the FISC's order. Only a handful of trained analysts are authorized to do this. Before typing the phone number into a search field, the analyst must document the “RAS” determination in writing. And if the results of the query reveal a pattern of calls that seems worth investigating further, the analyst must jump through a series of additional hoops before gathering more information about the communications or distributing that information to other agencies. As a result, only an infinitesimal percentage of the records collected are ever viewed by any human being, much less used for any further purpose.⁶⁹²

With the safeguards already in place and the additional limitations this Board recommends, I believe the *actual* intrusion on privacy interests will be small.

On the other side of the equation is the national security value of the program. The Board concludes that the program has little, if any, benefit. I cannot join this conclusion.

There is no easy way to calculate the value of this program. But the test for whether the program's potential benefits justify its continuation cannot be simply whether it has already been the key factor in thwarting a previously unknown terrorist attack. Assessing the benefit of a preventive program such as this one requires a longer-term view.

The overwhelming majority of the data collected under this program remains untouched, unviewed, and unanalyzed until its destruction. But its immediate availability *if it is needed* is the program's primary benefit. Its usefulness may not be fully realized until we face another large-scale terrorist plot against the United States or our citizens abroad. But if that happens, analysts' ability to very quickly scan historical records from multiple service providers to establish connections (or avoid wasting precious time on futile leads) could be critical in thwarting the plot.

Evidence suggests that if the data from the Section 215 program had been available prior to the attacks of September 11, 2001, it could have been instrumental in preventing

⁶⁹² As the Board discusses, there have been lapses in compliance with the program's limitations. Most of these violations have been minor and technical. A few have been significant, though apparently unintentional. Compliance problems are always a matter of concern and demonstrate the need for robust oversight. But it is important to remember that the lapses the Board mentions came to light only because the government *self-reported* violations to the FISC. Those problems were then corrected, under the supervision of the FISC. And these corrective measures and self-reporting occurred *before* these programs were publicly disclosed. That is, they were identified and fixed not because of the scrutiny brought about by an unlawful leak of classified information, but because existing oversight mechanisms worked.

those attacks.⁶⁹³ The clear implication is that this data could help the government thwart a future attack. Considering this, I cannot recommend shutting down the program without an adequate alternative in place, especially in light of what I view to be the relatively small actual intrusion on privacy interests.

That said, if an adequate alternative that imposes less risk of privacy intrusions can be identified, the government should adopt it. The President appears to believe that the government can craft an alternative that retains the important intelligence capabilities of the program but reduces privacy concerns by storing the data outside the government. Although I expect this Board to have a role in crafting any such alternative and I look forward to those discussions, I doubt I could support a solution that transfers responsibility for the data to telephone service providers. This approach would make sense only if it both served as an effective alternative and assuaged privacy concerns, but I am skeptical it would do either. Because service providers are not required to retain all telephony metadata for any particular length of time, asking the service providers to hold the data could not be an effective alternative without legislatively mandating data retention. But data retention could increase privacy concerns by making the data available for a wide range of purposes other than national security, and would raise a host of questions about the legal status and handling of the data and the role and liabilities of the providers holding it. In my view, it would be wiser to leave the program as it is with the NSA than to transfer it to a third party.

Whatever happens to the Section 215 program in the short term, the government should frequently assess whether it continues to provide the potential benefits it is currently believed to have, including whether the incremental benefit provided by the program is eroded by the development of additional investigative tools. This process of re-evaluation should not consist merely of ad hoc conversations among individuals involved in the programs, but should be formalized, conducted at regular intervals with involvement by this Board, approved by officials at the highest levels of the Executive Branch, and briefed to the Intelligence and Judiciary Committees. I look forward to working with the intelligence agencies in conducting this analysis.

⁶⁹³ See, e.g., *Oversight of the Federal Bureau of Investigation: Hearing before the H. Comm. on the Judiciary, 113th Cong. 25-26 (2013)* (statement of Robert S. Mueller III, Director, Federal Bureau of Investigation) (testifying that if the data from the Section 215 program had been available to investigators before 9/11, it would have provided an “opportunity” to prevent those attacks); Decl. of Teresa H. Shea, Signals Intelligence Director, Nat’l Sec. Agency, ¶ 35, Dkt. 63, in *Am. Civil Liberties Union v. Clapper*, *supra* note 2; Michael Morell, *Correcting the Record on the NSA Review*, WASH. POST, Dec. 27, 2013 (had data from the Section 215 program been available at the time, “it would likely have prevented 9/11”).

ANNEX B**Separate Statement by Board Member Elisebeth Collins Cook**

I appreciate the thorough work of my colleagues, as well as the staff, and agree with almost all of the recommendations of the Report. I think it bodes well for the future effectiveness of the Board that we are virtually unanimous as to the policy-based recommendations reflected in the Report, and I urge that serious consideration be given to each of recommendations two through eleven. I agree that to date the Executive Branch has failed to demonstrate that the program, as currently designed, justifies its potential risks to privacy, and for that reason I join the recommendations to immediately modify its operation. I also agree with the Board that modifications to the operations of the Foreign Intelligence Surveillance Court (“FISC”) and an increased emphasis on transparency are warranted—to the extent such changes are implemented in a way that would not harm our national security efforts.

I must part ways with the Report, however, as to several points. First, although I believe the Section 215 program should be modified, I do not believe it lacks statutory authorization or must be shut down. Second, I do not agree with the Board’s constitutional analysis of the program, as it is concerned primarily with potential evolution in the law, and the potential risks from programs that do not exist. Third, I write separately to emphasize that our transparency and FISC recommendations must be implemented in a way that is fully cognizant of their potential impact on national security. Finally, I disagree with the Board’s analysis of the efficacy of the program.

Fundamentally, I believe that the Board has erred in its approach to this program, which has been (a) authorized by no fewer than fifteen Article III judges, (b) subject to extensive Executive branch oversight, and (c) appropriately briefed to Congress. The Board has been unanimous that as a policy matter the Program can and should be modified prospectively, including by limiting the analysis the National Security Agency (“NSA”) could do with the records and the amount of time NSA could keep the records. The Board has nonetheless engaged in a lengthy and time-consuming retrospective legal analysis of the Program prior to issuing those recommendations. I am concerned that this type of backward-looking analysis, undertaken years after the fact, will impact the willingness and ability of our Intelligence Community to take the proactive, preventative measures that today’s threats require. And there is no doubt that should the Intelligence Community fail to take those proactive, preventative measures, it will be blamed in the event of an attack.⁶⁹⁴

⁶⁹⁴ By the same token, having undertaken this legal analysis, I do not understand the Board’s apparent recommendation that the program it considers unauthorized continue for some interim period of time.

First, based on my own review of the statutory authorization, I conclude that the Section 215 program fits within a permissible reading of the Foreign Intelligence Surveillance Act business records provision.⁶⁹⁵ I am not persuaded that the reading of the statute advanced by the government and accepted by the Foreign Intelligence Surveillance Court⁶⁹⁶ and Judge Pauley of the United States District Court for the Southern District of New York⁶⁹⁷ is the only reading of Section 215, but I am persuaded that it is a reasonable and permissible one. Perhaps as important, I think the program itself represented a good faith effort to subject a potentially controversial program to both judicial and legislative oversight and should be commended. Moreover, the program has been conducted pursuant to extensive safeguards and oversight. When mistakes were discovered (and mistakes will occur at any organization the size of the National Security Agency), they were self-reported to the court and briefed to appropriate congressional committees; corrective measures were implemented, and the program reauthorized by the FISC.⁶⁹⁸

Second, the Board has engaged in an extensive discussion of emerging concepts of Fourth Amendment jurisprudence, none of which I join. Our conclusion that the program does not violate the Fourth Amendment is unanimous, as it should be: *Smith v. Maryland* is the law of the land.⁶⁹⁹ The government is entitled to rely on that decision, and the judges of the FISC (and our federal district and circuit courts) are required to do so, unless and until it is reversed. Analysis of whether, when, or how the Supreme Court may revisit that decision and its application is inherently speculative and unnecessary to the Board's report.

Nor do I join the Board's First Amendment analysis (which also informs the balancing/policy section). The First Amendment implications the Board finds compelling arise not from the Section 215 program but from perceived risks from a potential program that does not exist. Although the Board focuses on the "complete" pictures the NSA could paint of each and every American in concluding that it has a significant chilling effect, that is not an accurate description of the Section 215 program. The information the NSA receives *does not include the identity of the subscribers*. As the Board's Report acknowledges, a number is paired with its subscriber information (in other words,

⁶⁹⁵ See Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861).

⁶⁹⁶ See, e.g., Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 06-05 (FISA Ct. May 24, 2006); Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013).

⁶⁹⁷ See Memorandum & Order, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013).

⁶⁹⁸ See, e.g., Primary Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 09-13 (FISA Ct. Sept. 3, 2009).

⁶⁹⁹ *Smith v. Maryland*, 442 U.S. 735 (1979).

information that would allow the NSA or other agency to identify the person associated with the number) only after a determination is made that there is a reasonable, articulable suspicion that a number queried through the database is associated with one of the terrorist organizations identified in the FISC's orders. For a telephone number reasonably believed to be used by a U.S. person, the reasonable articulable suspicion standard cannot be met solely on the basis of activities protected by the First Amendment. Any investigative steps related to that number can be taken only after a determination that the number associated with its subscriber information has potential counterterrorism value. There is no disagreement that this process is applied to only an extraordinarily small percentage of the numbers in the database, yet the Board Report's balancing/policy and First Amendment analyses proceed as if each and every number of every American is systematically paired with its subscriber information and analyzed in great detail.

In addition, the Board nowhere meaningfully grapples with two key questions. One, what is the *marginal* constitutional and policy impact of the Section 215 program, particularly in view of the Board's assertion that essentially everything the Section 215 program is designed to accomplish can be accomplished through other existing national security and law enforcement tools? Two, is there a difference as a policy and constitutional matter between an order or program that is designed by its very terms to force disclosure of each and every individual's protected activities (such as the disclosure requirement addressed in *NAACP v. Alabama*⁷⁰⁰), and a program such as the one under consideration today, in which information is *collected* about innumerable individuals, but human eyes are laid on less than .0001% of individuals' information? To the Board, there is no apparent constitutional or policy difference between mere collection of information and actually accessing and using that information. I do not agree.

Third, I agree with the Report's recommendations as to transparency (except recommendation twelve) and the operations of the FISC, both sets of which are designed to foster increased confidence in the government's national security efforts. I also understand that each of our recommendations is to be implemented with full consideration of the potential impact on our national security, and without hindering the operations of the FISC. As to transparency, we have always understood that not everything can be publicly discussed, *see, e.g.*, U.S. Const. Art. I § 5, cl. 3. ("Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy"), as we would like to avoid providing our adversaries with a roadmap to evade detection. The rational alternative, which occurred here, is to brief the relevant committees and members of Congress, seek judicial authorization, and subject a program to extensive executive branch oversight. In a representative democracy such as

⁷⁰⁰ *NAACP v. Alabama*, 357 U.S. 449 (1958).

ours, it is simply not the case that a particular use or related understanding of a statutory authorization is illegitimate unless it has been explicitly debated in an open forum.

Finally, I have a different view from the Board as to the efficacy and utility of the Section 215 program. Although the Report purports to consider whether the program might be valuable for reasons other than preventing a specific terrorist attack, the tone and focus of the Report make clear that the Board does believe that to be the most important (and possibly the only) metric. I consider this conclusion to be unduly narrow. Among other things, in today's world of multiple threats, a tool that allows investigators to triage and focus on those who are more likely to be doing harm to or in the United States is both good policy and potentially privacy-protective. Similarly, a tool that allows investigators to more fully understand our adversaries in a relatively nimble way, allows investigators to verify and reinforce intelligence gathered from other programs or tools, and provides "peace of mind," has value.

I would, however, recommend that the NSA and other members of the Intelligence Community develop metrics for assessing the efficacy and value of intelligence programs, particularly in relation to other tools and programs. The natural tendency is to focus on the operation of a given program, without periodic reevaluations of its value or whether it could be implemented in more privacy-protective ways. Moreover, the natural tendency of the government, the media, and the public is to ask whether a particular program has allowed officials to thwart terrorist attacks or save identifiable lives. Periodic assessments would not only encourage the Intelligence Community to continue to explore more privacy-protective alternatives, but also allow the government to explain the relative value of programs in more comprehensive terms. I hope that our Board will have the opportunity to work with the Intelligence Community on such an effort.

* * * * *

In many ways, the evaluation of this long-running program was the most difficult first test this Board could have faced. Unfortunately, rather than focusing on whether the program strikes the appropriate balance between the necessity for the program and its potential impacts on privacy and civil liberties, and moving immediately to recommend corrections to any imbalance, the Board has taken an extended period of time to analyze (a) statutory questions that are currently being litigated, and (b) somewhat academic questions of how the Fourth Amendment might be applied in the future and the First Amendment implications of programs that do not presently exist. I believe that with

respect to this longstanding program, the highest and best use of our very limited resources⁷⁰¹ is instead found in our unanimous recommendations.

The development of a modified approach to the very difficult questions raised by the government's non-particularized collection of data presents an ideal opportunity for the Board to fulfill its statutory advisory and oversight role. In this regard, I would note that some frequently mentioned alternatives pose numerous potential difficulties in their own right. For example, some have suggested that the NSA could essentially request that the telephone companies run the queries, rather than collecting and retaining records for querying. However, even assuming the companies currently keep the relevant records, there is no guarantee that those records will continue to be retained in the future. By the same token, if another terrorist attack happens, the pressure will be immense to impose data retention requirements on those companies, which would pose separate and perhaps greater privacy concerns. Finally, it is not at all clear how a third party entity to hold the data could be structured in a way that would (a) be an adequate substitute for the Section 215 program and (b) preserve the security of those records, while (c) ameliorating the perceived privacy concerns raised by that program.

There is much to consider in the near future, and I look forward to working with my colleagues on these important issues.

⁷⁰¹ Although many agencies claim to lack adequate resources, the situation of the PCLOB is particularly remarkable. The agency currently has a full-time Chairman, four part-time Members limited to 60 days of work per year, and two permanent staff members. The decision to engage in such an extended discussion of largely hypothetical legal issues was therefore not without practical consequences: the Board has delayed consideration of the 702 program, and has not addressed any of the other issues previously identified by the Board as meriting oversight. Moreover, the decision of three Members of the Board to allocate the entirety of the permanent staff's time to the drafting of the Board Report, while simultaneously drafting and refining that Report until it went to the printer, has made a comparably voluminous response impossible.

ANNEX C

AGENDA OF PUBLIC WORKSHOP

HELD ON JULY 9, 2013

Link to Workshop transcript:

<http://www.pclob.gov/All%20Documents/July%209,%202013%20Workshop%20Transcript.pdf>



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act

July 9, 2013

**Renaissance Mayflower Hotel – Grand Ballroom
1127 Connecticut Ave NW, Washington D.C.**

AGENDA

09:00 Doors Open

09:30 – 09:45 Introductory Remarks (David Medine, PCLOB Chairman)

**09:45 – 11:30 Panel I: Legal/Constitutional Perspective
Facilitators: Rachel Brand and Patricia Wald, Board Members**

Panel Members:

- **Steven Bradbury (Formerly DOJ Office of Legal Counsel)**
- **Jameel Jaffer (ACLU)**
- **Kate Martin (Center for National Security Studies)**
- **Hon. James Robertson, Ret. (formerly District Court and Foreign Intelligence Surveillance Court)**
- **Kenneth Wainstein (formerly DOJ National Security Division/ White House Homeland Security Advisor)**

**12:30 – 2:00 Panel II: Role of Technology
Facilitators: James Dempsey and David Medine, Board Members
Panel Members:**

- **Steven Bellovin (Columbia University Computer Science Department)**
- **Marc Rotenberg (Electronic Privacy Information Center)**

- **Ashkan Soltani (Independent Researcher and Consultant)**
- **Daniel Weitzner (MIT Computer Science and Artificial Intelligence Lab)**

2:00 – 2:15 Break

**2:15 – 4:00 Panel III: Policy Perspective
Facilitators: Elisebeth Collins Cook and David Medine, Board
Members**

Panel Members:

- **James Baker (formerly DOJ Office of Intelligence and Policy Review)**
- **Michael Davidson (formerly Senate Legal Counsel)**
- **Sharon Bradford Franklin (The Constitution Project)**
- **Elizabeth Goitein (Brennan Center for Justice)**
- **Greg Nojeim (Center for Democracy and Technology)**
- **Nathan Sales (George Mason School of Law)**

4:00 – 4:10 Break

4:10 – 4:30 Open for Public Comment

4:30 Closing Comments (David Medine, PCLOB Chairman)

**Affiliations are listed for identification purposes only.*

ANNEX D

AGENDA OF PUBLIC HEARING

HELD ON NOVEMBER 4, 2013

Link to Hearing transcript:

<http://www.pclob.gov/SiteAssets/PCLOB%20Hearing%20-%20Full%20Day%20transcript%20Nov%204%202013.pdf>



**PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
PUBLIC HEARING**

***Consideration of Recommendations for Change:
The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act
and Section 702 of the Foreign Intelligence Surveillance Act
November 4, 2013***

**Renaissance Mayflower Hotel – Grand Ballroom
1127 Connecticut Ave NW, Washington D.C.**

AGENDA

- 08:45 Doors Open**
- 09:15 – 09:30 Introductory Remarks (David Medine, PCLOB Chairman, with Board
Members
Rachel Brand, Elisebeth Collins Cook, James Dempsey, and Patricia
Wald)**
- 09:30 – 11:45 Panel I: Section 215 USA PATRIOT Act and Section 702 Foreign
Intelligence
Surveillance Act**
- **Rajesh De (General Counsel, National Security Agency)**
 - **Patrick Kelley (Acting General Counsel, Federal Bureau of
Investigation)**
 - **Robert Litt (General Counsel, Office of the Director of National
Intelligence)**
 - **Brad Wiegmann (Deputy Assistant Attorney General, National
Security Division, Department of Justice)**
- 11:45 – 1:15 Lunch Break (on your own)**

- 1:15 – 2:30 Panel II: Foreign Intelligence Surveillance Court**
- **James A. Baker (formerly DOJ Office of Intelligence and Policy Review)**
 - **Judge James Carr (Senior Federal Judge, U.S. District Court, Northern District of Ohio and former FISA Court Judge 2002-2008)**
 - **Marc Zwillinger (Founder, ZwillGen PLLC and former Department of Justice Attorney, Computer Crime & Intellectual Property Section)**
- 2:30 – 2:45 Break**
- 2:45 – 4:15 Panel III: Academics and Outside Experts**
- **Jane Harman (Director, President and CEO, The Woodrow Wilson Center and former Member of Congress)**
 - **Orin Kerr (Fred C. Stevenson Research Professor, George Washington University Law School)**
 - **Stephanie K. Pell (Principal, SKP Strategies, LLC; former House Judiciary Committee Counsel and Federal Prosecutor)**
 - **Eugene Spafford (Professor of Computer Science and Executive Director, Center for Education and Research in Information Assurance and Security, Perdue University)**
 - **Stephen Vladeck (Professor of Law and the Associate Dean for Scholarship at American University Washington College of Law)**
- 4:15 Closing Comments (David Medine, PLCOB Chairman)**

All Affiliations are listed for identification purposes only.

ANNEX E

Request for Public Comments on Board Study

The Federal Register

The Daily Journal of the United States Government

56952 Federal Register/Vol. 78, No. 179/Monday, September 16, 2013/Notices
PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

[Notice-PCLOB-2013-06; Docket No. 2013- 0005; Sequence No. 6]

Notice of Hearing

A Notice by the Privacy and Civil Liberties Oversight Board on 10/25/2013

Action

Notice Of A Hearing.

Summary

The Privacy and Civil Liberties Oversight Board (PCLOB) will conduct a public hearing with current and former government officials and others to address the activities and responsibilities of the executive and judicial branches of the federal government regarding the government's counterterrorism surveillance programs. This hearing will continue the PCLOB's study of the federal government's surveillance programs operated pursuant to Section 215 of the USA PATRIOT Act and Section 702 of Foreign Intelligence Surveillance Act. Recommendations for changes to these programs and the operations of the Foreign Intelligence Surveillance Court will be considered at the hearing to ensure that counterterrorism efforts properly balance the need to protect privacy and civil liberties. Visit www.pcllob.gov for the full agenda closer to the hearing date. This hearing was re-scheduled from October 4, 2013, due to the unavailability of witnesses as a result of the federal lapse in appropriations.

DATES:

Monday, November 4, 2013; 9:00 a.m.-4:30 p.m. (Eastern Standard Time).

Comments:

You may submit comments with the docket number PCLOB-2013-0005; Sequence 7 by the following method:

- *Federal eRulemaking Portal*: Go to <http://www.regulations.gov>. Follow the on-line instructions for submitting comments.
- Written comments may be submitted at any time prior to the closing of the docket at 11:59 p.m. Eastern Time on November 14, 2013. This comment period has been extended from October 25, 2013, as a result of the new hearing date.

All comments will be made publicly available and posted without change. Do not include personal or confidential information.

ADDRESSES:

Mayflower Renaissance Hotel Washington, 1127 Connecticut Ave. NW., Washington D.C. 20036. Facility's location is near Farragut North Metro station.

FOR FURTHER INFORMATION CONTACT:

Susan Reingold, Chief Administrative Officer, 202-331-1986. For email inquiries, please email info@pclub.gov.

SUPPLEMENTARY INFORMATION:

Procedures for Public Participation

The hearing will be open to the public. Individuals who plan to attend and require special assistance, such as sign language interpretation or other reasonable accommodations, should contact Susan Reingold, Chief Administrative Officer, 202-331-1986, at least 72 hours prior to the meeting date.

Dated: October 21, 2013.

Diane Janosek,
Chief Legal Officer, Privacy and Civil Liberties Oversight Board.

<https://www.federalregister.gov/articles/2013/10/25/2013-25103/notice-of-hearing>

ANNEX F

Index to Public Comments received to PCLOB Docket No. 2013-005 on www.regulations.gov.

Comments Received on PCLOB Docket No. 2013-005

Can also view all entries at: <http://www.regulations.gov/#!docketDetail;D=PCLOB-2013-0005>

Entity submitting comment - listed in order as they appear on docket	Go to URL to see comment on Docket	Additional details:
Global Network Initiative (GNI)	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0027	GNI is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics
Private individual	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0044	
Nathan Sales	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0022	Panel member at PCLOB Workshop
European Digital Rights (EDRi) and the Fundamental Rights European Experts Group (FREE)	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0024	EDRi is an association of 35 digital civil rights organizations from 21 European countries. FREE is an association whose focus is on monitoring, teaching and advocating in the EU.
Michael Davidson	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0020	Panel member at PCLOB Workshop

Project On Government Oversight (POGO), National Security Counselors, and OpenTheGovernment.org.	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0029	
Center for National Security Studies	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0033	Kate Martin was a panel member at PCLOB Workshop
Michael Davidson-second submission	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0028	Providing the July 30th opinion of the U.S. Court of Appeals for the Fifth Circuit in In re: Application of the United States of America for Historical Cell Site Data, No. 11-20884
Mr. Juan Fernando López Aguilar, Chair of the European Parliament's Civil Liberties, Justice and Home Affairs Committee	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0059	
Ashkan Soltani	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0023	Panel member at PCLOB Workshop
Alliance for Justice	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0035	
Alan Charles Raul	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0065	Has four attachments
"Three former intelligence professionals - all former employees of the National Security Agency"	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0053	Statement submitted

Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0014	
Coalition of 53 groups- letter	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0038	This is an updated coalition letter to PCLOB
The Constitution Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0009	Sharon Bradford Franklin was a panel member at PCLOB Workshop
Computer and Communications Industry Association	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0025	
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0017	
Electronic Frontier Foundation	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0030	
-BSA -The Software Alliance Computer & Communications Industry Association (CCIA) -Information Technology Industry Council (ITI) - SIIA (Software & Information Industry Association) - TechNet	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0061	

Ashkan Soltani	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0039	Revised submission, was a panel member at PCLOB Workshop
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0005	
Daniel J. Weitzner, Massachusetts Institute of Technology	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0040	Panel member at PCLOB Workshop
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0052	
Access - AccessNow.org	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0048	
Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0057	
Privacy Times	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0011	
Electronic Privacy Information Center	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0064	Marc Rotenberg was a panel member at PCLOB Workshop
ACLU Statement	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0032	Jameel Jaffer was a panel member at PCLOB Workshop
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0046	
Mark Sokolow	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0046	

	ntDetail;D=PCLOB-2013-0005-0018	
GodlyGlobal.org	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0019	A faith-based initiative based in Switzerland with global scope
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0041	
ACCESS NOW	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0047	Second posting
Coalition letter	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0010	
Center for Democracy & Technology, Gregory T. Nojeim	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0034	Gregory Nojeim was a panel member at PCLOB Workshop
Reporters Committee for Freedom of the Press	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0063	
Center for National Security Studies	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0060	Kate Martin was a panel member at PCLOB Workshop
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0037	
Brennan Center for Justice's Liberty and National Security Program	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0049	Elizabeth Goitein was a panel member at PCLOB Workshop
Jeffrey H. Collins	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0049	

	ntDetail;D=PCLOB-2013-0005-0043	
Jeffrey H. Collins	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0045	Amended
Steven G. Bradbury	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0012	Panel member at PCLOB Workshop
Human Rights Watch	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0036	
“Human rights organizations and advocates from around the world”	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0042	Dozens of countries represented
Steven M. Bellovin	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0021	Panel member at PCLOB Workshop
Board of the U.S. Public Policy Council of the Association for Computing Machinery	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0026	Eugene H. Spafford, was a panelist at the Hearing
Private citizen	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0066	
Caspar Bowden, Prepared for the European Parliament LIBE Committee	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0068	
Stephanie Pell	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0068	Panel member at hearing

	ntDetail;D=PCLOB-2013-0005-0069	
Congressman Bennie Thompson	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0071	Ranking Member, Committee on Homeland Security
Government Accountability Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0072	

This Report is the Privacy and Civil Liberties Oversight Board's effort to analyze and review actions the executive branch takes to protect the Nation from terrorism to ensure the proper balancing of these actions with privacy and civil liberties.