TESTIMONY OF STEVEN G. BRADBURY

Before the
HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

Open Hearing on Legislative Proposals for Modifying NSA Programs and Amending FISA Authorities

October 29, 2013

Thank you, Chairman Rogers, Ranking Member Ruppersberger, and distinguished Members of the Committee.

I'm honored to appear before the Committee today to discuss the foreign intelligence acquisition and surveillance authorities of the executive branch—with particular focus on the recently revealed programs of the National Security Agency ("NSA")—and to offer views on several proposals currently under consideration in Congress for modifying or curtailing the NSA's programs and for amending key provisions of the Foreign Intelligence Surveillance Act, or "FISA."[1]

Summary

Any debate over proposals to restrict the NSA activities revealed by the Snowden leaks or to make significant amendments to FISA in response to those leaks should carefully consider whether the foreign intelligence programs that would be affected by the proposals are lawful and whether they continue to be necessary.

If the NSA programs are lawful and if, in the estimation of this Committee, they remain necessary to protect the Nation from foreign threats, then Congress should be very wary indeed about approving any legislative changes that might undermine the effectiveness of the programs or that might diminish the ample

[1] The author is an attorney in Washington, D.C., and the former head of the Office of Legal Counsel in the U.S. Department of Justice from 2005 to 2009, where he advised the executive branch on legal matters relating to national security, including surveillance authorities under FISA. The views presented are solely the personal views of the author and do not represent the views of his law firm or of any current or former client.

existing security measures, privacy protections, and oversight protocols under which they operate.

Based on that premise, I wish to emphasize the following three points:

First, there is no serious argument that the NSA programs as currently configured violate any applicable statutory or constitutional restrictions.

The independent federal judges who sit on the FISA court have repeatedly scrutinized these programs over the past several years and ensured that they comply in all respects with the requirements of FISA and are fully consistent with the Fourth and First Amendments of the Constitution. A review of the FISA court opinions recently declassified and released to the public amply demonstrates that the FISA court is no rubber stamp for the surveillance policies of the executive branch.

The judges of the FISA court, as well as the attorneys of the National Security Division of the Justice Department, the Inspectors General of the Intelligence Community and the Justice Department, and the diligent oversight of the Intelligence Committees of Congress, have held the NSA to the highest standards possible in the operations of these programs, including by ordering the prompt correction of significant compliance issues identified to the court by the Agency and its overseers.

The FISA court's decisions confirm that both the bulk telephone metadata acquisition and focused analysis currently occurring under the business records provision of FISA (commonly known as section 215 of the PATRIOT Act) and the broad foreign-targeted surveillance of international communications conducted under section 702 of FISA comply in all respects with the Constitution and the terms of the relevant statutes and are consistent with the intent of Congress.

Indeed, I understand that all Members of Congress, specifically including the Judiciary Committees, were informed about the details of these two NSA programs or were at least given the opportunity to receive such briefings in connection with the reauthorizations of sections 215 and 702. The large majorities of both Houses that voted to reauthorize these statutes in 2011 and 2012 therefore represented, at least constructively, a clear approval and ratification of the legal

interpretations supporting the NSA's collection and surveillance activities, including the bulk acquisition of telephone metadata. Any claim in recent months of lack of prior awareness and understanding of these programs in reaction to the public controversy generated by the Snowden leaks should be taken with a truckload of salt.

Second, I accept the judgment of the President, the Director of National Intelligence ("DNI"), and Gen. Alexander, the Director of the NSA, that the NSA programs revealed by Snowden are critically important to preserving the security of the United States and its allies and that these programs continue to make an essential contribution to our counterterrorism defenses. From everything I know, these programs are, as they were designed to be, among the most effective tools for detecting and identifying connections between foreign terrorist organizations and active cells within the United States and for discovering new leads, including new phone numbers, in furtherance of counterterrorism investigations.

If that's true, it is, of course, primarily the duty of the President to stand up and defend the programs before the American people and Congress. But as an important supplement to presidential leadership, or in the absence of such leadership, it is incumbent on this Committee and the Intelligence Committee of the Senate to validate the necessity and effectiveness of these programs and to educate and persuade a majority of colleagues in both Houses of the need to support and preserve these essential foreign intelligence capabilities in the face of popular reaction. The national interest must trump narrow political interests.

Third, it is my conviction that all of the major proposals under consideration in Congress for curtailing, restricting, or modifying the NSA programs (most especially the section 215 telephone metadata program) and for reforming the scope and use of FISA authorities in reaction to the Snowden leaks should be rejected.

As discussed in more detail below, certain proposals would expose the Nation to vulnerability by substantially weakening or even destroying outright the effectiveness of the 215 program. Other proposals would significantly diminish the ability of the government to ensure the security and oversight of the program. Still others would unnecessarily hamper foreign intelligence efforts by adding layers of lawyering or litigation-like process that would not actually achieve

greater civil liberties protections for the public but that would, I fear, prove dangerously unworkable in the event of the next catastrophic attack on the United States.

I therefore strongly urge the Committee to avoid endorsing proposals for substantial modification of the NSA programs or FISA provisions. If reforms are adopted that would severely constrain the effectiveness and utility of the NSA programs, then Edward Snowden and his collaborators will have achieved their explicit objective of weakening the national security defenses and capabilities of the United States and diminishing the position of strength that America occupies in the world post-9/11.

The NSA Programs Satisfy All Statutory and Constitutional Requirements

I have previously explained in detail why both the section 215 bulk acquisition of telephone metadata and the section 702 foreign-targeted surveillance of international communications are authorized by statute, consistent with the Constitution and congressional intent, and appropriately protective of privacy and civil liberties.[2] I will not repeat the full analysis here, but I do offer the following brief summary.

Section 215 Telephone Metadata Program.

The telephone metadata acquired by the NSA under the section 215 business records order consists only of tables of numbers indicating which phone numbers called which numbers and the time and duration of the calls. It does not reveal any other subscriber information, and it does not enable the government to listen to anyone's phone calls.

The Fourth Amendment does not require a search warrant or other individualized court order for the government to acquire this type of purely transactional metadata, as distinct from the content of communications. The acquisition of such call-detail information, either in bulk or for the

[2] *See* Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata under Section 215 and Foreign-Targeted Collection under Section 702*, 1 Lawfare Res. Paper Series No. 3 (Sept. 2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf.

communications of identified individuals, does not constitute a "search" for Fourth Amendment purposes with respect to the individuals whose calls are detailed in the records. The information is voluntarily made available to the phone company to complete the call and for billing purposes, and courts have therefore consistently held that there is no reasonable expectation by the individuals making the calls that this information will remain private. *See Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).[3]

The force of this conclusion is not diminished by the large size of the data set being acquired by the NSA. Indeed, the individual privacy interests of the tens of millions of telephone customers whose calling records are collected by the NSA are lessened even further because of the vastness and anonymity of the data set.

This acquisition is authorized under the terms of section 215, which permits the acquisition of business records that are "relevant to an authorized investigation." Here, the telephone metadata is "relevant" to counterterrorism investigations because the use of the database is essential to conduct a link analysis of terrorist phone numbers, and this type of analysis is a critical building block in these investigations. Acquiring a comprehensive database is needed to enable effective analysis of the telephone links and calling patterns of terrorist suspects, which is often the only way to discover new phone numbers being used by terrorists. To "connect the dots" effectively requires the broadest set of telephone metadata.

The legal standard of relevance incorporated into section 215 is the same common standard that courts have long held governs the enforcement of administrative subpoenas, grand jury subpoenas, and document production orders in civil litigation, which, unlike section 215 business records orders, do not require the advance approval of a court.[4]

---

[3] *Accord Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904-05 (9th Cir. 2008) (same analysis for email addressing information).

[4] *See* 152 Cong. Rec. 2426 (2006) (Statement of Sen. Kyl) (explaining the "relevant to" language added to section 215 in 2006) ("Relevance is a simple and well established standard of law. Indeed, it is the standard for obtaining every other kind of subpoena, including administrative subpoenas, grand jury subpoenas, and civil discovery orders.").

The Supreme Court has long held that courts must enforce administrative subpoenas so long as the agency can show that the subpoena was issued for a lawfully authorized purpose and seeks information relevant to the agency's inquiry.[5] This standard of relevance is exceedingly broad; it permits agencies to obtain "access to virtually any material that might cast light on" the matters under inquiry,[6] and to subpoena records "of even *potential* relevance to an ongoing investigation."[7] Grand jury subpoenas are given equally broad scope and may only be quashed where "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."[8] And in civil discovery, the concept of relevance is applied "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."[9]

The relevance standard does not require a separate showing that every individual record in a subpoenaed database is "relevant" to the investigation.[10] The standard is satisfied if there is good reason to believe that the database contains information pertinent to the investigation and if, as here, the acquisition of the database is needed to preserve the data and to be able to conduct focused queries to find particular records useful to the investigation.[11]

---

[5] *See United States v. LaSalle Nat'l Bank*, 437 U.S. 298, 313 (1978); *United States v. Powell*, 379 U.S. 48, 57 (1964); *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 209 (1946).

[6] *EEOC v. Shell Oil Co.*, 466 U.S. 54, 68-69 (1984).

[7] *United States v. Arthur Young & Co.*, 465 U.S. 805, 814 (1984) (emphasis in original).

[8] *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).

[9] *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978).

[10] *See In re Grand Jury Proceedings*, 616 F.3d 1186, 1202, 1205 (10th Cir. 2010) (confirming (1) that the categorical approach to relevance for grand jury subpoenas "contemplates that the district court will assess relevancy based on the broad types of material sought" and will not "engag[e] in a document-by-document" or "line-by-line assessment of relevancy," and (2) that "[i]ncidental production of irrelevant documents . . . is simply a necessary consequence of the grand jury's broad investigative powers and the categorical approach to relevancy").

[11] *See, e.g., In re Subpoena Duces Tecum*, 228 F.3d 341, 350-51 (4th Cir. 2000); *FTC v. Invention Submission Corp.*, 965 F.2d 1086 (D.C. Cir. 1992); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987); *Associated Container Transp. (Aus.) Ltd. v. United States*, 705 F.2d 53, 58 (2d Cir. 1983). The same approach is sanctioned in the federal rules governing criminal search warrants. *See* Fed. R. Crim. P. 41(e)(2)(B) ("A warrant . . . may authorize the

The effective analysis of terrorist calling connections and the discovery through that analysis of new phone numbers being used by terrorist suspects require the NSA to assemble and maintain the most comprehensive set of telephone metadata, and the section 215 order provides that unique capability.

While the metadata order is extraordinary in the amount of data acquired, it's also extraordinarily narrow and focused because of the strict limitations placed on accessing the data. There's no data mining or trolling through the database looking for suspicious patterns. By court order, the data can only be accessed when the government has reasonable suspicion that a particular phone number is associated with a foreign terrorist organization, and then that number is tested against the database to discover its connections. If it appears to be a U.S. number, the necessary suspicion cannot be based solely on First Amendment-protected activity.

Because of this limited focus, only a tiny fraction of the total data has ever been reviewed by analysts. The database is kept segregated and is not accessed for any other purpose, and FISA requires the government to follow procedures overseen by the court to minimize any unnecessary dissemination of U.S. numbers. Any data records older than five years are continually deleted from the system.

The order must be reviewed and reapproved every 90 days, and since 2006, this metadata order has been approved at least 35 times by at least 15 different federal judges.

In addition to court approval, the 215 program is also subject to oversight by the executive branch and Congress. FISA mandates periodic audits by inspectors general and reporting to the Intelligence and Judiciary Committees of Congress. When section 215 was reauthorized in 2011, the administration briefed the leaders of Congress and the members of these Committees on the details of this program. The administration also provided detailed written descriptions of the program to

---

seizure of electronic storage media or . . . information" subject to "a later review of the media or information consistent with the warrant"); *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006) (sanctioning "blanket seizure" of computer system based on showing of need); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (sanctioning "seizure and subsequent off-premises search" of computer database).

the chairs of the Intelligence Committees, and the administration requested that those descriptions be made available to all Members of Congress in connection with the renewal of section 215.

These briefing documents specifically included the disclosure that under this program, the NSA acquires the call-detail metadata for "substantially all of the telephone calls handled by the [phone] companies, including both calls made between the United States and a foreign country and calls made entirely within the United States."[12] Public reports indicate that the Intelligence Committees provided briefings on the details of the program to all interested Members of Congress, and the administration has conducted further detailed briefings on this program since the Snowden leaks became public.

Section 702 Collection.

The second NSA program revealed by the Snowden leaks—the foreign-targeted surveillance of international communications—is conducted under section 702 of FISA.

With court approval, section 702 authorizes a program of foreign-focused surveillance for periods of one year at a time. This authority may only be used if the surveillance does ***not*** (1) intentionally target any person, of any nationality, known to be located in the United States, (2) target a person outside the U.S. if the purpose is to reverse target any particular person believed to be in the U.S., (3) intentionally target a U.S. person anywhere in the world, and (4) intentionally acquire any communication as to which the sender and all recipients are known to be in the U.S.

Section 702 mandates court approval of the targeting protocols and of minimization procedures to ensure that any information about U.S. persons that may be captured in this surveillance will not be retained or disseminated except as necessary for foreign intelligence purposes.

---

[12] Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization at 3, *enclosed with* Letters for Chairmen of House and Senate Intelligence Committees from Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, Department of Justice (Feb. 2, 2011). The identical disclosure was also made in a similar report enclosed with letters dated December 14, 2009.

From everything that's been disclosed about the foreign-targeted surveillance program, including the so-called PRISM Internet collection, it appears to be precisely what section 702 was designed to permit.

The 702 program is also fully consistent with the Constitution. As a background principle, the Fourth Amendment does not require the government to obtain a court-approved warrant supported by probable cause before conducting foreign intelligence surveillance. The Supreme Court has reserved judgment on the question,[13] but the courts of appeals have consistently held that the President has inherent constitutional authority to conduct warrantless searches and surveillance to obtain intelligence information about the activities of foreign powers, both inside and outside the United States and both in wartime and peacetime.[14]

The absence of a warrant requirement does not mean the Fourth Amendment has no application to foreign intelligence surveillance. Rather, searches and surveillance conducted in the United States by the executive branch for foreign intelligence purposes are subject to the general reasonableness standard of the Fourth Amendment. *See Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995) (holding that the touchstone for government compliance with the Fourth Amendment is whether the search is "reasonable" and recognizing that the warrant requirement is inapplicable in situations involving "special needs" that go beyond routine law enforcement).

---

[13] *See United States v. United States District Court* (the "*Keith*" case), 407 U.S. 297, 308 (1972) (explaining that the Court did not have occasion to judge "the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country"); *Katz v. United States*, 389 U.S. 347 (1967).

[14] *See, e.g.*, *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 914-15 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir.), *cert. denied*, 434 U.S. 890 (1977); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir.), *cert. denied sub nom. Ivanov v. United States*, 419 U.S. 881 (1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir.1973), *cert. denied*, 415 U.S. 960 (1974). *But see Zweibon v. Mitchell*, 516 F.2d 594, 619-20 (D.C.Cir.1975) (en banc) (plurality opinion suggesting in dicta that a warrant may be required even in a foreign intelligence investigation), *cert. denied*, 425 U.S. 944 (1976).

The reasonableness of foreign intelligence surveillance, like other "special needs" searches, is judged under a general balancing standard "by assessing, on the one hand, the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). In the context of authorized NSA surveillance directed at protecting against foreign threats to the United States, the governmental interest is of the highest order. *See 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.").

On that basis, prior to 1978, Presidents conducted surveillance of national security threats without court supervision. That practice led to the abuses that were documented by the Church and Pike Committees and eventually resulted in the passage of FISA.

FISA was enacted as an accommodation between Congress and the executive branch. It was designed to ensure the reasonableness of surveillance by requiring the approval of a federal judge for certain defined types of clandestine foreign intelligence surveillance conducted in the United States, instituting oversight of the process by the Intelligence Committees of Congress, providing for procedures to "minimize" the retention and dissemination of information about U.S. persons collected as part of foreign intelligence investigations, and regularizing procedures for the use of evidence obtained in such investigations in criminal proceedings.

Under FISA, electronic surveillance of persons in the United States for foreign intelligence purposes requires an order approved by a judge and supported by individualized probable cause to believe the target is an agent of a foreign power or engaged in international terrorism.

Ever since FISA was enacted, it's been recognized that FISA raises significant constitutional issues to the extent it might impinge on the President's ability to carry out his constitutional duty to protect the United States from foreign attack.

Importantly, in its original conception, FISA was not intended to govern the conduct of communications intelligence anywhere overseas or the NSA's collection and surveillance of international communications into and out of the United States. FISA's definition of "electronic surveillance" focuses on the interception of wire communications on facilities in the United States and on the interception of certain categories of domestic radio communications. *See* 50 U.S.C. § 1801(f). In 1978, most international calls were carried by satellite, and thus the statute's definition of "electronic surveillance" was carefully designed at the time to exclude from the jurisdiction of the FISA court not only all surveillance conducted outside the United States, but also the surveillance of nearly all international communications.[15]

FISA also exempted from statutory regulation the acquisition of intelligence information from "international or foreign communications" not involving "electronic surveillance" as defined in FISA,[16] and this change, too, was "designed to make clear that the legislation does not deal with the international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."[17] Congress specifically understood that the NSA surveillance that these carve-outs would categorically exclude from FISA included the monitoring of international communications into and out of the United States of U.S. citizens.[18]

In the years following the passage of FISA, however, communications technologies evolved in ways that Congress had not anticipated. International lines of communications that once were transmitted largely by satellite migrated to undersea fiber optic cables. This evolution increased greatly with the advent of the Internet. In the new world of packet-switched Internet communications and

---

[15] *See* S. Rep. No. 95-604, at 33-34, reprinted in 1978 U.S.C.C.A.N. 3904, 3934-36.

[16] *See* Pub. L. No. 95-511, § 201(b), (c), 92 Stat. 1783, 1797 (1978), *codified at* 18 U.S.C. § 2511(2)(f) (1982).

[17] S. Rep. No. 95-604, at 64, 1978 U.S.C.C.A.N. at 3965.

[18] *See id.* at 64 n.63 (describing the excluded NSA activities by reference to a Church Committee report, S. Rep. No. 94-755, at Book II, 308 (1976), which stated: "[T]he NSA intercepts messages passing over international lines of communication, some of which have one terminal within the United States. Traveling over these lines of communication, especially those with one terminal in the United States, are messages of Americans . . . .").

international fiber optic cables, FISA's original regime of individualized court orders for foreign intelligence surveillance conducted on facilities in the United States became cumbersome, because it now required case-by-case court approvals for the surveillance of international communications that were previously exempt from FISA coverage. Nevertheless, prior to 9/11, the executive branch found the FISA system to be adequate and workable for most national security purposes.

All of that changed with the attacks of 9/11. In the estimation of the President and the NSA, the imperative of conducting fast, flexible, and broad-scale signals intelligence of international communications in order to detect and prevent further terrorist attacks on the U.S. homeland proved to be incompatible with the traditional FISA procedures for individualized court orders and the cumbersome approval process then in place. As the Justice Department later explained in a public white paper addressing the legal basis for the NSA's warrantless surveillance of international communications involving suspected terrorists that was authorized by special order of the President following 9/11, "[t]he President ha[d] determined that the speed and agility required to carry out the[se] NSA activities successfully could not have been achieved under FISA."[19]

The public disclosures in 2005 and 2006 concerning the President's authorization of warrantless surveillance by the NSA precipitated extensive debates and hearings in Congress. Ultimately, these debates culminated in passage of the FISA Amendments Act of 2008 and the addition of section 702 to FISA. Section 702 was designed to return to a model of foreign surveillance regulation similar to the original conception of FISA by greatly streamlining the court review and approval of a program of surveillance of international communications targeted at foreign persons believed to be outside the United States. Under section 702, such foreign-targeted surveillance may be authorized by the Attorney General and DNI without individualized court orders for periods of up to one year at a time upon the approval by the FISA court of the required targeting protocols and minimization procedures. *See* 50 U.S.C. § 1881a.

By establishing procedures for court approval (albeit more streamlined and "programmatic" approval than required for traditional individualized FISA surveillance orders) and by strengthening congressional oversight of the resulting

[19] U.S. Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President 34 (Jan. 19, 2006).

program, section 702 continues to provide a system of foreign intelligence surveillance, including for international communications and surveillance targeted at foreign persons outside the U.S., that is more restrictive and protective than the Constitution would otherwise require.

As publicly described, the NSA's section 702 program of foreign-targeted Internet surveillance easily meets the reasonableness requirements of the Fourth Amendment. The surveillance is conducted for foreign intelligence purposes, which carry great weight in the Fourth Amendment balance, and the retention and use of information collected in the program about U.S. persons are subject to extensive and detailed minimization procedures designed to protect the reasonable privacy interests of Americans, and these minimization procedures have been reviewed and approved by a federal court.

There Is Every Reason to Believe that the NSA Programs Remain Necessary to Protect the National Security of the United States and Its Allies

As an institutional matter, this Committee and the Intelligence Committee of the Senate are in the best position to affirm for Members of Congress the ongoing importance and necessity of the NSA programs.

Both of the programs at issue are intended to provide quick and efficient detection and identification of contacts between known agents of foreign terrorist organizations and unknown operatives that may be hiding out within the United States. For my part, I believe that the need for such detection is just as acute today as it was in the immediate wake of 9/11.

More specifically with regard to the 215 order, from all that I know, I have every confidence that the bulk acquisition of the telephone metadata is necessary to preserve the data for use in the FBI's counterterrorism investigations and to combine the call-detail records generated by multiple telephone companies into a single searchable database. Furthermore, the use of the entire integrated database is essential to conduct focused link analysis and contact chaining of terrorist phone numbers and thereby discover new terrorist phone numbers that we did not know about before.

It is necessary to retain the data for a sufficient period, such as five years, to be able to conduct historical analysis to find connections between newly discovered phone numbers and the numbers of known terrorist agents that may have been the subjects of past investigations.

I believe that the 215 program provides a frequent and important input for ongoing investigations of terrorist activities. I don't believe the proper test of the program's necessity is whether it has provided the one primary piece of information required to thwart a specific terrorist plot just before an attack has been carried out. Any such narrow focus on the interdiction of particular mature plots is unrealistic because it does not take account of how these investigations are conducted and the fact that nearly all counterterrorism efforts involve numerous inputs from diverse sources over an extended period of time.

The Major Proposals for Curtailing or Modifying the NSA Programs and for Amending the FISA Authorities Should Be Rejected

I offer the following thoughts on why the principal legislative proposals for modifying the authorities of the NSA under FISA should not be approved.

The most sweeping change under consideration, as I understand it, would restrict the government's authority under section 215 to acquiring on an item-by-item basis only those individual business records, including telephone call-detail records, that directly pertain to the person who is the subject of the counterterrorism investigation. A variation on this proposal would limit the NSA to conducting one-by-one queries of the call-detail databases of the phone companies only while the data is retained by the companies in the ordinary course of business.

Such requirements would kill the NSA's telephone metadata program, because they would, by design, deny the NSA the broad field of data needed to conduct in an efficient and workable manner the link analysis and contact chaining that is enabled by the current program.

At the same time, denying the NSA the authority to acquire the metadata in bulk and to retain it for a period of years would preclude any historical analysis of connections between a terrorist phone number and other, yet undiscovered

numbers, and the ability to examine historical connections and patterns is among the most valuable capabilities of the 215 metadata program. Indeed, any proposal to limit the length of metadata retention to a period of less than the current five years should be approached with great care, because it would by definition diminish the capacity of the NSA to conduct this important historical contact analysis.

A less sweeping but still very significant restriction would prohibit the NSA from taking possession of the call-detail records obtained under the 215 order and would instead require that the data be maintained for an extended period under the control of the telephone companies, presumably at the expense of the federal government. The current program enables the NSA to acquire all of the telephone metadata on an ongoing basis from several companies in order to preserve the data in a segregated and secure manner and combine it together in a form that is efficiently usable and searchable. Ceding control of the combined database to the phone companies would presumably require the involvement of a private, third-party contractor to house and manage the data, since no single phone company has the ability to maintain and aggregate all of the data of the several companies and host the data on servers for a sufficient period of years in a searchable form.

Any such arrangement involving a third-party contractor, however, would be distinctly less efficient, less secure, and less subject to effective oversight by the executive branch, the FISA court, and Congress than the current program. That result cannot be a desirable one, both in terms of national security and in terms of the privacy of the data and the potential for its abuse.

Another proposal would require FISA court approval in advance of each query of the telephone metadata—in other words, a one-by-one court determination that there is reasonable articulable suspicion that the phone number to be queried against the database is associated with one of the specified foreign terrorist organizations. Such a requirement would place a significant restraint on the speed and flexibility of the program, and, if applied to second and third "hops" from the original seed number, would throttle the utility of the program entirely. Moreover, requiring court approval of each reasonable articulable suspicion determination would impose a legalistic judicial overlay on a judgment that is more appropriately made by seasoned intelligence analysts. The alternative proposal of requiring approval by the lawyers of the National Security Division of

the Justice Department would suffer from the same defect: It would interpose a lawyer's sensibility in place of the practical judgment of intelligence professionals.

One further proposal often raised is to attempt to graft onto the traditionally ex parte procedures of the FISA court a litigation-like adversary process—for example, by creating the position of a "Public Advocate" for the FISA court. Under certain of these proposals, the Public Advocate would be charged with representing the "public interest" or the "privacy interests" of the targets of the surveillance and would be expected to oppose the government's applications, at least in cases raising novel interpretations of FISA or asking to extend the law beyond how it has previously been applied. One such proposal would require that the Public Advocate receive a copy of each application for a FISA order and would give the Public Advocate the right to appeal any FISA order approved by the court.

This concept of introducing a Public Advocate into the FISA process raises constitutional concerns. Because the review of FISA applications requires access to the most sensitive national security information, any appointed advocate would have to be a permanent, trusted officer of the executive branch or of the FISA court with the necessary security clearances. Constitutional issues would arise in any mandate that the President invariably permit the Public Advocate to have access to the most sensitive classified information. Constitutional issues would also follow if the Public Advocate, an employee of the Judicial Branch, were given the power to appeal a decision of the FISA court over the objections of the executive branch. Among other things, the Public Advocate would lack the Article III standing necessary to initiate an appeal. If intended to act as an "independent" officer within the Judicial Branch, not simply an adviser to the judges but empowered to appeal rulings of the FISA court and granted the mandate to appear in court as an adversary to the executive branch, the Public Advocate would fall outside the three-branch framework established in the Constitution.

Moreover, if done in a constitutional form, introducing such an advocate position would not likely achieve the meaningful benefits that proponents hope for. The judges assigned to the FISA court are already assisted by permanent legal advisers who are steeped in the precedents of the court and whose job is to second guess the arguments and analyses of the executive branch. If a particular FISA application raises significant questions, the legal advisers are already asked to prepare separate, in-depth analyses for the judges. The recently disclosed opinions

of the FISA court convincingly show that the judges of the court and their legal advisers are not shy about applying a thoroughly independent review of the issues that is in no way beholding to the executive branch. If a Public Advocate were part of the executive branch, the advocate would always ultimately be answerable to the President. If employed by the court, the advocate would be little different from the existing legal advisers. Either way, the Public Advocate could never actually be a true independent adversary representing the interests of those under surveillance.

One final observation that I believe is important to keep in mind: Many of the reform proposals discussed above, including those that would attempt to convert the FISA process into an adversary proceeding and those that would impose more frequent judicial approvals or bureaucratic processing of decisions heretofore made in real time by intelligence analysts, would run the risk of recreating the type of cumbersome, overlawyered foreign intelligence regime that proved so inadequate in the face of 9/11.

This Committee knows far better than I how likely it is (or rather how inevitable) that America will suffer another catastrophic terrorist attack at some point in the years ahead. In the event of such an attack, I fear that the constrained and lawyerly process for conducting signals intelligence required under the proposed reforms would prove inadequate, and the President, any President, would be forced once again to fall back on his Article II authority to conduct the effective surveillance he determines necessary to protect the country from follow-on attacks. Indeed, I believe the American people would demand no less.

That cannot be a result this Congress would prefer. But it is, unfortunately, a very real possibility if the proposals currently under consideration were to be adopted.