UNDERSTANDING THE NSA PROGRAMS: BULK ACQUISITION OF TELEPHONE METADATA UNDER SECTION 215 AND FOREIGN-TARGETED COLLECTION UNDER SECTION 702

Steven G. Bradbury *

In response to the disclosures by former government contractor Edward J. Snowden, the Director of National Intelligence (“DNI”) has confirmed the existence of two foreign intelligence collection programs of the National Security Agency (“NSA”) and declassified key information. Executive branch officials have testified about the programs in open hearings in Congress, and the administration has released white papers providing further details to inform the public.

The first NSA program involves the bulk acquisition of telephone metadata through court orders issued under the business records provision of the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. § 1861—a provision added to FISA in 2001 by section 215 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), and therefore commonly referred to as “section 215.” The second, conducted under section 702 of FISA, 50 U.S.C. § 1881a, involves a broad program of electronic surveillance carried out on facilities within the United States and targeted at foreign persons reasonably believed to be located outside the United States. This second program includes, among other things, the so-called “PRISM” collection of Internet communications.

Relying on the information declassified and acknowledged by the government, this paper analyzes the legal basis for each of the programs and explains in detail why both are authorized by statute and fully consistent with the Constitution.

* Partner, Dechert LLP, and former head of the Office of Legal Counsel of the U.S. Department of Justice, 2005-2009. While in the Justice Department, the author led the legal effort to obtain initial court approval for the telephone metadata program in 2006 and also participated in the Bush administration’s work with Congress to secure passage of amendments to the Foreign Intelligence Surveillance Act in 2007 and 2008. The views expressed in this paper are the personal views of the author and do not represent the views of Dechert LLP or any current or former client.
I. SECTION 215 ORDER FOR ACQUISITION OF TELEPHONE METADATA

Section 215 provides that the Federal Bureau of Investigation (“FBI”) may apply for an order from the FISA court requiring the production of any “tangible things (including books, records, papers, documents, and other items)” needed “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 upon the basis of activities protected by the first amendment to the Constitution.” 50 U.S.C. § 1861. An application for a section 215 order must be supported by “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)” and by detailed minimization procedures designed to ensure that information about U.S. persons that may be obtained under the order will not be retained or disseminated unnecessarily. Id. § 1861(b)(2), (g).

As the government has confirmed, the NSA acquires telephone metadata in bulk under a section 215 business records order obtained by the FBI. This section 215 order must be reviewed and reapproved by the federal judges who sit on the FISA court every 90 days. It has been approved 34 times by 14 different federal judges since its initial approval in 2006.

The metadata acquired under this order consists of the transactional information that phone companies retain in their systems for a period of time in the ordinary course of business for billing purposes and that appears on typical phone bills. It includes only data fields showing which phone numbers called which numbers and the time and duration of the calls. The order does not give the government access to any information about the content of calls or any other subscriber information, and it does not enable the government to listen to or record any phone calls. The NSA needs to acquire control of the metadata from the phone companies in order (1) to preserve the data, since the companies retain it only for so long as necessary to bill their customers and resolve billing disputes. They are required by the Federal Communications Commission to retain the data for no longer than 18 months. 47 CFR § 42.6.

Access to the data is strictly limited under the terms of the court order. The order does not permit random searching of the database. Rather, the

---

1 As used in FISA, the term “United States person” means a U.S. citizen, a lawful permanent resident of the U.S., an association whose members include a substantial number of U.S. citizens or lawful permanent residents, or a corporation incorporated in the U.S., unless the corporation or association is part of or openly controlled by a foreign government. See 50 U.S.C. § 1801(i).

2 The phone companies retain the call-detail metadata in the ordinary course of business only for so long as necessary to bill their customers and resolve billing disputes. They are required by the Federal Communications Commission to retain the data for no longer than 18 months. 47 CFR § 42.6.
database may only be accessed through queries of individual phone numbers and only when the government has reasonable articulable suspicion that the “seed” number is associated with one of several specified foreign terrorist organizations. If the number appears to be a U.S. number, the reasonable suspicion cannot be based solely on activities protected by the First Amendment, such as statements of opinion, books or magazines read, Web sites visited, or places of worship frequented. Any query of the database requires approval from a small circle of designated NSA officers.

The output of a query will be a list of any phone numbers that have been called from the suspicious number or that have called it and the time and duration of those connections. The database includes metadata going back five years, to enable an analysis of historical connections. Any records older than five years are continually purged from the system and deleted, per the requirements of the court order.

In analyzing links to suspicious numbers, the government will be most interested in any connections that are found to numbers inside the United States, because the analysis of those numbers may suggest the presence of an agent of one of the foreign terrorist organizations in the U.S. Based in part on that information, the FBI may seek a separate FISA order for surveillance of the U.S. number, but that surveillance would have to be supported by individualized probable cause under FISA.

The NSA has confirmed that it is authorized to review connections two or three “hops” out from the suspicious seed number, depending on the analysis of those connections. Nevertheless, the NSA has also confirmed that only a very tiny fraction of the total database has ever been subject to review by analysts as a product of the queries. The database is kept segregated and is not accessed for any other purpose beyond this specific counterterrorism program, and FISA requires the government to follow procedures overseen by the court to minimize any unnecessary dissemination of U.S. numbers generated from the queries.

In addition to court approval, the section 215 telephone metadata 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 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.”

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.

A. Compliance with the Statutory Requirements of Section 215

Fourteen different federal judges on 34 occasions have concluded that the NSA’s bulk acquisition of telephone metadata for purposes of conducting the focused link analysis of suspected terrorist phone numbers described above meets all of the statutory requirements of section 215. That conclusion is confirmed by the plain terms of section 215 and by the background case law addressing the well-established “relevance” standard that governs the scope of administrative subpoena authorities and grand jury subpoenas for records.

Section 215 permits the acquisition of “any tangible things (including books, records, papers, documents, and other items)” so long as “there are reasonable grounds to believe that the [records] are relevant to an authorized investigation . . . to protect against international terrorism.” 50 U.S.C. §§ 1861(a)(1), 1861(b)(2)(A). The records will be “presumptively relevant to an authorized investigation” if the FBI shows, among other things, “that they pertain to . . . the activities of a suspected agent of a foreign power who is the subject of such authorized investigation” or to “an individual in contact with, or known to, [such] suspected agent of a foreign power.” Id. § 1861(b)(2)(A). The records also must be of the type 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.” Id. § 1861(c)(2)(D). The telephone metadata order satisfies each of these requirements.

1. Authorized counterterrorism investigations. — There are now and have been since the section 215 order was first approved in 2006 numerous open and formally authorized FBI investigations directed at protecting the people and interests of the United States against the threats posed by the foreign terrorist organizations that are the targets of the telephone metadata program.

2. Tangible things. — The telephone company call-detail metadata records obtained with the section 215 order are “tangible things” within the meaning of section 215 and are a type of record that may be obtained with a subpoena duces tecum or other order for the production of records (as distinct from oral

---

3 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.

testimony) that could be issued or enforced by a federal court. There is no doubt that “tangible things,” as used in the context of subpoenas and orders for the production of records includes, among other things, all forms of “documents,” broadly defined, including “electronically stored information.”

A subpoena duces tecum or other order requiring the production of “records or tangible things” may also require production of records on an ongoing basis, including electronic business records, like the telephone metadata records acquired with the section 215 order, that are created or generated in the ordinary course after the issuance of the order.  

3. Relevance. — 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.

In the context of administrative subpoenas, including civil investigative demands issued by regulatory agencies, the Supreme Court has long held that courts must enforce such 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. 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, and to subpoena records “of even potential relevance to an ongoing investigation.” Relevance is not a one-size-fits-all standard but is judged in light of the nature, purpose, and scope of the

---

5 See, e.g., 7 U.S.C. § 7733(a) (granting Secretary of Agriculture authority to issue administrative subpoenas requiring “production of all evidence (including books, papers, documents, electronically stored information, and other tangible things that constitute or contain evidence”) (emphasis added); Fed. R. Civ. Pro. 34, Notes of Advisory Committee on 2006 Amendments (confirming that a request for production of “documents” under the Federal Rules of Civil Procedure should be interpreted to include “electronically stored information,” as well as “paper documents”).

6 See, e.g., Chevron v. Salazar, 275 F.R.D. 437, 449 (S.D.N.Y. 2011) (holding that court may order prospective production of “materials created after the return date of the subpoena”); In re Application for Order Authorizing Use of Two Pen Register & Trap & Trace Devices, 632 F. Supp. 2d 202, 207 n.8 (E.D.N.Y. 2008) (under Stored Communications Act, “prospective . . . information sought by the Government . . . becomes a ‘historical record’ as soon as it is recorded by the provider”).

7 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.”).


inquiry, including the importance of the governmental interests involved in the investigation and the need for the records sought, \(^{11}\) and courts generally defer to the agency’s determination of relevance, provided the agency has a reasonable basis to believe the records will lead to useful information. \(^{12}\) 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.” \(^{13}\) 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.” \(^{14}\)

The relevance standard does not require a separate showing that every individual record in a subpoenaed database is “relevant” to the investigation. \(^{15}\) 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. \(^{16}\)

Under the concept of relevance endorsed in these cases and authorities, all of the bulk telephone metadata acquired by the NSA under the section 215 order is “relevant” to the counterterrorism investigations of the specified foreign terrorist organizations that are the targets of investigation. The entire database is appropriately treated as relevant because (1) the bulk acquisition of the metadata is necessary to preserve the data for use in the investigations and to combine the call-detail records generated by multiple companies into a

\(^{11}\) See Oklahoma Press, 327 U.S. at 209.

\(^{12}\) See, e.g., EEOC v. Randstad, 685 F.3d 433, 451 (4th Cir. 2012).


\(^{15}\) 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”).

\(^{16}\) 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 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).
single searchable database, and (2) the use of the entire integrated database is essential to conduct the focused link analysis of terrorist phone numbers described above, a type of analysis that provides a critical building block in these investigations.

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. The critical importance of these investigations for national security purposes also weighs heavily in the relevance analysis and supports the FISA court’s approval of an arrangement that enables the NSA to acquire all of the telephone metadata on an ongoing basis from several companies in order to preserve the data and combine it together in a form that is efficiently usable and searchable. Any alternative arrangement, including an arrangement that would cede control of the combined database to the private phone companies (probably under the management of a private, third-party contractor), would be less efficient, less secure, and less subject to effective oversight by the executive branch, the FISA court, and Congress.

B. The Metadata Program’s Compliance with the Constitution

The section 215 telephone metadata order as currently configured and implemented is also fully consistent with the Constitution, including both the Fourth and First Amendments.

1. Fourth Amendment. — 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 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) (holding that the acquisition of call-detail information through use of a pen register or trap and trace device is not a search for purposes of the Fourth Amendment and does not require a warrant).17

The force and relevance of Smith v. Maryland are not diminished in the present context because of the large size of the data set being acquired by the NSA. The Court’s conclusion in Smith that the defendant in that case did not have a reasonable expectation of privacy in his own call-detail information did not turn on the fact that the case involved a law enforcement investigation of a

---

17 Accord Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904-05 (9th Cir. 2008) (same analysis for email addressing information).
single person conducted over a short period of time. Indeed, if anything, the individual privacy interests of the tens of millions of telephone customers whose calling records are collected by the NSA as part of the bulk metadata acquisition approved in the section 215 order are lessened even further because of the very vastness and anonymity of the data set and the fact that the chances that the call-detail records of any one individual will ever be reviewed by an NSA analyst are vanishingly small.18

Furthermore, a government request for a company’s business records is not a “search” within the meaning of the Fourth Amendment that requires a warrant supported by probable cause. As discussed above, government agencies have authority under many federal statutes to issue administrative subpoenas without court approval for documents relevant to an authorized inquiry. In addition, grand juries have broad authority to subpoena records potentially relevant to whether a crime has occurred, and grand jury subpoenas also do not require court approval. In the modern world of electronic storage and data compilation, reliance on the same “relevance” standard in these other contexts can also result in extremely expansive requests for business records, as noted. If each such request for business records required a search warrant supported by probable cause, many of the civil investigations conducted by regulatory agencies and many grand jury investigations would come to a halt.

Even if the acquisition of the telephone calling records maintained by the phone companies could be considered a search for Fourth Amendment purposes, the circumstances of the NSA’s section 215 acquisition show that it would readily satisfy the basic reasonableness requirement that is the hallmark of the Fourth Amendment.19 Under established Supreme Court doctrine, the reasonableness of “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.”20

Foreign intelligence collection has long been recognized to be an area of “special needs” far removed from the ordinary criminal context to which the

18 The Supreme Court’s recent decision in United States v. Jones, 132 S. Ct. 945 (2012), does not mean that telephone metadata may only be acquired for individual phone users or that the acquisition of such metadata requires a warrant supported by individualized probable cause. In Jones, the Court held that the physical installation of a GPS tracking device on a suspect’s car for purposes of tracking the suspect’s every move as part of a criminal investigation required a search warrant. The section 215 metadata acquisition involves no physical invasion of anyone’s property, and it does not entail the tracking of any customer’s movements.

19 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).

warrant requirement applies, and the imperative of protecting the Nation against foreign threats is a governmental interest of the highest order.\(^{21}\) On the other side of the balance with regard to the section 215 order, any arguable intrusion on individual privacy interests is minimal. In addition, all of the many restrictions and safeguards applicable to the order establish its reasonableness for Fourth Amendment purposes. These include: (1) the prior approval of the FISA court, (2) the fact that the phone companies may challenge the scope and legality of the order before the court,\(^ {22}\) (3) the court-ordered limitation that queries of the database may only be conducted for individual phone numbers where the government has a reasonable articulable suspicion that the number is associated with a particular foreign terrorist organization, (4) the prohibition on using the database for any other purpose and the requirement that it be kept segregated from other data, (5) the restrictions on the number of officials who can approve access to the database and the other oversight and reporting requirements that apply to the program, and (6) the extensive minimization procedures that govern the retention and dissemination of any information about U.S. persons generated from the database.

Furthermore, the NSA has a strong imperative to collect and control the metadata in bulk, and alternative arrangements that would involve the retention of control over the data by the private phone companies would be less secure and less effective. The NSA must acquire the metadata in bulk for preservation of the data generated by the various phone companies and to enable the NSA to combine the data together into one searchable database that is kept under secure control. This bulk acquisition and control of the data by the NSA is critical for ensuring that the assembled database is not misused in violation of the court order and for making the program more readily susceptible to effective oversight by the executive branch, the FISA court, and the Intelligence Committees of Congress. For these reasons, the bulk acquisition of the metadata by the NSA would comply with the reasonableness requirement of the Fourth Amendment, if that requirement were applicable.

2. First Amendment. — The section 215 telephone metadata acquisition does not violate the First Amendment. The acquisition does not involve or relate to the content of any phone call, and in the case of any phone numbers that appear to be U.S. numbers, the reasonable articulable suspicion required to test the seed number against the database may not be based solely on activities protected by the First Amendment. Moreover, by its terms, section 215 does not permit the collection of any records in furtherance of an investigation of a U.S. person if the investigation is based solely on First Amendment-protected activity. Finally, the collection of data or other materials and the review of

\(^{21}\) 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.”).

\(^{22}\) See 50 U.S.C. § 1861(f)(2) (providing procedures for challenges to section 215 orders by persons receiving such orders).
those materials as part of an authorized investigation and in a manner reasonable under the Fourth Amendment cannot be condemned on First Amendment grounds based on assertions of a subjective “chilling effect” on the part of individuals whose records may be included in the materials under review.23

II. SECTION 702 SURVEILLANCE AUTHORITY AND THE NSA PROGRAM

Section 702 of FISA authorizes a broad program of electronic surveillance carried out in the U.S. where the collection is for a significant foreign intelligence purpose and is targeted at foreign persons reasonably believed to be located outside the U.S. See 50 U.S.C. § 1881a. Congress added section 702 to FISA in the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436. Similar foreign-targeted, programmatic surveillance authority was initially provided on a temporary basis in the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552. Congress reauthorized and extended the authority enacted in the FISA Amendments Act in 2012. On each occasion, this statutory authorization was approved by overwhelming majorities in both the House and the Senate.

Section 702 provides that the Attorney General and the DNI may jointly authorize, for up to one year at a time, surveillance targeted at non-U.S. persons who are reasonably believed to be located outside the United States to acquire foreign intelligence information, provided the FISA court approves the targeting procedures under which the surveillance occurs and the minimization procedures that govern use of the acquired information. 50 U.S.C. § 1881a(a). The surveillance is conducted through compelled assistance from communications service providers. See id. § 1881a(h).

The program encompasses surveillance of telephone and Internet communications, and the NSA’s Internet collection under this authority includes both (1) electronic communications and stored communications acquired directly from Internet service providers, and (2) electronic communications acquired at “upstream” points on the Internet backbone networks. See NSA, The National Security Agency: Missions, Authorities, Oversight and Partnerships 4 (Aug. 9, 2013) (describing the NSA’s section 702 program). The NSA generates specific “identifiers,” which may include, for example, email addresses and telephone numbers used by non-U.S. persons overseas who the government believes “possess, communicate, or are likely to receive foreign intelligence information authorized for collection under an approved certification.” Id. “Once approved, those identifiers are used to select communications for acquisition,” and the communications service providers “are compelled to assist NSA in acquiring the communications associated with those identifiers.” Id.

---

The surveillance authorized under section 702 may 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, or (4) intentionally acquire any communication as to which the sender and all recipients are known to be in the U.S. 50 U.S.C. § 1881a(b). Section 702 requires the Attorney General to adopt, and the FISA court to approve, targeting procedures reasonably designed to ensure compliance with these limitations, as well as detailed minimization procedures designed to ensure that any information about U.S. persons captured through this surveillance will not be unnecessarily retained and will not be disseminated in intelligence reports unless the information is needed to understand the intelligence significance of the report. See id. § 1881a(c)-(g).

In short, section 702 may not be used for any electronic surveillance targeted at a U.S. person or at any person believed to be in the United States, and under FISA, electronic surveillance designed to intercept the communications of U.S. persons anywhere in the world requires an individualized court order supported by probable cause. See id. § 1804 (setting forth the requirements for individualized FISA court orders authorizing electronic surveillance); see also id. § 1802 (providing a limited exception authorizing electronic surveillance without a court order of communications wholly between or controlled by foreign governments or nations where “there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party”).

According to the information declassified and publicly released by the DNI, the FISA court has concluded that the NSA’s Internet content surveillance as currently conducted, including the PRISM collection, accords with section 702 and the requirements of the Constitution. This surveillance is targeted at non-U.S. persons reasonably believed to be located outside the United States, is not designed to target any U.S. person or any person known to be in the U.S., and does not involve the intentional surveillance of wholly domestic communications. Furthermore, the FISA court has determined that the nature and scope of this collection and the current minimization procedures that apply to the retention and use of any U.S. person information obtained as part of this program ensure that the surveillance meets the general reasonableness requirements of the Fourth Amendment.

As part of the materials recently made available to the public, the DNI has partially declassified and released FISA court opinions from 2011 that addressed and resolved a significant compliance issue relating to one aspect of the section 702 Internet surveillance. These opinions reveal that in 2011, the NSA reported to the FISA court that there are technical limitations in the
upstream Internet collection that make it impossible to isolate and acquire only those electronic communications that contain the approved “identifiers” when the targeted communications are transmitted as part of a multi-communication batch. Because upstream collection accounts for about nine percent of the NSA’s Internet surveillance and the relevant communications involve only a fraction of the upstream collection, this technical limitation affects a very small percentage of the overall section 702 collection; nevertheless, the technical issue means that the upstream collection will inevitably capture several thousand wholly domestic Internet communications per year (out of the tens of millions of communications properly targeted for surveillance).  

As a result, the FISA court issued an opinion on October 3, 2011 concluding that the minimization procedures for the upstream collection as applied at the time did not comply with section 702 and did not satisfy the reasonableness requirements of the Fourth Amendment because the collection entailed the retention, possibly for up to five years, of the inadvertently captured domestic communications and the ongoing potential that analysts might access those communications in conducting searches of the collected data. In response to the court’s opinion, within a month, the NSA adopted more stringent minimization procedures for the upstream collection to put further screens and restrictions in place to avoid the review and use of the multi-communication batches likely to contain the inadvertently collected domestic communications, and the NSA also took the further step of purging from its database all such multi-communication batches that had been acquired prior to the implementation of the revised procedures. In an opinion dated November 30, 2011, the FISA court concluded that the revised minimization procedures adequately corrected the deficiencies identified in the October 3 opinion and brought the upstream collection into compliance with both section 702 and the Fourth Amendment.

Accordingly, the collection as presently configured and implemented has been determined by the FISA court to be the type of foreign-targeted intelligence surveillance that Congress intended to authorize when it enacted and reauthorized section 702 in 2008 and 2012.

In addition to stringent, in-depth examination by the FISA court for compliance with the requirements of the statute and the Constitution, the section 702 program is also subject to thorough review and oversight within

---


26 See id. at 59-63, 69-80. The October 3, 2011 FISA court opinion demonstrates beyond dispute that the FISA court is no “rubber stamp” for NSA surveillance. Indeed, it is doubtful that any other complex, technical federal program—whether a national security, law enforcement, or regulatory program—is subjected to more rigorous judicial review than these NSA programs.

27 See FISA Court Memorandum Opinion of Nov. 30, 2011 (Bates, J.) (available on the DNI’s Web site, as noted above).
NSA, including by the NSA’s Director of Compliance, a position created by the Director of NSA as part of reforms instituted in 2009. The section 702 program is further subject to extensive reviews and periodic reports to Congress by inspectors general, as well as vigorous ongoing oversight by the Intelligence Committees of Congress. Moreover, the administration has stated that in advance of the reauthorization of section 702 in 2012, the leaders and full membership of the Intelligence Committees of both Houses of Congress were briefed on the history, operation, and use of this program and all members of Congress were offered the opportunity for a similar detailed briefing. Since the Snowden disclosures, the NSA and DNI have conducted additional extensive briefings of Congress.

A. Constitutional and Historical Context for NSA’s Section 702 Program

A full understanding of the legality of this NSA program requires discussion of the governing constitutional principles and the historical context that led up to enactment of section 702.

It is important to realize that 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 held only that warrants are generally required for ordinary criminal investigations and for the investigation of purely domestic security threats. While the Supreme Court has not had occasion to judge “the scope of the President’s surveillance power with respect to the activities of foreign powers, within or without this country,” the federal courts of appeals have consistently held that the President has inherent authority under Article II of the Constitution to conduct warrantless searches and surveillance within the United States for foreign intelligence purposes. Thus, in 2002, the Foreign Intelligence Surveillance Court of Review stated that “all the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . We take for granted that the President does have that


30 Keith, 407 U.S. at 308.

authority and, assuming that is so, FISA could not encroach on the President’s constitutional power.”

Accordingly, prior to enactment of FISA in 1978, the executive branch conducted foreign intelligence surveillance, including surveillance of Americans in the United States, without any court involvement. Indeed, the pre-FISA version of the federal wiretap statute, enacted as Title III to the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”), specifically provided that nothing in the federal wiretap laws “shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.” 18 U.S.C. § 2511(3) (1976). Title III further provided that “[t]he contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial, hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.” Id.

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 always remain 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). Foreign intelligence collection has long been recognized to be an area of “special needs” far removed from the ordinary criminal context to which the warrant requirement applies.

---

32 In re Sealed Case, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002).


34 See FISA Court Memorandum Opinion and Order of Oct. 3, 2011, at 69-70; Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence, 103d Cong., 2d Sess. 62, 63 (1994) (statement of Deputy Attorney General Jamie S. Gorelick) (”[I]t is important to understand that the rules and methodology for criminal searches are inconsistent with the collection of foreign intelligence and would unduly frustrate the President in carrying out his foreign intelligence responsibilities. . . . [W]e believe that the warrant clause of the Fourth Amendment is
Under established Supreme Court doctrine, 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.”). 35

In the post-Watergate period, concerns were raised about the scope and abuse of warrantless surveillance conducted unilaterally by the executive branch in the 1960s and 1970s, including concerns over surveillance directed at domestic political dissent rather than foreign threats, and these concerns were highlighted in the investigations of the Church and Pike Committees of Congress. Responding to these issues, Congress and the President, with the support of the Justice Department, came together in 1978 to agree on the enactment of FISA, an unprecedented statutory scheme 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 select 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. 36

As the D.C. Circuit described this new regime, whereas in the Title III wiretap provisions covering domestic criminal surveillance, “Congress emphasized the privacy rights of U.S. citizens,” in FISA, “Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements.” United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982) (Wilkey, Bork, & Scalia, JJ.). “The statute is meant to ‘reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights.’ In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which

governs law-enforcement surveillance.” *Id.* (quoting S. Rep. No. 95-701, 95th Cong., 2d Sess. 16 (1978)). The court concluded, “In FISA Congress has made a thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence.” 692 F.2d at 148.

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. 37 FISA also repealed the former provision of Title III that had disclaimed any intent to regulate the President’s conduct of foreign intelligence activities and replaced it with a provision exempting from statutory regulation the acquisition of intelligence information from “international or foreign communications” not involving “electronic surveillance” as defined in FISA, 38 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.” 39 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. 40

In the years following the passage of FISA, 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 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

---


40 *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 . . . ”).
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 a follow-on attack on the U.S. homeland in the immediate wake of 9/11 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.”

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 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.

B. Final Analysis of Section 702 Program

As publicly described, the NSA’s program of foreign-targeted Internet surveillance involves the collection and review of communications of Americans, including Americans inside the United States, where those communications are to or from the foreign targets of the communication, and it may involve other forms of incidental collection of communications of U.S.

---

41 U.S. Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President 34 (Jan. 19, 2006).
persons. One recent unconfirmed news report indicates that the program may also include the scanning of all Internet packet data crossing into and out of the United States at certain communications gateways for telltale references to the foreign targets of the surveillance. As long as all such collection is not intentionally targeted at U.S. persons or persons known to be in the U.S. and is not designed intentionally to acquire communications as to which the sender and all recipients are known to be in the U.S., it would appear to comply with the terms of section 702. The approval of the required targeting and minimization procedures by the FISA court is confirmation that the court has determined, as required by section 702, that the scope and contours of this surveillance program satisfy the restrictions imposed by the statute.

It is also evident that this surveillance program 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.\textsuperscript{42} Even if reports are correct that the program also involves the brief machine scanning of international Internet communications, including of U.S. persons, for references to specified foreign targets, such machine scanning would entail minimal intrusion into legitimate privacy interests, since (1) it would be limited to international communications, for which expectations of privacy are significantly diminished,\textsuperscript{43} (2) for the vast bulk of communications, it would involve only the initial brief scanning of data packets by a machine, not any monitoring or retention of the communications and not any review by human analysts, and (3) any monitoring, review, or retention of U.S.-person communications would be limited to communications that specifically relate in some way to a specified foreign target of the program.

For all of these reasons, it appears quite clear that the NSA’s foreign-targeted Internet collection program, as described, fully accords with the Constitution and the applicable federal statutes.

\textsuperscript{42} See, e.g., FISA Court Memorandum Opinion of Nov. 30, 2011.

\textsuperscript{43} Americans presumably well understand that international communications are potentially subject to all manner of interception and surveillance by foreign governments operating without the limitations imposed in FISA and without the restraints applied by the NSA.