5-1-2014

# Seizure of Electronic Data under the USA PATRIOT Act

John Ahn

**Seizure of Electronic Data under the USA PATRIOT Act**

John Ahn

## I. Introduction

This article examines how the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act") has been interpreted and applied by federal agencies to collect electronic data in the United States for the purpose of combating terrorism. In addition, it reviews whether the federal agencies' programs are legally valid under the USA PATRIOT Act and the Fourth Amendment.

Part II provides the constitutional framework that establishes and limits the authority of federal agencies to conduct surveillance operations domestically. This includes an overview of the Fourth Amendment and the related case law governing surveillance. Part III provides the statutory framework that examines the relevant statutes, in addition to the USA PATRIOT Act, that pertain to intelligence collection and surveillance law, such as the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III") and the Stored Communications Act of 1986 ("SCA").

Part IV reviews the recently exposed government surveillance programs that have been collecting information on U.S. citizens at home. This section focuses on the two primary federal agencies that have used the USA PATRIOT Act to conduct domestic surveillance – the Federal Bureau of Investigation ("FBI") and the National Security Agency ("NSA"). In addition, the

section evaluates the constitutionality of these programs and explains why they are not in violation of the Fourth Amendment. It also explains how the programs are legally valid when considering the interest of maintaining national security.

## II. Constitutional Framework

The United States Supreme Court has examined the topic of surveillance in relation to the Fourth Amendment in numerous cases. These cases shed light into whether the current surveillance programs by the FBI and NSA are constitutional. However, an initial examination of the Fourth Amendment is necessary to fully understanding the case law. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[1]

Thus, the Fourth Amendment can be broken down into two sections: the first portion as "Reasonableness Clause" and the second portion as the "Warrant Clause." While the "Reasonableness Clause" establishes the protection against unreasonable searches and seizures by the government, the "Warrant Clause" provides the requirements for a warrant to be issued.

The matter of surveillance was first reviewed by the Supreme Court in *Olmstead v. United States*.[2] There, law enforcement officers intercepted communications by inserting wires along the original telephone cables that were outside the properties of the defendants.[3] The Court held that the wiretapping of the defendants' telephone conversations did not constitute a

[1] U.S. Const. amend. IV.
[2] *Olmstead v. United States*, 277 U.S. 438 (1928).
[3] *Id.* at 456-7.

"search" or "seizure" within the meaning of the Fourth Amendment and thus, no Fourth Amendment protection applied.[4]

In 1967, the Supreme Court reviewed two cases relating to wiretapping and eavesdropping surveillance: *Berger v. New York* and *Katz v. United States*. In *Berger v. New York*, the defendant was convicted of conspiracy to bribe a public official based primarily on evidence gathered by eavesdropping.[5] The Supreme Court found that the New York statute granting the authority to eavesdrop was too broad in scope and thus, violated the Fourth Amendment.[6] The Court further held that because phone conversations were within the protection of the Fourth Amendment, the use of electronic devices to capture such conversations constituted a "search" within the meaning of the Amendment.[7]

In *Katz v. United States*, the Supreme Court again addressed the collection of evidence obtained by surveillance of telephone conversations.[8] There, FBI agents heard the defendant's telephone conversations through an electronic listening and recording device that was placed on the outside of the public telephone booth used by the defendant.[9] The Court specifically overruled *Olmstead* and found that because the defendant expected his conversations to remain private despite being in a public telephone booth, the government surveillance constituted a "search" within the meaning of the Fourth Amendment and thus, provided the defendant with protection in the form of a warrant needing to be secured prior to the wiretapping surveillance.[10]

Prior to the *Katz* decision, the Court utilized a property-rights test that required a trespass or physical intrusion into a "constitutionally protected area" in order for the Fourth Amendment

---

[4] *Id.* at 466.
[5] *Berger v. New York*, 388 U.S. 41, 44-5 (1967).
[6] *Id.* at 60.
[7] *Id.* at 62-4.
[8] *Katz v. United States*, 389 U.S. 347 (1967).
[9] *Id.* at 348.
[10] *Id.* at 352-9.

to apply.[11] *Katz*, however, established not only the warrant requirement for wiretapping, but also replaced the property-based approach with a two-prong framework for determining what constitutes a search under the Fourth Amendment.[12] The first prong asks whether the individual in question demonstrates an actual expectation of privacy; in other words, a subjective test.[13] The second prong revolves around an objective test of whether that expectation is reasonable in the eyes of society.[14]

The Supreme Court's next case dealing with electronic surveillance was *Smith v. Maryland*.[15] There, law enforcement officers requested that the local phone company install a device called a pen register[16] to record the phone numbers dialed from the defendant's home phone.[17] However, the officers did not obtain a warrant or court order prior to the installation.[18] The Supreme Court applied the two prong test established in *Katz* to find that neither the defendant manifested an expectation of privacy nor society could reasonably expect privacy in the numbers dialed on a phone.[19] In essence, by dialing phone numbers that a third-party phone company would ultimately receive, the defendant had voluntarily disclosed that information to the public and thus, relinquished any anticipated notion of privacy. The Court went on to hold that because the installation and use of the pen register did not constitute a search according to the Fourth Amendment, law enforcement officers did not need to obtain a search warrant.[20]

---

[11] Joshua Dressler, Alan C. Michaels, *Understanding Criminal Procedure Volume 1: Investigation* 68-9 (6th ed, 2013).
[12] *Id.* at 70-1.
[13] *Id.* at 72-3.
[14] *Id.*
[15] *Smith v. Maryland*, 442 U.S. 735 (1979).
[16] A pen register should be distinguished from a trap and trace device. While a pen register records phone numbers that are dialed (*i.e.*, outbound phone calls), a trap and trace device shows what phone numbers dialed a specific location (*i.e.*, inbound phone calls).
[17] *Id.* at 737.
[18] *Id.*
[19] *Id.* at 745.
[20] *Id.* at 745-6.

The improvement of technology has required the Supreme Court to reconsider what constitutes a "search" within the meaning of the Fourth Amendment. For instance, in *Kyllo v. United States*, law enforcement officials, without a warrant, used a thermal-imaging device at the defendant's home to determine whether there were heat signatures consistent with the growth and maintenance of marijuana.[21] After the device produced sufficient evidence indicating that marijuana was in the defendant's home, a search warrant was obtained and executed.[22] The Court, however, found that because the thermal imaging device was "not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[23]

Finally, in *United States v. Jones*, the Supreme Court addressed the issue of whether the use of a Global Positioning System ("GPS") device to track the defendant's movements constituted a "search" within the meaning of the Fourth Amendment.[24] Although a warrant was obtained by law enforcement officials, the GPS monitoring exceeded the scope of the warrant.[25] The Court held that law enforcement's use of the GPS did amount to a "search" within the meaning of the Fourth Amendment and as such, invalidated any evidence obtained outside the scope of the warrant.[26]

In reviewing these cases, the decisions indicate a trend by the Supreme Court that despite advancements in technology, privacy expectations under the Fourth Amendment exist to protect U.S. citizens against warrantless searches and seizures. For instance, while *Katz* shows how privacy expectations can be found in a public telephone booth – a form of communications

---

[21] *Kyllo v. United States*, 533 U.S. 27, 29 (2001).
[22] *Id.*
[23] *Id.* at 40.
[24] *United States v. Jones*, 132 S. Ct. 945, 948 (2012).
[25] *Id.*
[26] I*d.* at 949.

technology rarely used today due to the dawn of mobile phones – the *Kyllo* decision demonstrates how law enforcement's use of modern technology in the form of a thermal imaging device demands protection under the Fourth Amendment.

## III. Statutory Framework

### A. Omnibus Crime Control and Safe Streets Act of 1968

As a result of the Supreme Court decisions in *Berger* and *Katz*, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").[27] In general, the statute requires the government to secure a warrant or another form of judicial approval in order to conduct electronic surveillance for criminal investigation purposes.[28] Applications for court orders approving the wiretap or electronic surveillance must show probable cause that the surveillance will produce evidence of a crime.[29] Title III establishes criminal penalties and civil damages against any individual who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept" any of the covered communications.[30] The statute defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[31] Although the original version of Title III covered only wire and oral communications, Congress enacted the Electronic Communications Privacy Act of 1986 ("ECPA") as an amendment to Title III to include electronic communications.[32]

---

[27] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211.
[28] 18 U.S.C. § 2516.
[29] 18 U.S.C. § 2518(1)(d).
[30] 18 U.S.C. § 2511(1)(a).
[31] 18 U.S.C. § 2510(4).
[32] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

Title III does grant certain exceptions, however, such as a provider exception and "readily accessible to the public" exception.[33] It is noteworthy to mention that the provider exception allows for providers to assist government agencies in the interception of wire, oral, or electronic communications or electronic surveillance operations with a court order or Executive Branch certification.[34] In essence, Title III forbids either private party or governmental entity from the interception of wire, oral, and electronic communication unless one of the exceptions applies.

B. Stored Communication Act of 1986

In 1986, Congress enacted the Stored Communications Act ("SCA") as part of the ECPA.[35] The primary purpose of the SCA was to provide Internet network account users statutory privacy rights due to the limited protection offered by the Fourth Amendment.[36] In essence, the statute enhances protection against not only government requests to access users' private information from Internet Service Providers ("ISPs"), but also voluntary disclosure by ISPs to the government about their customers.[37] Section 2701 of the SCA establishes criminal penalties for any individual who:

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.[38]

C. Road to Foreign Intelligence Surveillance Act of 1978

---

[33] 18 U.S.C. § 2511(2)(a)(i) and 18 U.S.C. § 2511(2)(g)(i).
[34] 18 U.S.C. § 2511(2)(a)(i).
[35] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.
[36] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1212 (2004).
[37] *Id.* at 1212-3.
[38] 18 U.S.C. § 2701(a).

In enacting Title III, Congress did not tackle the issue of warrantless surveillance in the United States for foreign intelligence collection purposes. However, since the mid twentieth century, presidents beginning with Franklin D. Roosevelt have used their Executive authority to authorize warrantless electronic surveillance. The Supreme Court directly addressed the matter in *United States v. United States District Court for the Eastern District of Michigan* ("Keith").[39] The case involved a conspiracy by a domestic group to bomb an office of the Central Intelligence Agency ("CIA") in Michigan.[40] There, the Court held that under the Fourth Amendment, the government must secure a warrant or another form of judicial authorization before conducting electronic surveillance for the purpose of combating a domestic threat.[41] The Court, however, limited its finding by stating that because of the "potential distinctions between Title III criminal surveillances and those involving the domestic security…the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection."[42] The Court noted:

> that domestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime
>
> . . . . Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant

[39] *United States v. United States District Court for the Eastern District of Michigan (Keith)*, 407 U.S. 297 (1972). The case is also known as the Keith case because of U.S. District Court Judge Damon Keith's decision, rejecting the government's argument that a search warrant was not required to conduct surveillance for issues pertaining to "domestic security."
[40] *Id.* at 299.
[41] *Id.* at 321.
[42] *Id.* at 322-3.

> application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.[43]

Thus, the Court recognized a critical distinction of Fourth Amendment requirements between domestic surveillance operations for national security and criminal investigations.

After the Court's decision, another case involving warrantless electronic surveillance for national security reasons arose in the D.C. Circuit. In *Zweibon v. Mitchell*, federal law enforcement officers, with the approval of the Attorney General, conducted a warrantless electronic surveillance operation of the Jewish Defense League (JDL).[44] The JDL was a political group located in the United States that the government argued was committing acts of aggression that threatened U.S.-Soviet relations and thus resulted in the Soviet Union, a foreign power, posing a national security threat to the United States.[45] The D.C. Circuit, sitting en banc, disagreed with the government's argument, and held that despite the surveillance having been approved by the executive branch in the name of national security and foreign intelligence collection, the Fourth Amendment required that a warrant be obtained.[46]

The Watergate scandal exposed gross abuses by the Nixon Administration to conduct warrantless surveillance operations on various opposition political groups and individuals in the name of national security, but in reality, to further the Administration's own goals and agendas. For instance, some of the government's surveillance activities included gathering information on civil rights leader and activist Martin Luther King, Jr., and the Women's Liberation Movement.[47] In essence, this resulted in collection of "enormous amounts of personal and political information

---

[43] *Id.*
[44] *Zweibon v. Mitchell*, 516 F.2d 594, 605-6 (D.C. Cir. 1975).
[45] *Id.* at 608-9.
[46] *Id.* at 614.
[47] Foreign Intelligence Surveillance Act of 1978: Hearings Before the Subcomm. on Intelligence and the Rights of Americans of the Senate Select Comm. on Intelligence, 95th Cong. 266 (1978) at 271, 277 (1978).

serving no legitimate governmental interest."[48] As a result, a U.S. Senate committee, headed by Senator Frank Church, was formed in 1975 to investigate the activities of U.S. intelligence and law enforcement agencies. The investigation uncovered domestic intelligence collection efforts that critics argued violated the Fourth Amendment.[49]

D. Foreign Intelligence Surveillance Act of 1978

In response to Watergate and the D.C. Circuit's decision in *Zweibon*, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") in 1978 to establish oversight of domestic surveillance activities by intelligence and law enforcement agencies that are conducted for foreign intelligence purposes.[50] FISA provides that federal law enforcement agencies must obtain some form of judicial authorization to conduct electronic surveillance or physical searches of individuals or groups engaged in international terrorism against the United States on behalf of a foreign power.[51] The statute establishes criminal penalties and civil liabilities for any individual who intentionally engages in electronic surveillance not authorized by the statute.[52] Although FISA contains provisions related to physical searches, our primary focus will be on electronic surveillance.[53]

Court-ordered electronic surveillance requests are granted by a special court created by FISA, the Foreign Intelligence Surveillance Court ("FISC").[54] FISC oversees application requests made by federal law enforcement agencies for surveillance orders.[55] The FISC meets in

---

[48] *Id.* at 261.
[49] *See* S. REP. NO. 95-701, at 9 (1978) (stating that the "report of the Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, issued in 1976, provided firm evidence that foreign intelligence electronic surveillance involved abuses and that checks upon the exercise of those clandestine methods were clearly necessary").
[50] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783.
[51] 50 U.S.C. § 1804 and 50 U.S.C. § 1802.
[52] 50 U.S.C. § 1809 and 50 U.S.C. § 1810.
[53] 50 U.S.C. § 1821 to § 1829.
[54] 50 U.S.C. § 1803.
[55] *Id.*

secret and is comprised of eleven United States District Court judges that are selected by the Chief Justice of the United States.[56] Although arguments have been made challenging the constitutionality of FISA, courts have generally disagreed and upheld FISA's constitutionality.[57]

For FISC to grant a court order permitting surveillance, the federal law enforcement officer applying for surveillance order must initially obtain the Attorney General's approval and then submit an application to FISC containing the following:

> (1) the identity of the Federal officer making the application;
> (2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;
> (3) the identity, if known, or a description of the target of the electronic surveillance;
> (4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—
>
> > (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and
> > (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (5) a statement of the proposed minimization procedures;
> (6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
> (7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate—
>
> > (A) that the certifying official deems the information sought to be foreign intelligence information;
> > (B) that the purpose of the surveillance is to obtain foreign intelligence information;
> > (C) that such information cannot reasonably be obtained by normal investigative techniques;
> > (D) that designates the type of foreign intelligence information being sought according to the categories described in section 101 (e); and
> > (E) including a statement of the basis for the certification

[56] The number of judges on FISC was increased from seven to eleven after the enactment of the USA PATRIOT Act.
[57] *See United States v. Cavanagh*, 807 F.2d 787, 791 (9th Cir. 1987) (holding that special courts such as the FISA Court do not violate Article III of the Constitution); *United States v. Rosen*, 447 F. Supp. 2d 538, 550 (E.D. Va. 2006) (holding that FISC did not violate First Amendment rights of defendants for their lobbying activities).

that—

(i) the information sought is the type of foreign intelligence information designated; and
(ii) such information cannot reasonably be obtained by normal investigative techniques…[58]

An initial application for electronic surveillance under FISA contains several significant requirements that demand emphasis. They include the requirement of executive branch approval from the Attorney General; minimization procedures that must comply with the definition established in the statute; and the executive branch official's certification that the surveillance is being conducted for a foreign intelligence information purpose. Minimization procedures under FISA are defined as:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
> (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802 (a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.[59]

[58] Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, § 104(a)(7), 92 Stat. 1783.
[59] 50 U.S.C. § 1801(h).

In addition, FISC must determine that probable cause[60] exists as to the target of the surveillance being a "foreign power" or an "agent of foreign power" and the location of the surveillance being used by that foreign power or its agent.[61] In the event that the target is a "United States person," FISC must evaluate whether the individual is being "considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States" as part of the probable cause determination.[62] Because FISC's probable cause determination revolves around distinguishing whether a "United States person" can be an "agent of foreign power," FISA's definition is of utmost importance. FISA defines a "United States person" who is considered an "agent of foreign power" as any person who:

> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
> (D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).[63]

FISA also establishes that the purpose of the surveillance order must be for foreign intelligence. The statute defines foreign intelligence information to mean:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

---

[60] Probable cause in the context of domestic intelligence collection differs from probable cause in the criminal investigation context. For instance, while probable cause in criminal investigation centers on whether the crime has been or will be committed, probable cause in domestic intelligence collection depends on whether the target and location of the surveillance is a foreign power or agent of foreign power and that the foreign power or agent will use the targeted surveillance location.
[61] 50 U.S.C. § 1805(a)(2)(A) and (B).
[62] *Id.*
[63] 50 U.S.C. § 1801(i).

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States.[64]

Since the Supreme Court in *Katz* found that electronic surveillance constitutes a search within the meaning of the Fourth Amendment, the lower courts have wrestled with the issue of whether warrantless electronic surveillance could ever be conducted. In the landmark case of *United States v. Truong Dinh Hung*, the FBI conducted a warrantless surveillance operation on one of the defendants, Truong Dinh Hung, who was a Vietnamese citizen suspected of committing espionage by transmitting classified information to the Vietnam government.[65] There, the Fourth Circuit established a foreign intelligence exception to the Fourth Amendment's warrant requirement and held that warrants should not need to be obtained for every foreign intelligence surveillance operation.[66]

Additionally, the Fourth Circuit underscored that the "executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons."[67] In applying the "primary purpose" test, the court affirmed the district court's conclusion that because the investigation of Truong had become more of a criminal investigation than one with a foreign intelligence purpose as of July 20, 1977, evidence collected after that

[64] 50 U.S.C. § 1801(e).
[65] *United States v. Truong Dinh Hung*, 629 F.2d 908, 911-912 (4th Cir. 1980).
[66] *Id.* at 914-5.
[67] *Id.* at 915.

date should be excluded due to the lack of a warrant.[68] Thus, the court distinguished warrantless surveillance for criminal investigation from that of foreign intelligence collection.

Because the case was decided immediately after the enactment of FISA, the Fourth Circuit did not have an opportunity to undergo its analysis under the statute. Nonetheless, *Truong* is significant for two main reasons. First, Truong recognized the inherent power of the Executive to conduct warrantless electronic surveillance for foreign intelligence gathering purposes.[69] Second, the primary purpose test established a bright line rule for federal intelligence and law enforcement agencies to follow when conducting warrantless electronic surveillance.[70]

In addition to reviewing the constitutionality of warrantless electronic surveillance, courts have examined domestic intelligence collection with a court order under FISA in relation to an individual's privacy rights under the Fourth Amendment.[71] In *United States v. Duggan*, the Second Circuit not only held that FISA was constitutional, but also underscored the Supreme Court's decision in the *Keith* case that Fourth Amendment requirements are fluid when "differing governmental interests are at stake."[72] There, the defendants, who were members of the Irish Republican Army, argued that the government's surveillance leaned more towards criminal investigation purposes than national security reasons.[73] The court, however, applied the primary purpose test established in *Truong* to determine that the surveillance application met

---

[68] *Id.*
[69] *Id.* at 914-5.
[70] *Id.*
[71] *See United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (applying the primary purpose test to find that the purpose of the surveillance was for the collection of foreign intelligence).
[72] *United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (holding that "governmental interests presented in national security investigations differ substantially from those presented in traditional criminal investigations").
[73] *Id.* at 77.

"the statutory requirement for certifying that the information sought was foreign intelligence information."[74]

E. USA PATRIOT Act of 2001

The tragic events of September 11 prompted Congress, under the direction of the Bush Administration, to take a more aggressive posture against terrorism by amending FISA with the USA PATRIOT Act.[75] In effect, the USA PATRIOT Act provides federal agencies with more powerful tools to combat terrorism ranging from stronger anti-money laundering measures to enhanced border security and surveillance procedures. For instance, the "Enhanced Surveillance Procedures" section of the USA PATRIOT Act contains modifications to FISA that allow surveillance activities that the original statute did not permit.[76] Several of these provisions include: (1) the expanded access to records and other tangible things; (2) the enhanced use of pen register and trap and trace devices; (3) roving surveillance; and (4) the lone wolf amendment.[77] These provisions will be examined in turn to show how federal agencies can apply the statutory enhancements to their surveillance programs.

Section 215 under the USA PATRIOT Act dispenses with the limitation in Section 501[78] under FISA regarding the seizure of business records from a "common carrier, public accommodation facility, physical storage facility, or vehicle rental facility."[79] Not only does Section 215 now allow the FBI to obtain business records from any business or entity, but it also

---

[74] *Id.*
[75] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107–56, 115 Stat. 272.
[76] *Id.* at tit. II.
[77] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 101(b)(1)(C), 118 Stat. 3638.
[78] Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 502(a)-(b), 112 Stat. 2396.
[79] 50 U.S.C. § 1861(a)(1).

grants the agency authority to seize more than just business records by modifying the language to "any tangible things," which includes "books, records, papers, documents, and other items."[80]

Additionally, Section 215 relaxes the application requirements for a court order. Originally, the application had to contain "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." [81] However, an application for a court order under Section 215 requires only "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities..."[82] Thus, by granting the FBI enhanced authority to collect items, Section 215 plays a crucial role in the intelligence collection programs conducted by the federal agencies.

Section 214 under the USA PATRIOT Act also eases the application requirements for a court order to use pen register and trap and trace devices.[83] Essentially, Section 214 follows a similar certification process as the business records application for a court order under Section 215 and thus allows for more flexible use of the pen register and trap and trace devices by federal agencies.[84]

Section 206 allows for roving surveillance[85] and dispenses with the previous requirement of having to identify the target of surveillance when obtaining a court order.[86] Lastly, Section

---

[80] *Id.*
[81] Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 502(a)-(b), 112 Stat. 2396.
[82] 50 U.S.C. § 1861(b)(2).
[83] 50 U.S.C. § 1842.
[84] 50 U.S.C. § 1842(c)(2).
[85] *See* http://www.law.cornell.edu/wex/electronic_surveillance (defining a "roving wiretap [to] occur when a court grants a surveillance warrant without naming the communications carrier and other third parties involved in the tap. The FBI and intelligence gathering communities find these necessary because terrorists have the ability to change

6001 or the "lone wolf" provision modifies the definition of "agent of foreign power" to include any non-U.S. person who "engages in international terrorism or activities in preparation therefore."[87] This allows for surveillance of individuals who have no affiliation to a foreign power or entity, but still engage or prepare to engage in international terrorism.

Another main adjustment of the USA PATRIOT Act to FISA was changing the language to allow for electronic surveillance without collecting foreign intelligence as the primary purpose of the surveillance. In essence, the USA PATRIOT Act sought to replace the more restrictive primary purpose test with a more liberal test that would allow for surveillance to be obtained more easily. The Act did so by amending FISA's certification requirement so that only "a significant purpose" rather than "a purpose" of the surveillance be related to collecting foreign intelligence.[88] This modification to FISA resulted in expanding the government's ability to more easily obtain a surveillance order from FISC because the government did not need to demonstrate that foreign intelligence information collection was the "primary purpose" of the application. With the threshold lowered, the government could submit a surveillance application for other reasons so long as foreign intelligence information was a "significant purpose."

This modification was challenged in *In re Sealed Case No. 02-001*.[89] There, the government appealed a decision by the FISC which despite approving the government's application for surveillance, the court imposed certain restrictions in its order.[90] These restrictions were:

---

computers, email accounts, or cellular telephones quickly upon reading an order and learning that the government had tapped their device").

[86] 50 U.S.C. § 1805(c)(2)(B).

[87] 50 U.S.C. § 1801(b)(1)(C).

[88] 50 U.S.C. § 1804(a)(6)(B).

[89] *In re Sealed Case No. 02-001*, 310 F.3d 717 (FISA Ct. Rev. 2002). FISA also established an appellate court to review the FISA trial court's decisions. It is this Court of Review that reviewed the government's appeal of the FISA trial court's decision.

[90] *Id.* at 721.

> law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division [of the Department of Justice] shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives.[91]

The FISC's concern revolved around their belief that FISA erected a barrier or "wall" between the intelligence and law enforcement realms[92], which required the court to "approve applications for electronic surveillance only if the government's objective is not primarily directed toward criminal prosecution of the foreign agents for their foreign intelligence activity."[93] The FISC court of review, however, dismissed this concern by recognizing that because counterintelligence involves both intelligence collection and law enforcement tactics, a barrier or "wall" separating the two could prove harmful to intelligence collection as a whole and the ultimate goal of protecting against terrorist attacks.[94]

In addition, the FISC court of review rejected the "primary purpose" test established in *Truong* and applied by courts in subsequent cases.[95] The court reviewed the legislative history of the USA PATRIOT Act and found that "there is simply no question … that Congress was keenly aware that this amendment relaxed a requirement that the government show that its primary purpose was other than criminal prosecution."[96] The court went on to hold that "accordingly, the

---

[91] *Id.* at 720.
[92] The world of intelligence includes counterintelligence, which involves intelligence activities designed to thwart or oppose the actions of a hostile intelligence service. Counterintelligence contains law enforcement traits that requires the participation of law enforcement agencies to make arrests of any individuals suspected of committing espionage against the United States. For instance, pursuant to the National Security Act of 1947, the CIA is only allowed to conduct intelligence operations overseas. Because the agency does not have any authority to operate domestically, it must involve the FBI when pursuing counterintelligence leads in the United States.
[93] *Id.*
[94] *Id.* at 732-6.
[95] *Id.* at 735-6.
[96] *Id.* at 732.

Patriot Act amendments clearly disapprove the primary purpose test. And as a matter of straightforward logic, if a FISA application can be granted even if 'foreign intelligence' is only a significant - not a primary - purpose, another purpose can be primary. One other legitimate purpose that could exist is to prosecute a target for a foreign intelligence crime."[97] Thus, the court found that under the PATRIOT Act, an application for a surveillance order to FISC does not need to show that the primary purpose is not for criminal prosecution.[98]

Lastly, the court reviewed whether the application requirements for obtaining a surveillance order from FISC complied with the Fourth Amendment.[99] The court initially drew a comparison between FISA's procedures with Title III in order to demonstrate the legitimacy of FISA.[100] For instance, the court found that "in many significant respects the two statutes are equivalent" despite some differences in protection.[101] In addition, the court underscored the significant difference between ordinary criminal law and foreign intelligence crimes:

> The main purpose of ordinary criminal law is twofold: to punish the wrongdoer and to deter other persons in society from embarking on the same course. The government's concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity. As we discussed in the first section of this opinion, the criminal process is often used as part of an integrated effort to counter the malign efforts of a foreign power. Punishment of the terrorist or espionage agent is really a secondary objective; indeed, punishment of a terrorist is often a moot point.[102]

The court then used this distinction in weighing the government's interest against individual privacy interests and found that "FISA as amended is constitutional because the surveillances it authorizes are reasonable."[103]

---

[97] *Id*. at 734.
[98] *Id* at 736.
[99] *Id* at 736-8.
[100] *Id* at 737-742.
[101] *Id*. at 741.
[102] *Id*. at 744-5.
[103] *Id*. at 746.

## IV. Surveillance Programs

In December 2005, the *New York Times* revealed the existence of a warrantless surveillance program authorized by then President George W. Bush.[104] The article reported that "under a presidential order signed in 2002, the [NSA] intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years…"[105] The article noted that although warrants were still required for conducting surveillance on purely domestic calls, "the agency has been conducting some warrantless eavesdropping on people in the United States who are linked, even if indirectly, to suspected terrorists through the chain of phone numbers and e-mail addresses…"[106]

### A. Terrorist Surveillance Program

In response to the *New York Times* disclosure, then President Bush acknowledged the existence of the NSA program[107] and identified it as the Terrorist Surveillance Program ("TSP").[108] The Department of Justice ("DOJ") responded as well by issuing a legal opinion on the program that argued its legitimacy based on the President's inherent executive authority and statutory authorization via the Authorization for Use of Military Force ("AUMF").[109] Shortly after the September 11, 2001 terrorist attacks, Congress passed the AUMF, which provided the President with the authority to "use all necessary and appropriate force against those nations,

---

[104] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, December 16, 2005.
[105] *Id*.
[106] *Id*. *See also* James Risen and Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. Times, December 21, 2005. (reporting in a later article from the N.Y. Times that technical issues with the NSA program may have resulted in inadvertent interception of some domestic-to-domestic calls).
[107] President George W. Bush, President's Radio Address from The White House (December 17, 2005). http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html
[108] President George W. Bush, President Discusses Global War on Terror at Kansas State University (January 23, 2006), http://georgewbush-whitehouse.archives.gov/news/releases/2006/01/20060123-4.html
[109] *See* U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (2006).

organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks…"[110] The DOJ thus contended that "Congress in the AUMF gave its express approval to the military conflict against al Qaeda and its allies and thereby to the President's use of all traditional and accepted incidents of force in this current military conflict—including warrantless electronic surveillance to intercept enemy communications both at home and abroad."[111]

The constitutionality of the NSA program was challenged by the American Civil Liberties Union (ACLU) along with several other plaintiffs in a lawsuit against the agency. In *ACLU v. Nat'l Sec. Agency*, the district court found that the surveillance program violated not just the First and Fourth Amendments, but the separation of powers doctrine as well due to the lack of judicial authorization in conducting the surveillance as required under FISA.[112] The district court's decision, however, was vacated for lack of jurisdiction after an appeal by the NSA to the Sixth Circuit.[113]

In January 2007, then Attorney General Alberto Gonzalez announced the Bush administration's plans not to pursue the reauthorization of the TSP.[114] In addition, he indicated that electronic surveillance under the TSP would be reviewed by FISC.[115] However, later that same year, President Bush signed the Protect America Act of 2007 ("PAA"), which amended key provisions of FISA to allow for surveillance similar to TSP to be conducted.[116] The Act eliminated the requirement for a court order when conducting electronic surveillance so long as

---

[110] Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (Sept. 18, 2001).
[111] *See* U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (2006).
[112] *ACLU v. Nat'l Sec. Agency / Central Sec. Serv.*, 438 F. Supp. 2d 754, 773-8 (E.D. Mich. 2006).
[113] *ACLU v. NSA*, 493 F.3d 644, 647 (6th Cir. 2007). (holding that plaintiffs lacked standing for their claims).
[114] *See* Letter from Attorney General Alberto Gonzalez for Senator Patrick Leahy and Senator Arlen Specter (January 17, 2007) http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf
[115] *Id.*
[116] Protect America Act of 2007, Pub. L. No. 110–55, 121 Stat. 552.

the surveillance targets were "reasonably believed" to be located outside of the United States.[117] Additionally, the statute stripped FISC's authority in being the judicial arbiter for approving government surveillance applications by redirecting that power to the Director of National Intelligence ("DNI") and Attorney General ("AG").[118] Under the PAA, the DNI and AG were granted authority to approve surveillance requests from intelligence officers instead of FISC.[119] And in those instances when electronic surveillance without court order was authorized, the statute required notification to FISC within 72 hours of the authorized surveillance.[120] In essence, the PAA effectively weakened FISC's authority and removed the court from the process it was granted under FISA.

B. The Road to the Current Surveillance Programs

Due to a six month sunset provision, the PAA was slated to expire in 2008.[121] In 2008, however, Congress enacted the FISA Amendments Act of 2008 ("FAA"), which established a new Title VII that contained similar provisions to the PAA.[122] Specifically, Section 702 under Title VII establishes procedures for surveillance of non-U.S. persons and U.S. persons outside of the United States.[123] Like the PAA, Section 702 provides that "the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[124] However, there are limitations to that surveillance:

b) Limitations An acquisition authorized under subsection (a)—

[117] *Id.* at § 105B(a).
[118] *Id.* at § 105B(a)(1).
[119] *Id.* at § 105B(a).
[120] *Id.* at § 105B(a).
[121] *Id.* at § 105(c).
[122] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110–261, 122 Stat. 2436.
[123] 50 U.S.C. § 1881a.
[124] 50 U.S.C. § 1881a(a).

> (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
> (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
> (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
> (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
> (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.[125]

The certification procedure revolves around two scenarios. The first involves FISC granting a court order approving of a written certification and any supporting affidavit by the AG and the DNI.[126] The second scenario occurs when a court order has not been issued by FISC, but there are exigent circumstances which require the AG and DNI to authorize the surveillance of non-U.S. persons reasonably believed to be outside the United States.[127] The AG and DNI are then required to submit to FISC "a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made."[128] In addition, surveillance can be conducted prior to the submission of the certification.[129] Thus, the second scenario allows for surveillance without court order so long as exigent circumstances exist.

In response to the FAA's enactment, a group of attorneys and organizations filed a lawsuit against the government in July 2008 challenging the constitutionality of Title VII and arguing that the FAA violated the Fourth Amendment.[130] The plaintiffs contended that since their work involved electronically communicating "with colleagues, clients, journalistic sources, witnesses, experts, foreign government officials, and victims of human rights abuses located

---

[125] 50 U.S.C. § 1881a(b)(1)-(5).
[126] 50 U.S.C. § 1881a(a).
[127] 50 U.S.C. § 1881a(c)(2).
[128] 50 U.S.C. § 1881a(g)(1)(B).
[129] *Id*.
[130] Complaint, *Amnesty Int'l USA v. McConnell*, 646 F. Supp. 2d 633 (S.D.N.Y. 2009).

outside the United States," the FAA undermined their ability to adequately perform their duties and represent their clients.[131] Thus, the plaintiffs argued that the costs they incurred from having to protect their communications granted them standing to bring suit.[132]

The district court, however, disagreed and found that "plaintiffs have not shown that any specific action is threatened or contemplated against them because they have not shown that they are subject to the FAA."[133] Although the Second Circuit reversed the district court's judgment,[134] the U.S. Supreme Court ultimately held that the plaintiffs lacked standing and thus, did not reach the issue of whether the FAA violated the Fourth Amendment.[135]

C. Telephony Metadata Surveillance Program

In December 2012, President Obama extended Title VII of FISA for another five years until December 2017. Under his term, two NSA surveillance programs have been revealed: NSA collection of telephony metadata authorized under the auspices of Section 215 and PRISM. Regarding the former, London's *Guardian* newspaper reported in June 2013 that pursuant to a FISC order issued in April 2013 and set to expire in July 2013, the NSA has been collecting telephone records of Verizon customers in the United States.[136] Specifically, the FISC order compels Verizon to:

> "produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or 'telephony metadata' created by Verizon

[131] *Id.* at 2
[132] *Id.*
[133] *Amnesty Int'l USA v. McConnell*, 646 F. Supp. 2d 633, 655 (S.D.N.Y. 2009)
[134] *Amnesty Int'l USA v. Clapper*, 638 F.3d 118, 122 (2d Cir. 2011).
[135] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013).
[136] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian (Jun. 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

> communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[137]

It is noteworthy to mention that the order applies to the collection of telephony metadata, not substantive content.[138]

The NSA telephony metadata surveillance program appears to be authorized by Section 215's business records collection under the USA PATRIOT Act. Not only did Section 215 expand the language of business records to include "any tangible things," but it also relaxed the purpose requirement to allow for collection of "any tangible things" when "the records concerned are sought for an authorized investigation to obtain foreign intelligence information."[139] Thus, it can be argued that a broad reading of Section 215 allows for the NSA collection of telephony metadata since Congress approved of the modified language from business records to any tangible things, which includes "books, records, papers, documents, and other items."[140] Although telephony metadata is not explicitly listed, the inclusion of "other items" as part of "any tangible things" is wide enough language that the collection of telephony metadata is within the reach of the statute.[141]

---

[137] *See In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. D/B/A Verizon Business Services,*, http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order

[138] *See In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, etc.*, http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf (defining telephony metadata for purposes of FISC court order to include "comprehensive communications, routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity Number (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, financial information of a subscriber or customer. Similarly, e-mail metadata includes the e-mail addresses of senders and receivers of e-mails.

[139] 50 U.S.C. § 1861(a)(1).

[140] *Id.*

[141] *See* Noah Feldman, *The Secret Law Behind NSA's Verizon Snooping*, Bloomberg News (Jun. 6, 2013, 11:44 AM), http://www.bloomberg.com/news/2013-06-06/the-secret-law-behind-nsa-s-verizon-snooping.html. (noting that FISC's reading of the statute may be correct).

In *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, etc.*, FISC examined the issue of the FBI's collection of telephony metadata under Section 215 and determined not only that the surveillance applications complied with the Fourth Amendment, but also that the requests were "lawful and required" under the statute.[142] There, FISC initially underwent a Fourth Amendment analysis and established that "the production of telephone service provider metadata is squarely controlled by the U.S. Supreme Court decision in *Smith v. Maryland*.[143] FISC then underscored the importance of the FBI's surveillance application requesting "daily production of certain telephony metadata in bulk belonging to companies without specifying the particular number of an individual."[144] FISC found that because there was no legitimate expectation of privacy in such information maintained by telephone companies as held by *Smith*, Fourth Amendment protection did not apply to the FBI surveillance requests.[145] In addition, FISC noted that without the presence of an individualized Fourth Amendment interest, "grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*.[146]

FISC then analyzed the FBI's surveillance application under Section 215 of the USA PATRIOT Act.[147] The court found that the statutory provisions "are designed to ensure not only that the government has access to the information it needs for authorized investigations, but also that there are protections and prohibitions in place to safeguard U.S. person information."[148]

---

[142] *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, etc.*, No. 13-109 at 3 (FISA Ct. 2013).
[143] *Id.* at 8.
[144] *Id.*
[145] *Id.* at 9.
[146] *Id.*
[147] *Id.*
[148] *Id.* at 9-10. (underscoring the protections under the statute, including First Amendment protection, the executive branch approval via the Attorney General; and minimization procedures).

Additionally, FISC compared Section 215 with Section 2703(d) of the SCA and noted Congress' intent to enact two statutes dealing with the same subject, but having distinct purposes; while Section 215's purpose is foreign intelligence information, Section 2703(d)'s purpose is criminal investigation.[149]

The court also reviewed the government's burden under Section 215, which requires "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant…"[150] FISC found that because "international terrorist operatives are using telephone communications and … it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations", the government has met the statutory burden under Section 215 to obtain records.[151] FISC's opinion thus establishes both constitutional and statutory legitimacy of the government agency programs collecting telephone metadata.

D. PRISM

In June 2013, the *Washington Post* reported the existence of a data-mining program by the FBI and NSA, code-named PRISM.[152] Unlike the telephony metadata collection program, PRISM is alleged to be obtaining content-based communications.[153] Based on classified information leaked by former CIA employee and NSA contractor Edward Snowden, the *Washington Post* revealed that the two agencies have been "tapping directly into the central

---

[149] *Id.* at 16-7
[150] *Id.* at 18
[151] *Id.* at 22-3
[152] Barton Gellman and Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, Washington Post (Jun. 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1 (last updated Jun. 7, 2013).
[153] *Id.*

servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets."[154]

Although the companies have denied allegations of granting the government direct, unfettered access to their servers, they have acknowledged their compliance in responding to individual court orders under FISA and establishing an efficient data sharing system with the government.[155] Slide FAA 702 of the leaked PRISM program documents indicates that there are two types of collection programs: upstream and downstream, such as PRISM.[156] While the former suggests that there are parasitic surveillance programs collecting communications "as data flows past," the latter shows that "the NSA is receiving data sent to them deliberately by the tech companies, as opposed to intercepting communications as they're transmitted to some other destination."[157] Thus, PRISM and other downstream programs allow the NSA to obtain data from the major tech companies in a mechanical and formalized way rather than directly tapping into the servers and collecting information.[158]

The NSA's surveillance program is governed by Section 702 of the FAA, which allows the AG and DNI to authorize "targeting of persons reasonably believed to be located outside the United States."[159] Surveillance of U.S. persons therefore cannot be intentionally conducted under 702(b)'s limitations.[160] However, the *Washington Post* reported that under the program, analysts input search terms "that are designed to produce at least 51 percent confidence in a

---

[154] *Id.* The companies included Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.
[155] Claire Cain Miller, *Tech Companies Concede to Surveillance Program*, N.Y. Times (Jun. 7, 2013) http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?_r=0
[156] NSA Prism program slides, The Guardian (Nov. 1, 2013) http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document
[157] *Id. See also* Timothy B. Lee, Here's everything we know about PRISM to date, Washington Post (Jun. 12, 2013) http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/
[158] *Id.*
[159] 50 U.S.C. § 1881a(a).
[160] 50 U.S.C. § 1881a(b)(1)-(5).

target's 'foreignness.'"[161] Concluding that it is "not a very stringent test," the newspaper further reported that incidental collection of American content is difficult to avoid since targeting a foreign suspect requires communications from all persons in the suspect's inbox or outbox to be collected.[162] Known as contact chaining, "intelligence analysts are typically taught to chain through contacts two 'hops' out from their target, which increases 'incidental collection' exponentially."[163] In essence, although American content cannot be intentionally targeted by the NSA, there is a possibility that such information can be collected.

Despite the incidental collection of U.S. content, the NSA's activities appear to be legally valid under Section 702. As an initial matter, it is important to note that the probable cause standard for national security investigations is less stringent than that for criminal investigations. Not only did the USA PATRIOT Act further relax the language so that foreign intelligence be only a "significant purpose" rather than the primary purpose for FISC surveillance orders, but the orders themselves are not considered warrants. Moreover, Section 702 requires that the certification, targeting, and minimization procedures be met and the surveillance be conducted in a manner consistent with the Fourth Amendment before FISC will grant an order approving the surveillance. In addition, the requirement that deficiencies in any of the procedures be corrected within a certain time demonstrates the role that FISC plays as judiciary in overseeing the activities authorized by Section 702. For instance, Section 702(i)(3)(B) states that:

> If the Court finds that a certification submitted in accordance with subsection (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United

---

[161] Barton Gellman and Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, Washington Post (Jun. 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1 (last updated Jun. 7, 2013).
[162] *Id.*
[163] *Id.*

> States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order—
>
> (i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or
>
> (ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.[164]

Two FISC opinions issued in October and November 2011 demonstrate the significant role played by the judiciary in overseeing the NSA's surveillance activities under Section 702.[165] The FISC opinion from October 3, 2011 examined one of the NSA's upstream surveillance programs collecting Internet communications.[166] The opinion shows that FISC was not completely aware of what and how much information the NSA had been acquiring as part of its Internet communications collection.[167] FISC stated:

> Based on the government's prior representations, the Court has previously analyzed NSA's targeting and minimization procedures only in the context of NSA acquiring discrete communications. Now, however, in light of the government's revelations as to the manner in which NSA acquires Internet communications, it is clear that NSA acquires "Internet transactions,"[168] including transactions that contain a single discrete communication ("Single Communication Transactions" or "SCTs"), and transactions that contain multiple discrete communications ("Multi-[C]ommunication Transactions" or "MCTs")… [F]or the first time, the government has now advised the Court that the volume and nature of the information it has been collecting is fundamentally different from what the Court has been led to believe. [169]

In response to the revelation, FISC underscored the importance of needing to examine the "government's targeting and minimization procedures … in light of the communications actually

---

[164] 50 U.S.C. § 1881a(i)(3)(B).

[165] Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates) (FISA Ct. 2011) Oct. 3, 2011; Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates) (FISA Ct. 2011) Nov. 30, 2011.

[166] Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates) (FISA Ct.) Oct. 3, 2011. It is important to note that FISC distinguishes the upstream program at issue in the opinion from NSA's downstream PRISM collection by stating that "the Court understands that NSA does not acquire Internet transactions through its PRISM collection." (internal quotations omitted) at 29 (FISA Ct. 2011).

[167] *Id.*

[168] *Id.* at 28. There is a footnote in the opinion that provides the government description of an "Internet transaction as a complement of packets traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device." (internal quotations omitted)

[169] *Id.* at 27-8.

acquired."[170] Specifically, FISC reviewed whether the NSA's collection of Internet transactions complied with the targeting and minimization procedures required by the statute and the Fourth Amendment.[171] Although FISC determined that the targeting procedures were in compliance, the court found that the minimization procedures failed to meet the standard established by statute.[172] FISC also found that both targeting and minimization procedures did not satisfy the Fourth Amendment.[173]

FISC separated the minimization procedures analysis into acquisition, retention, and dissemination of collected information.[174] Regarding acquisition, FISC determined that despite the NSA's acquisition of "non-target communications, which are highly unlikely to have foreign intelligence value," the agency lacked the technical capability to "limit its collection only to the relevant portion or portions of each MCT – i.e., the particular discrete communications that are to, from, or about a targeted selector."[175] FISC thus found that this portion of the NSA's minimization procedures complied with the statute's requirements.[176]

FISC next focused on retention and the NSA's proposed procedures after its acquisition of MCTs.[177] FISC expressed concerns that "the measures proposed by the government for MCTs … largely dispense with the requirement of prompt disposition upon initial review by an analyst [and] NSA's proposed handling of MCTs tends to maximize the retention of such information, including information of or concerning United States persons with no direct

---

[170] *Id.* at 28.
[171] *Id.*
[172] *Id.* at 29.
[173] *Id.*
[174] *Id.* at 56, 59, 63.
[175] *Id.* at 56-7. The court also undergoes an analysis of SCTs in its opinion, but determines that that incidental domestic collection of SCTs does not "raise the same minimization-related concerns." FISC notes that such collection is "reasonably likely to contain foreign intelligence information" and references a previous order that satisfied the foreign power probable cause requirement.
[176] In a footnote, FISC emphasizes the importance of the NSA to "enhance its capability to limit acquisitions only to targeted communications."
[177] *Id.* at 59.

connection to any target."[178] Specifically, FISC highlighted three areas for improvement: 1.) limiting the access to domestic MCTs to a smaller group of NSA personnel who are specially trained in handling such information; 2.) requiring personnel to indicate that the MCT contains domestic information; and 3.) reducing the retention period from five years.[179]

Initially noting that "FISA imposes a stricter standard for dissemination than for acquisition or retention", FISC reviewed the government's dissemination measures ranging from destruction of domestic MCTs to the limitation preventing dissemination by the NSA of domestic MCTs.[180] The court found that despite the possibility of information concerning United States persons being inadvertently collected, the proposed dissemination procedures satisfied the requirements of the statute.[181]

Regarding the Fourth Amendment, FISC acknowledged that acquisition of electronic communications can constitute a "search" or "seizure" within the meaning of the Fourth Amendment.[182] In examining whether the NSA's targeting and minimization procedures were in violation of the warrant clause of the Fourth Amendment, the court determined that the NSA's upstream intelligence activities under Section 702 "fall within the 'foreign intelligence exception' to the warrant requirement of the Fourth Amendment."[183]

FISC then underwent a reasonableness analysis that involved considering the "nature of the government intrusion and how the government intrusion is implemented."[184] The court noted that it was required to balance the interests at stake and consider the "totality of the

---

[178] *Id.*
[179] *Id.* at 61-2.
[180] *Id.* at 63.
[181] *Id.* at 65-7. Similar to the targeting procedures analysis, the court noted the NSA's technology limitations separating the relevant information in the MCT.
[182] *Id.* at 67.
[183] *Id.* at 68.
[184] *Id.* at 69.

circumstances" as part of its balancing test.[185] FISC found that although the "government's national security interest in conducting acquisitions pursuant to Section 702 is of the highest order of magnitude … the NSA's acquisition of MCTs substantially broadens the circumstances in which Fourth Amendment-protected interests are intruded upon by NSA's Section 702 collection.[186]

The court then underscored the significance of the minimization procedures in its Fourth Amendment analysis.[187] FISC found that due to the deficiencies in the procedures that "seem to enhance, rather than reduce, the risk of error, overretention, and dissemination of non-target information, including information protected by the Fourth Amendment," the NSA's targeting and minimization procedures pertaining to the upstream collection violated the Fourth Amendment.[188]

In response to FISC's October 3, 2011 opinion finding constitutional and statutory deficiencies in the NSA's upstream surveillance program, the government made adjustments that specifically addressed those issues and submitted another application for court approval.[189] The court issued an opinion on November 30, 2011 and found that the "government has adequately corrected the deficiencies identified in the October 3 Opinion, and the request for approval is therefore granted."[190] Thus, taken together, the FISC opinions demonstrate how the judicial oversight process by FISC is sufficient in monitoring the federal agencies' surveillance activities and fixing any problems that exist.

---

[185] *Id.* at 70.
[186] *Id.* at 70-2.
[187] *Id.* at 77.
[188] *Id.* at 78-9.
[189] Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates), at 2 (FISA Ct. 2011) Nov. 30, 2011.
[190] *Id.*

## V. Conclusion

This article examined the constitutional framework of cases determining what kind of surveillance constitutes a search within the meaning of the Fourth Amendment. It also reviewed the statutory framework not only governing the surveillance activities being conducted today, but also distinguishing surveillance conducted for criminal and national security purposes. In conclusion, unless the Supreme Court undergoes a Fourth Amendment analysis to determine the constitutionality of the current FBI and NSA programs, the government's surveillance activities are legally valid under Section 215 of the USA PATRIOT Act and Section 702 of the FAA. In other words, as long as the issue of whether the surveillance activities constitute a search within the meaning of the Fourth Amendment and thus require a warrant remains open, a statutory analysis will have to suffice to determine the FBI and NSA programs' legal legitimacy.

The above statutory analysis demonstrates that the agencies' collection of metadata complies with Section 215 since metadata can qualify as "any tangible things" under a broad interpretation. In addition, so long as NSA programs like PRISM comply with the certification, targeting, and minimization procedures, inadvertent collection of U.S. content is lawful under Section 702. NSA's adherence to the procedures is evident in the FISC opinions from October and November 2011.

Lastly, the materials on the DNI website demonstrate a proper response by the government in addressing the unauthorized leaks and disclosures from this year. They also provide sufficient declassified information that when taken as a whole, establishes the legal validity of the current surveillance programs. Thus, although critics argue that these programs are in constitutional violation of the Fourth Amendment, the government's surveillance activities will likely continue until the Supreme Court hears the matter and decides otherwise. The trend

towards finding privacy expectations despite advancements in technology indicated in Part II's constitutional framework may shed some light on how the Supreme Court will rule.