I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

STEPHEN MANUEL WOLFSON*

# The NSA, AT&T, and the Secrets of Room 641A

**Abstract:** This note discusses the possible existence of a domestic surveillance/data collection program conducted by the National Security Agency ("NSA") with the assistance of AT&T, and the implications of such a program under the Electronic Communications Privacy Act ("ECPA"). This article first examines a May 11, 2006 USA Today article reporting that the NSA was given access to a huge number of call records from AT&T. Next, it turns to the story of former AT&T technician Mark Klein and the Electronic Frontier Foundation's ("EFF") case, *Hepting v. AT&T Corporation*. Klein claims that the NSA has built a "secret room" in AT&T's San Francisco switching center that grants the agency access to a vast amount of customer information. In *Hepting*, the EFF alleges that AT&T violated the Stored Communications Act, Title II of the ECPA; the Wiretap Act, Title I of the ECPA; and the Pen Register Statute, Title III of the ECPA. Finally, this article addresses the Protect America Act of 2007 and provides analysis of expert opinions in the field.

* Author is a J.D. candidate at The Ohio State University Moritz College of Law (expected 2008).

## I. INTRODUCTION: MAY 11, 2006

On May 11, 2006, USA Today published an article reporting that AT&T, Verizon, and Bellsouth had been providing the NSA with the telephone records of "tens of millions of Americans" since shortly after September 11, 2001.[1] Called "the largest database ever assembled in the world" by the newspaper's source, its purported goal was to "'create a database of every call ever made' within the nation's borders."[2]

Supposedly, this program did not listen to or record conversations. Instead, it collected customer "call-detail records" ("CDRs") from the telecommunication companies ("telecos").[3] Ordinarily, CDRs contain information such as the parties to a call, duration, and billing period, not records of conversations.[4] According to USA Today's source, the CDRs received by the NSA through this program contained only telephone numbers: names, addresses, and other personal information were not included.[5]

Although it was not implicated in the story, Qwest, a teleco that operates primarily in the West and Northwest, quickly stated that it had not participated in the NSA program.[6] Shortly thereafter, both

---

[1] Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[2] *Id.*

[3] *Id.*

[4] Declan McCullagh & Anne Broache, *FAQ: NSA's Data Mining Explained*, CNET NEWS.COM, May 12, 2006, http://news.com.com/FAQ+NSAs+data+mining+explained/2100-1028_3-6071780.html?tag=st.prev. *See also* Call Detail Records (CDR), http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t2/cdrfm.htm#wp8482 (last visited Jan. 23, 2008); What is a Call Detail Record?, http://searchvoip.techtarget.com/sDefinition/0,,sid66_gci1032982,00.html (last visited Jan. 23, 2008). For an example of the information collected in CDRs, *see* Call Data Records, http://www.csoft.co.uk/reports/cdr1.htm (last visited Jan. 23, 2008).

[5] Cauley, *supra* note 1. It should be noted that the NSA may still be receiving conversation records from another source. In August 1999, the agency patented a system for extracting data from computer-generated text such as a call records. *See* McCullagh & Broache, *supra* note 4.

[6] Cauley, *supra* note 1 ("Qwest provides local phone service to 14 million customers in 14 states in the West and Northwest."). Since AT&T and Verizon provide some services to people in Qwest's region, the NSA may have obtained CDRs this area. *Id.*

BellSouth and Verizon also denied involvement.[7] BellSouth demanded that USA Today state for the record that it had not been involved with the NSA.[8] Eventually, on June 30, 2006, USA Today withdrew the story as it applied to Verizon and BellSouth.[9] At the same time, however, the newspaper reaffirmed the existence of some domestic data-collection program, even if BellSouth and Verizon were not associated with the program. USA Today reported that Congressional Intelligence Committee members had confirmed the existence of an NSA data-collection program and that AT&T was involved.[10] Unlike BellSouth and Verizon, AT&T neither confirmed nor denied assisting the NSA, asserting that the U.S. Department of Justice said discussing the program would harm national security.[11]

President Bush acknowledged the NSA program shortly after the story broke. In a statement similar to one he made in December 2005,[12] the President said he had authorized the NSA to "intercept international communications of people with known links to al Qaeda and related terrorist organizations."[13] The President made three important points: first, the program specifically targeted members of al Qaeda and was not random data-collection; second, it did not involve listening to domestic calls without court approval; and third, it was legal and that members of Congress knew about the program. According to President Bush, the government was "not mining or

---

[7] *BellSouth Denies Giving Records to NSA*, May 15, 2006, CNN.COM, http://www.cnn.com/2006/POLITICS/05/15/bellsouth.nsa. *See also* Jim Drinkard, *Verizon Says it Isn't Giving Call Records to NSA*, USA TODAY, May 16, 2006, http://www.usatoday.com/news/washington/2006-05-16-verizon-nsa_x.htm.

[8] Jim Drinkard, *BellSouth Calls for a Retraction of Report it Cooperated with NSA*, USA TODAY, May 18, 2006, http://www.usatoday.com/news/washington/2006-05-18-bellsouth-nsa_x.htm.

[9] Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY, June 30, 2006, http://www.usatoday.com/news/washington/2006-06-30-nsa_x.htm.

[10] *Id.* ("Five members of the intelligence committees said they were told by senior intelligence officials that AT&T participated in the NSA domestic calls program.").

[11] *Id.*

[12] Press Release, President George W. Bush, Press Conference of the President (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html.

[13] Press Release, President George W. Bush, President Bush Discusses NSA Surveillance Program (May 11, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/05/20060511-1.html.

trolling through the personal lives of millions of innocent Americans."[14]

Soon after the President's statement, Massachusetts Representative Ed Markey asked the Federal Communications Commission ("FCC") to address and investigate the claims against the NSA program.[15] Initially, FCC Commissioner Michael J. Copps called for an inquiry into whether the NSA program violated § 222 of the Communications Act,[16] which prohibits telephone companies from divulging information concerning customer calling habits. The FCC "can levy fines of up to $130,000 per day, per violation, with a cap of $1.325 million per violation" of this law.[17]

After briefly considering the matter, the FCC halted its inquiry. The agency decided it could not explore the issue further because the United States government had invoked the state secrets privilege in the related case, *Hepting v. AT&T*.[18] Fearing that it might breach the privilege, the FCC chose not to investigate further.[19]

## II. MARK KLEIN AND *HEPTING V. AT&T*

The USA Today article was not the first NSA/AT&T data-collection story of 2006; when it broke, Mark Klein's story about secret room 641A was already public and *Hepting v. AT&T* was being litigated.

---

[14] *Id.*

[15] Letter from Representative Edward Markey, Seventh District of Georgia, to Kevin Martin, Chairman of the FCC (May 15, 2006), *available at* http://markey.house.gov/docs/telecomm/iss_telecom_ltr060515.pdf.

[16] Press Release, FCC, Comm'r Michael J. Copps Calls for the FCC to Open an Inquiry into the Lawfulness of the Disclosure of America's Phone Records (May 15, 2006), *available at* http://hraunfoss.fcc.gov/edocs_public/ attachmatch/DOC-265373A1.pdf.

[17] Cauley, *supra* note 1.

[18] Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006).

[19] Letter from Kevin Martin, Chairman, FCC, to Representative Edward Markey, Seventh District of Georgia (May 22, 2006), *available at* http://markey.house.gov/docs/privacy/iss_telecom_resp060522.pdf. The state secrets doctrine is discussed *infra* in footnotes 164–83 and accompanying text.

In April 2006, Wired News reported that AT&T had built a "secret room" ("641A")[20] in its San Francisco switching center that gave the NSA direct access to the phone calls and internet usage records of its customers.[21] Mark Klein, a former AT&T technician, witnessed 641A being built adjacent to the call routing room when he toured the switching center in January 2003.[22] However, he was unable to see inside; the NSA conducted interviews before granting access to work in Room 641A and regular technicians were not allowed to enter.[23]

In October 2003, Klein was transferred to AT&T's San Francisco office. At his new position, he learned more about 641A, including the facts that fiber optic cables from 641A tapped directly into the AT&T WorldNet circuits and that a Narus STA 6400 had been installed on the line.[24] The STA 6400 analyzes calls in real-time, connecting directly to the phone line or Internet Service Provider ("ISP"), and is commonly used by government intelligence agencies because of its ability to sort though vast amounts of data.[25] Klein also

---

[20] Mark Klein, AT&T'S IMPLEMENTATION OF NSA SPYING ON AMERICAN CITIZENS, 3 (Dec. 31, 2005), *available at* http://blog.wired.com/27BStroke6/att_klein_wired.pdf.

[21] Ryan Singel, *Whistle-Blower Outs NSA Spy Room*, WIRED NEWS, April 7, 2006, http://www.wired.com/science/discoveries/news/2006/04/70619. A switching center is "a facility in which switches are used to interconnect communications circuits on a circuit-, message-, or packet-switching basis." Federal Standard 1037C: Glossary of Telecommunications Terms, http://www.its.bldrdoc.gov/fs-1037 (last visited Jan. 23, 2008).

[22] *Id.*

[23] *Id.*

[24] *Id.* WorldNet is AT&T's Internet Service Program.

[25] *Id. See also* NarusInsight Intercept Suite, http://www.narus.com/products/intercept.html (last visited Jan. 23, 2008). Based in Mountain View, California, Narus calls itself "the leader in providing the real-time traffic insight essential to profitably manage, secure and deliver Services over IP." About Narus, http://www.narus.com/about/index.html (last visited Jan. 23, 2008). The STA (Semantic Traffic Analyzer) 6400 is a computer program that has the ability to inspect communications traffic in real-time. A communication company can install an analyzer at the entrance and exit points of their networks which then communicate with specialized computer programs. Together, the STA 6400 "can keep track of, analyze and record nearly every form of internet communication, whether email, instant message, video streams or VOIP phone calls that cross the network." Robert Poe, *The Ultimate Net Monitoring Tool,* WIRED NEWS, May 17, 2006, http://www.wired.com/science/discoveries/news/2006/05/70914.

learned that similar splitter systems were being installed in other cities such as Seattle, San Jose, Los Angeles, and San Diego.[26]

Shortly before his story went public, Klein submitted a declaration in support of *Hepting v. AT&T*, the class action suit filed by the EFF on behalf of several AT&T customers. The plaintiffs claimed that AT&T had violated federal electronic surveillance laws by cooperating with the NSA.[27]

*Hepting* arose as a result of December 2005 reports alleging that President Bush authorized the NSA to conduct warrantless surveillance inside the United States.[28] The New York Times wrote that the president issued an order in 2002 permitting the National Security Agency to monitor international phone calls and email messages without court approval.[29] Historically, the NSA's central mission consisted of the collection of foreign signals intelligence ("SIGINT"),[30] not conducting domestic surveillance.[31] However, the president said that he only "authorized the interception of international communications of people with known links to al Qaeda and related terrorist organizations."[32] Similarly, Attorney General ("AG") Alberto Gonzales stated that the program was specifically targeted at communications where one party was outside the United States.[33] According to The New York Times, at the time of the president's and

---

[26] Poe, *supra* note 25. For a visual depiction of the NSA data monitoring facilities, see The NSA Surveillance Octopus, http://www.nsawatch.org/nsa_octopus.jpg (last visited Jan. 23, 2008).

[27] Complaint, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006), *available at* http://www.eff.org/files/filenode/att/att-complaint.pdf [hereinafter *Complaint*].

[28] *Id.* at 2. *See also* James Risen & Eric Lichtenblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?ei=5090&en=e32072d786623ac1&ex=1292389200.

[29] *Id.*

[30] National Security Agency, Signals Intelligence, http://www.nsa.gov/sigint/index.cfm (last visited Jan. 23, 2008).

[31] Risen & Lichtenblau, *supra* note 28.

[32] Press Release, President George W. Bush, Press Conference of the President, *supra* note 12.

[33] Press Release, Att'y Gen. Alberto Gonzales, Press Briefing by Att'y Gen. Alberto Gonzales and General Michael Hayden, Principal Deputy Dir. for Nat'l Intelligence (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

the AG's statements, the NSA still obtained warrants for entirely domestic communications.[34]

Following The New York Times story and the subsequent qualified admissions by the president and the attorney general, the EFF filed suit in the Federal District Court for the Northern District of California.[35] The EFF alleged that AT&T improperly granted the NSA access to at least two enormous call record databases, thereby violating several federal laws including the ECPA.[36] The "Hawkeye,"[37] one of the databases the NSA was given access to, contains up to 312 terabytes of information.[38] Accordingly, the EFF alleged AT&T had improperly given this incredible amount of account information to the government without the consent or knowledge of its customers.

In total, the EFF made seven claims against AT&T.[39] The most important claims include allegations that AT&T violated the Stored Communications Act, the Electronic Communications Privacy Act, and the Pen Register Statute.[40]

## III. THE STORED COMMUNICATIONS ACT

One claim made in *Hepting* alleged that AT&T violated the Stored Communications Act ("SCA") by giving both CDRs and

---

[34] Risen & Lichtenblau, *supra* note 28.

[35] *Complaint*, *supra* note 27.

[36] *Id.* at 8–9

[37] AT&T, Daytona, http://www.research.att.com/~daytona/inuse.php (last visited Jan. 23, 2008).

[38] One terabyte = 1,048,576 megabytes or 1,024 gigabytes. Terabyte Computers, *What is a "Terabyte" Anyway?*, http://www.terabyte.net/terabyte.htm (last visited Jan. 23, 2008).

[39] Amended Complaint for Damages, Declaratory and Injunctive Relief at 1, 2, Hepting v. AT&T, 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. C-06-0672-JCS), *available at* http://www.eff.org/legal/cases/att/att_complaint_amended.pdf [hereinafter *Amended Complaint*]. The total list of claims that the EFF made is: (1) A violation of the First and Fourth Amendments to the U.S. Constitution; (2) Electronic surveillance in violation of 50 U.S.C. § 1809; (3) A violation of 18 U.S.C. § 2511; (4) Use of communications in violations of 47 U.S.C. § 605; (5) Divulging communications in violation of 18 U.S.C. §§ 2702(a)(1) and/or (a)(2); (6) Divulging communications records in violations of 18 U.S.C. § 2702(a)(3); and (7) Deceptive business practices. *Id.*

[40] 18 U.S.C. §§ 2702(a)(1), 2702(a)(2), 2702(a)(3).

communication content records to the NSA.[41] The SCA was enacted in 1986 as Title II of the Electronic Communications Privacy Act,[42] and provides "protections for wire and electronic communications retained in computer storage facilities."[43] As its name suggests, the SCA pertains to stored (meaning not in-transit/real-time) electronic communications, including CDRs.[44] Both the NSA and AT&T could be liable under this Act because the SCA applies to both government and private parties.[45]

Sections 2702 and 2703 are "the heart of the SCA."[46] Section 2702 details when a service provider can and cannot *voluntarily* disclose stored communications records.[47] Generally, this section prohibits telecommunications service providers from giving stored call records to "any governmental entity."[48] However, there are several exceptions, such as: when the information is going to its "addressee or intended recipient"[49]; when consent has been given[50]; and when the National Center for Missing and Exploited Children requires the information.[51] Notably, the statute provides an exception "to a law enforcement agency (A) if the contents – (i) were inadvertently

---

[41] *Amended Complaint*, *supra* note 39, at 23.

[42] 18 U.S.C. §§ 2701–2711 (2000 & Supp. V 2005).

[43] Michael D. Roundy, Note, *Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communications Following* United States v. Councilman's *Rejection of the Storage/Transit Dichotomy*, 28 W. NEW ENG. L. REV. 403, 413 (2006). *See also A Thinly Veiled Request for Congressional Action on E-Mail Privacy:* United States v. Councilman, 19 HARV. J. L. & TECH. 211, 214 (2005).

[44] Daniel J. Solove, *Reshaping the Framework: Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1283 (2004).

[45] Myrna L. Wigod, *Privacy in Public and Private E-Mail and On-Line Systems*, 19 PACE L. REV. 95, 113 (1998).

[46] 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, 1218 (2004), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860.

[47] *Id.* at 1220.

[48] 18 U.S.C. § 2702(a)(3) (Supp. V 2005).

[49] 18 U.S.C. § 2702(b)(1) (2000).

[50] § 2702(b)(3).

[51] § 2702(b)(6).

obtained by the service provider" and "(ii) appear to pertain to the commission of a crime"[52]; or "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[53]

Under § 2703, a telephone service provider may be *required* to turn over call records under certain circumstances. To compel disclosure of content records that are less than 180 days old, the government must obtain a search warrant.[54] For records older than 180 days, the government can obtain a search warrant,[55] use an "administrative subpoena,"[56] or obtain a court order pursuant to 18 U.S.C. § 2703(d).[57] Notice is required for the latter two methods.[58]

For non-content records such as CDRs,[59] § 2703 provides five ways that the government can *require* an electronic communications service provider to disclose this information: (1) by obtaining a warrant; (2) by obtaining a court order; (3) by obtaining customer consent; (4) by a formal government request for a telemarketing fraud investigation; and (5) by using an administrative subpoena.[60]

---

[52] § 2702(b)(7).

[53] § 2702(b)(8).

[54] 18 U.S.C. § 2703(a) (Supp. V 2005).

[55] § 2703(b)(1)(A).

[56] § 2703(b)(1)(B)(i). "Administrative subpoena authority . . . is the power vested in various administrative agencies to compel testimony or the production of documents or both in aid of the agencies' performance of their duties." CHARLES DOYLE, ADMINISTRATIVE SUBPOENAS AND NATIONAL SECURITY LETTERS IN CRIMINAL AND FOREIGN INTELLIGENCE INVESTIGATIONS: BACKGROUND AND PROPOSED ADJUSTMENTS, 1 (2005), *available at* http://www.fas.org/sgp/crs/natsec/RL32880.pdf.

[57] § 2703(b)(1)(B)(ii). The court order required is found in § 2703(d) and is "something like a mix between a subpoena and a search warrant." Kerr, *supra* note 46, at 1219.

[58] § 2703(b)(1)(B).

[59] "These records are sometimes known as 'basic subscriber information' because they mostly involve information about the subscriber's identity." Generally, this information includes: name, address, session times and durations, and length of service. Kerr, *supra* note 46, at 1219.

[60] Peter Swire & Judd Legum, *Telecos Could be Liable for Tens of Billions of Dollars for Illegally Turning Over Phone Records*, http://thinkprogress.org/2006/05/11/telcos-liable (last visited Jan. 23, 2008). *See also* 18 U.S.C. § 2703(c)(1)(A)–(E) (Supp. V 2005).

The first four exceptions clearly do not apply in the NSA/AT&T situation. No warrants or court orders were obtained, the program was conducted in secrecy without consulting customers, and the government is not investigating telemarketing fraud. "As for administrative subpoenas, where a government agency asks for records without court approval, there is a simple answer–the NSA has no administrative subpoena authority, and it is the NSA that reportedly received the phone records."[61]

The SCA draws two significant distinctions in §§ 2702 and 2703. First, because CDRs generally contain less private information, they are less protected and require less strenuous efforts to obtain than content records.[62] Second, the SCA applies to stored communications and not to communications as they occur.[63] Real-time/in-transit communications are protected by other sections of the ECPA: the Wiretap Act[64] and the Pen Register Statute.[65] Nevertheless, "[b]ecause the Wiretap Act requires the government to obtain a 'super' search warrant rather than the usual warrant required by the SCA, law enforcement agents have an incentive to try to do prospective surveillance normally undertaken under the Wiretap Act using the retrospective authority of the SCA."[66]

Section 2707 provides a cause of action to any electronic communication service provider, subscriber, or other person who is "aggrieved" by a violation of the SCA.[67] Relief may include preliminary or "other equitable or declaratory relief as may be appropriate," damages, and even attorney's fees and litigation costs.[68] Moreover, "the court may assess as damages . . . the actual damages suffered by the plaintiff and any profits made by the violator . . . but in no case shall a person entitled to recover receive less than the sum of

---

[61] *See id.*

[62] Solove, *supra* note 44, at 1283.

[63] *Id.*

[64] 18 U.S.C. §§ 2511–2522 (2000 & Supp. V 2005).

[65] 18 U.S.C. §§ 3121–3127 (2000 & Supp. V 2005).

[66] Kerr, *supra* note 46, at 1232. The Wiretap Act is discussed *infra* in footnotes 71–114 and accompanying text.

[67] 18 U.S.C. § 2707(a) (Supp. V 2005). *See also* Swire & Legum, *supra* note 60.

[68] § 2707(b)(1)–(3).

$1,000."[69] Accordingly, with potentially millions of CDRs given to the NSA, the penalties against AT&T or any other teleco that participated in the data-collection program could range in the billions of dollars.[70]

## IV. THE HISTORY AND ADVENT OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The roots of the Electronic Communications Privacy Act of 1986 lie in the Supreme Court's Fourth Amendment jurisprudence. In the early days of the country, the Supreme Court did not use the Fourth Amendment to protect an individual's privacy rights.[71] Then, in 1886 the Court suggested in *Boyd v. United States* that the Fourth Amendment might extend beyond physical invasions of property.[72] However, nearly forty years after *Boyd*, the Court refused to extend the protections of the Amendment in *Olmstead v. United States*.[73] *Olmstead* held that there must be a physical trespass to run afoul of the Fourth Amendment[74]; tapping a person's telephone from outside the house was not an unreasonable search and seizure.[75]

Around the time of *Olmstead*, Congress was more willing than the Supreme Court to offer protections against wiretapping. In 1934, the Legislature passed the Federal Communications Act ("FCA") that

---

[69] § 2707(c).

[70] Swire & Legum, *supra* note 60.

[71] Donald R.C. Pongrace, *Stereotypification of the Fourth Amendment's Public/Private Distinction: An Opportunity for Clarity*, 34 AM. U. L. REV. 1191, 1198 (1985).

[72] Boyd v. United States, 116 U.S. 616, 622 (1886).

[73] *See* Olmstead v. United States, 277 U.S. 438, 464 (1928); *see also* Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 15 (2002). "The Supreme Court's decision in Olmstead v. United States sounded the death knell for the Fourth Amendment theories that integrated property law with an expansive interpretation of constitutional provisions designed to protect individual liberty." *Id.* at 15.

[74] *Olmstead*, 277 U.S. at 464.

[75] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE, 197 (NYU Press 2004).

provided federal statutory protection against the electronic surveillance of private conversations.[76]

Following the FCA, the Supreme Court grew more willing to protect electronic privacy then it was in *Olmstead.* First, in *Nardone v. United States*, the Court held that the FCA prohibited using evidence obtained by illegal wiretaps in federal courts.[77] Then, in *Berger v. New York*, the Court held that electronic surveillance was only permissible under a narrow set of circumstances.[78] Finally, the Court explicitly overruled *Olmstead* when it decided *Katz v. United States* in 1967.[79] There it held that the Fourth Amendment protects people where there is a "reasonable expectation of privacy" regardless of physical intrusion.[80]

After these developments, "wiretap surveillance was (ostensibly) prohibited under federal law,"[81] but the protections were limited.[82] The Department of Justice interpreted *Nardone* to apply only to interception and divulgence of communications, but not to interception alone.[83] Therefore, the FBI could still wiretap for domestic security purposes; also, the Supreme Court held that the FCA did not apply to states, and the progress of technology created other ways of circumventing the FCA.[84] Moreover, after *Burger*, *Katz*, and a congressional investigation into organized crime in the 1960s, Congress realized that law enforcement needed some freedom to conduct wiretaps.[85]

---

[76] Roundy, *supra* note 43, at 408.

[77] Nardone v. United States, 302 U.S. 379, 382–83 (1937).

[78] Berger v. New York, 388 U.S. 41, 56 (1967).

[79] Katz v. United States, 389 U.S. 347 (1967).

[80] *Id.* at 353. Justice Harlan proposed the "reasonable expectation of privacy" test in his concurring opinion. It is still used today. Roundy, *supra* note 43, at 410–11; Solove, *supra* note 44, at 198. *See also* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 57–58 (1997).

[81] Roundy, *supra* note 43, at 411.

[82] *Id.* at 408–09.

[83] *Id.* at 408.

[84] *Id.*

[85] *Id.* at 411.

The Wiretap Act began as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[86] Its purpose was to "prohibit, on the pain of criminal and civil penalties, all interceptions of oral and wire communications, except those specifically provided for in the Act, most notably those interceptions permitted to law enforcement officers when authorized by court order in connection with the investigation of [certain] serious crimes."[87] The "first line of defense" against improper wiretapping was a rigid authorization process often referred to as a "super-warrant."[88] To obtain a legal wiretap, a state or federal prosecutor had to submit a request to a judge detailing the circumstances involved, while showing that normal investigative methods had failed or were likely to fail.[89] If the request was granted, the judge could then authorize surveillance for up to thirty days.[90]

In 1986, responding to developments in technology, Congress enacted the Electronic Communications Privacy Act.[91] Title I of the ECPA amended the Wiretap Act.[92] Previously, the definition of a "wire communication" was "any *communication* . . . by the aid of wire, cable or other like connection."[93] ECPA changed this to "'any *aural transfer* made . . . by the aid of wire, cable, or other like connection.'"[94] Further, the ECPA broadened the Wiretap Act to protect "electronic communications."[95] As amended, "any transfer of signs, signals, writing, images, sounds, data, or intelligence . . . by a wire, radio, electromagnetic, photoelectronic or photooptical system"

---

[86] *Id.*

[87] *See* Dorothy Higdon Murphy, Comment, United States v. Councilman *and the Scope of the Wiretap Act: Do Old Laws Cover New Technologies?*, 6 N.C. J. L. & TECH. 437, 441 (2005) (quoting United States v. Giordano, 416 U.S. 505, 514 (1974)).

[88] Roundy, *supra* note 43, at 412.

[89] 18 U.S.C. § 2518(3)(c) (2000).

[90] § 2518(5). *See also* Roundy, *supra* note 43, at 412.

[91] Murphy, *supra* note 87, at 442. *See also* 18 U.S.C. §§ 2510–2522 (emphasis added); S. Rep. No. 99-541 (1986).

[92] Roundy, *supra* note 43, at 413.

[93] 18 U.S.C. § 2510(1) (1970). *See also* Roundy, *supra* note 43, at 414.

[94] 18 U.S.C. § 2510(1) (Supp. V 2005). *See also* Roundy, *supra* note 43, at 414.

[95] Roundy, *supra* note 43, at 414.

was protected under the act.[96] Overall, Congress intended the ECPA to give electronic communications what the Wiretap Act of 1968 gave wire communications.[97]

## V. THE MODERN WIRETAP ACT

Today, the Wiretap Act[98] imposes liability on both government and private actors for intentionally intercepting electronic communications.[99] Evoking Mark Klein's story about 641A and the Narus STA 6400, the EFF claimed in *Hepting* that AT&T intentionally intercepted communications of its customers.[100] Section 2511(1)(a) of the Wiretap Act creates a general prohibition on the interception of wire, oral, or electronic communications.[101] Section 2511(1)(b) applies to the interception of oral communications and is more specific in its proscriptions than subsection (a).[102] Section 2511(1)(b)(i) makes it unlawful for any person to intentionally use any "electronic, mechanical, or other device to intercept any oral communication" [103] when that device is affixed to, or "otherwise transmits a signal through, a wire, cable, or other like connection used in wire

---

[96] *Id.* at 414–15. *See also* 100 Stat. at 1849 (codified as amended at 18 U.S.C. § 2510(12) (2000)).

[97] Roundy, *supra* note 43, at 415.

[98] Codified at 18 U.S.C. §§ 2510–2522 (Supp. V 2005).

[99] Richard C. Turkington, *Protection for Invasions of Conversational and Communication Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes under Federal and State Wiretap and Store Communications Acts and the Common Law Privacy Intrusion Tort*, 82 NEB. L. REV. 693, 704 (2004). *See also* Katherine A. Oyama, *E-mail Privacy After* United States v. Councilman*: Legislative Options for Amending ECPA*, 21 BERKELEY TECH. L.J. 499, 504 (2006). In 2001, Congress included stored voice communications, like voice-mail, in the definition of a "wire communication." *Id.* at 504; USA PATRIOT Act, Pub. L. No. 1070-56, 115 Stat. 272 (2001) (codified as amended at 18 U.S.C. § 2511 (Supp. V 2005)).

[100] *Amended Complaint*, *supra* note 39, at 21.

[101] 18 U.S.C. § 2511(1)(a) (2000).

[102] Criminal Resource Manual 1050 Scope of 18 U.S.C. 2511 Prohibitions (1997), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm01050.htm.

[103] § 2511(1)(b).

communication."[104] Those who violate The Wiretap Act are subject to up to five years in prison, a fine, or both.[105]

Section 2511 outlines two exceptions which allow a service provider to legally assist the government in intercepting electronic communications: first, when there is a court order directing the service provider to do so;[106] and second, where the Attorney General has provided a certification of legality.[107]

Section 2511(2)(a)(ii) makes service providers liable under 18 U.S.C. § 2520 for the improper disclosure of electronic communications.[108] Under § 2520, an electronic communications service provider may be required to pay the "actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation,"[109] or $10,000 for each day of the violation.[110] Also, preliminary or equitable relief, punitive damages, and reasonable attorney's fees are available.[111]

In *Hepting*, the EFF claimed that AT&T's program violated § 2511(3)(a).[112] This section prohibits an electronic communication service provider from divulging the contents of real-time communications to anyone other than the addressee or intended recipient of the communications.[113] Since the NSA did not have a court order, a warrant, or authorization from the AG, the EFF claimed that AT&T improperly gave the agency access to the communication contents of its customers.[114] Not only does Klein's information

---

[104] § 2511(1)(b)(i).

[105] 18 U.S.C. § 2511(4)(a) (2000). *See also* Peter P. Swire, Legal FAQs on NSA Wiretaps, http://www.peterswire.net/nsa_full_faq.htm (last visited Jan. 23, 2008).

[106] 18 U.S.C. § 2511(2)(a)(ii)(A) (2000). *See also* Swire & Legum, *supra* note 60.

[107] § 2511(2)(a)(ii)(B). *See also* Swire & Legum, *supra* note 60.

[108] § 2511(2)(a)(ii).

[109] 18 U.S.C. § 2520(c)(2)(A) (2000).

[110] § 2520(c)(2)(B).

[111] 18 U.S.C. § 2520(b)(1)–(3) (2000).

[112] *Amended Complaint*, *supra* note 39, at 21.

[113] 18 U.S.C. § 2511(3)(a) (2000).

[114] *Amended Complaint*, *supra* note 39, at 20.

corroborate what the EFF already claimed, but it could add further liability. If accurate, AT&T could be liable under § 2511(1)(b)(i), because the splitter device Klein described appears to violate the statute's prohibition on connecting such a device to a line used for wire communications.[115]

## VI. THE PEN REGISTER STATUTE

In *Hepting*, the EFF alleged AT&T violated the Pen Register Statute.[116] Like the Wiretap Act, the Pen Register Statute of the ECPA applies to real-time communications.[117] However, whereas the former predominantly covers in-transit content information, the latter only applies to non-content electronic communications.[118] Because the NSA/AT&T data collection program seems to be directed at collecting CDRs, it implicates this section of the ECPA as well.

A pen register is a tool that records the numbers of outgoing calls dialed from a telephone; its companion, a trap and trace device, works in the reverse, recording numbers of incoming calls.[119] Before the ECPA, the public was not protected from either of these devices. The Supreme Court first dealt with pen registers and trap and trace devices in *United States v. New York Telephone Company*.[120] The Court held that these tools were not governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, thus the protections of the Wiretap Act did not extend to them.[121] Given that pen registers and trap and trace devices do not collect the contents of communications,

---

[115] *See* Bartnicki v. Vopper, 532 U.S. 514, 523 (2001) (Section 2511(1)(b) applies "to the intentional use of devices designed to intercept oral conversations."). *See also* Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (refusing to find a claim under the Wiretap Act because there was no device used to collect information).

[116] *Amended Complaint*, *supra* note 39, at 26.

[117] *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1565 (2004).

[118] *See id.* at 1566.

[119] *See* Robert Ditzion, Note, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321, 1322 (2004); 18 U.S.C. § 3127.

[120] United States v. N.Y. Tel. Co., 434 U.S. 159 (1977).

[121] *Id.* at 167. *See also* Ditzion, *supra* note 119, at 1326.

but only numbers that are dialed, they do not fall within the ambit of the Wiretap Act.[122]

Notably, the decision in *New York Telephone* did not concern any Fourth Amendment implications of pen registers.[123] However, two years later, the Supreme Court dealt with precisely that issue in *Smith v. Maryland*.[124] In that case, police in Baltimore used a pen register to find an alleged stalker without obtaining a warrant.[125] The petitioner claimed the evidence used against him should not be admitted because it constituted an illegal search and seizure.[126] Nevertheless, the Court held the Fourth Amendment did not cover the type of information collected by a pen register, and that telephone customers do not have a reasonable expectation of privacy in the numbers they dial.[127] "Petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[128]

Because of these two judicial decisions, Congress included protections against pen register and trap and trace device surveillance in the ECPA.[129] Title 18 U.S.C. § 3121 provides a general prohibition on the use of pen registers and trap and trace devices without a prior court order.[130] When a government agency is authorized to use such a device, it may only decipher the numbers dialed and not record the contents of the communication.[131]

---

[122] 434 U.S. at 167.

[123] Ditzion, *supra* note 119, at 1327.

[124] Smith v. Maryland, 442 U.S. 735 (1979).

[125] *Id.* at 737.

[126] *Id.*

[127] *Id.* at 742.

[128] *Id.* at 744.

[129] Ditzion, *supra* note 119, at 1328.

[130] 18 U.S.C. § 3121(a) (Supp. V 2005).

[131] § 3121(c).

To obtain authorization to use a pen register or trap and trace device, a law enforcement official must request an order from a court.[132] The request must contain the identities of the target and whose phone is being tapped (if known), the location of the device, and "a statement of the offense to which the information likely to be obtained" relates.[133] After the order is made, and when the information that is "likely to be obtained by such installation and use is relevant to an ongoing criminal investigation," a court *shall* (not may) grant the use of the device.[134] Then, the court can compel a teleco to assist law enforcement officials with installation of the pen register or trap and trace device when necessary.[135] A number-collecting device may be used without a court order in an emergency situation involving the immediate danger of death or serious bodily harm, organized crime, a threat to national security, or an attack on a protected computer.[136] In such a situation, an order approving the device must be obtained within forty-eight hours of the device's use.[137] If someone unlawfully uses a pen register or a trap and trace device, he or she "shall be fined . . . or imprisoned for not more than one year, or both."[138]

## VII. STATE SECRETS PRIVILEGE

It was not long before the United States government intervened in *Hepting v. AT&T* and invoked the state secrets privilege, in an attempt to dismiss the case quickly and without sensitive information becoming public.[139] The state secrets privilege originated in the

---

[132] 18 U.S.C. §§ 3122–23 (Supp. V 2005). *See also*, Ditzion, *supra* note 119, at 1329.

[133] 18 U.S.C. § 3123(b)(1) (Supp. V 2005).

[134] § 3123(a)(2).

[135] 18 U.S.C. § 3124 (Supp. V 2005).

[136] 18 U.S.C. § 3125 (Supp. V 2005).

[137] *Id.*

[138] 18 U.S.C. § 3121(d) (Supp. V 2005).

[139] First Statement of Interest of the United States at 1, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006), 1, *available at* http://www.eff.org/legal/cases/att/USA_statement_of_interest.pdf [hereinafter *First Statement of Interest*].

common law during the early years of the United States,[140] and was used in court as early as 1807 in *United States v. Burr*.[141] In that case, Aaron Burr had been charged with treason and attempting to raise a rebellion.[142] President Jefferson refused to produce a document that was important to Burr's defense because turning it over would have been harmful to national security.[143] Ultimately, the Court decided the case without ruling on the state secrets issue, but implied in dictum that a certain degree of privilege belonged to the executive in disclosing sensitive information.[144]

The Supreme Court addressed the state secrets privilege more directly in *Totten v. United States*.[145] In that case, the plaintiff sought compensation for services rendered on a contract he had with President Lincoln to spy on the Confederate Army.[146] "The Court held that where the contract in issue is one to perform 'secret services,' the case must be dismissed, as it will inevitably result in the disclosure of confidential information."[147] Since the contract was a confidential matter, the action brought to enforce it had to be dismissed.[148] Confidential information would necessarily be disclosed in conducting the case and thus the action was not allowed to proceed.[149]

---

[140] Anthony Rapa, Comment, *When Secrecy Threatens Security*: Edmonds v. Department of Justice *and a Proposal to Reform the State Secrets Privilege*, 37 SETON HALL L. REV. 233, 237 (2006).

[141] United States v. Burr, 25 F. Cas. 30, 33 (C.C.D. Va. 1807); *see* Erin M. Stilp, Comment, *The Military and State-Secrets Privilege: The Quietly Expanding Power*, 55 CATH. U. L. REV. 831, 833 (2006).

[142] *Burr*, 25 F. Cas. at 37; *see* John C. Yoo, *The First Claim: The Burr Trial,* United States v. Nixon, *and Presidential Power*, 83 MINN. L. REV. 1435, 1436 (1999).

[143] Stilp, *supra* note 141, at 833.

[144] *Burr*, 25 F. Cas. at 37; Stilp, *supra* note 141, at 833–34.

[145] Totten v. United States, 92 U.S. 105 (1876).

[146] Rapa, *supra* note 140, at 241.

[147] *Totten*, 92 U.S. at 107.

[148] *Id.*

[149] *Id.*

Nearly eighty years later, the Supreme Court developed guidelines for invoking the privilege in *United States v. Reynolds*.[150] During Air Force testing of electronic equipment on B-29 bombers, a plane crashed killing six crew members and three civilians.[151] During discovery, the plaintiffs moved for production of an accident report the Air Force created regarding the crash.[152] The government argued that the report was privileged information and should not be disclosed, but this argument was rejected by both the District Court for the Eastern District of Pennsylvania and the United States Court of Appeals for the Third Circuit.[153] The Supreme Court, however, reversed the decisions of the lower courts and found that a special privilege exists for some military and state secrets.[154]

Even though a state secrets privilege exists, "it is not to be lightly invoked."[155] To do so, a head of a department must formally claim the privilege and a court must determine if the claim is appropriate. Further, the court must decide if the privilege can be used "without forcing a disclosure of the very thing the privilege is designed to protect."[156] Thus, the Court in *Reynolds* decided the state secrets privilege belonged to the government, must affirmatively be claimed by a department head, and must pass the scrutiny of a judge before it is properly invoked; the privilege cannot be claimed by a private party.[157]

"Courts have taken an expansive view of what constitutes a state secret" when applying *Totten* and *Reynolds*.[158] They have often deferred to the executive branch when the privilege has been invoked, citing a lack of expertise in the area.[159] Unfortunately, using the state

---

[150] United States v. Reynolds, 345 U.S. 1 (1953).

[151] *Id.* at 3; Holly L. McPherson, Tenet v. Doe*: Balancing National Security and Contracts to Spy*, 28 U. HAW. L. REV. 201, 217 (2005).

[152] *Reynolds*, 345 U.S. at 3.

[153] *Id.*

[154] *Id.* at 6.

[155] *Id.* at 7.

[156] *Id.* at 8.

[157] *Id.*

[158] Rapa, *supra* note 140, at 244.

[159] *Id.*

secrets privilege normally leads to several undesirable consequences. First, if the plaintiff cannot make a prima facie case without the privileged information, it will be dismissed.[160] Second, the case may also be dismissed "if the government is unable to defend itself without using the classified" information.[161] Third, if the government is prosecuting the case and the privilege deprives the defendant of evidence necessary to his or her defense, there will be a summary judgment for the defendant.[162] Finally, the court may dismiss the case if the subject matter itself is a state secret.[163]

In *Hepting v. AT&T*, the United States government filed a statement of interest with the court pursuant to 28 U.S.C. § 517, stating it intended to invoke the state secrets privilege.[164] The statement said "when allegations are made about purported classified government activities or relationships, regardless of whether those allegations are accurate, the existence or non-existence of the activity or relationship is potentially a state secret," thus claiming the very essence of the case is a state secret and the case should be dismissed.[165] In the statement, the government cited *Reynolds*, *Totten*, and *Burr* as authorities, noting that protecting state secrets often requires dismissal.[166] The government claimed that this case should not continue because it would necessarily disclose information that would be harmful to national security.[167] If the case verified that a NSA/AT&T data-collection program existed, a terrorist could easily switch to a different telephone carrier and avoid inspection.[168] At the same time, if the case revealed that the program did not exist, then more terrorists may start

---

[160] Stilp, *supra* note 141, at 837.

[161] *Id.*

[162] *Id.* at 837.

[163] *Id. See also* Rapa, *supra* note 140, at 250.

[164] "The Solicitor General, or any officer of the Department of Justice, may be sent by the Attorney General to any State or district in the United States to attend to the interests of the United States in a suit pending in a court of the United States, or in a court of a State, or to attend to any other interest of the United States." 28 U.S.C.A. § 517 (West 2008).

[165] *First Statement of Interest*, *supra* note 139, at 1.

[166] *Id.* at 1.

[167] *Hepting*, 439 F. Supp. 2d at 980.

[168] *Id.* at 990.

communicating via AT&T.[169] Shortly after issuing this statement of interest, the government did, in fact, file a motion to dismiss based on the state secrets privilege.[170]

When considering this issue, the *Hepting* court first looked to see if the information the government wanted to protect was actually a state secret. The court chose to consider only "publicly reported information that possesses substantial indicia of reliability and whose verification or substantiation possesses the potential to endanger national security."[171] It did not rely on Mr. Klein's statement or media reports, but instead considered only what the government had admitted or denied.[172]

The *Hepting* Court found that, unlike the secret spy program in *Totten*, the government had already admitted a terrorist surveillance program existed, albeit a legal one.[173] In his weekly radio address, President Bush confirmed the existence of the "terrorist surveillance program" that was first revealed by The New York Times.

> In the weeks following the terrorist attacks on our nation [on Sept 11, 2001], I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations.[174]

Two days later, Attorney General Alberto Gonzales further verified its existence when he stated that the president had authorized a program to intercept communications where one party to the communication is outside of the United States.[175] Moreover, while

---

[169] *Id.* at 990.

[170] Notice of Motion and Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. C 06-0672-VRW), *available at* http://www.eff.org/legal/cases/att/GovMotiontoDismiss.pdf.

[171] *Hepting*, 439 F. Supp. 2d at 990.

[172] *Id.* at 990–91.

[173] *Id.* at 991–92.

[174] Press Release, President George W. Bush, President's Radio Address (Dec. 17, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html.

[175] Press Release, Att'y Gen. Alberto Gonzales, *supra* note 33.

BellSouth, Verizon, and Qwest have denied association with the NSA program, AT&T has not.[176] Thus, "the public denials by these telecommunications companies undercut the government and AT&T's contention that revealing AT&T's involvement or lack thereof in the program would disclose a state secret."[177] Accordingly, the *Hepting* Court denied the government's motion to dismiss the case based on the state secrets privilege.[178] Still, it only required discovery of information at AT&T that was of the same level of generality as the government's disclosures.[179]

Nevertheless, the district court was reluctant to entirely rule out the state secrets privilege. It held that AT&T did not need to reveal the details of its relationship with the NSA because it might qualify as a protectable state secret that should be protected.[180] Still, the court noted that in the future, the government might reveal more information about the NSA program that would make disclosure by AT&T no longer a state secret.[181] If so, AT&T may be required to disclose more information about its involvement in the program at that time.[182] Thus, the court left the door open for the issue to be revisited in the future.[183]

## VIII. THE *HEPTING* APPEAL

After the first attempt to have the lawsuit dismissed, AT&T took the case to the United States Court of Appeals for the Ninth Circuit

---

[176] Marguerite Reardon, *Telecoms Deny Illegally Handing Over Call Records*, ZDNET NEWS, May 17, 2006, http://news.zdnet.com/2100-1009_22-6073179.html; John O'Neil & Eric Lichtenblau, *Qwest's Refusal of N.S.A. Query is Explained*, N.Y. TIMES, May 12, 2006, http://www.nytimes.com/2006/05/12/washington/12cnd-phone.html?ex=1305086400&en=16b1c1d512d1d04b&ei=5088&partner=rssnyt&emc=rss.

[177] *Hepting*, 439 F. Supp. 2d. at 997.

[178] *Id.* at 998.

[179] *Id.*

[180] *Id.* at 997.

[181] *Id.*

[182] *Id.* at 998.

[183] *Id.*

("Ninth Circuit").[184] The appeal was granted on November 7, 2006; as of the writing of this article, the Court has not made a ruling.[185]

AT&T argued that the plaintiffs could not establish standing and therefore the case must be dismissed.[186] As in *Reynolds*,[187] AT&T could not itself claim the state secrets privilege because it is a private entity and not a government actor. However, the government asserted the privilege and the court below acknowledged that it could be at least partially applicable in this case.[188] In its appeal, AT&T argued that the plaintiffs cannot establish that they were actually spied upon.[189] "When a plaintiff claims injury arising out of government surveillance . . . standing exists only when the plaintiff can furnish 'proof of actual acquisition of [his] communications.'"[190] The lawsuit cannot proceed without this "actual acquisition." What is more, Mark Klein's story does not help to establish standing because its validity cannot be litigated without running afoul of the state secrets privilege.[191]

AT&T further argued for dismissal of the case because the invocation of the state secrets privilege prevents full and fair litigation of the case.[192] Recall that in *Totten v. United States*, the Supreme Court dismissed a case because litigating a government surveillance contract would necessarily reveal state secrets.[193] As in *Totten*, AT&T argued that this case should be dismissed because it necessarily would

---

[184] Petition for Permission to Appeal Under 28 U.S.C. § 1292(b), Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006), *available at* http://www.eff.org/legal/cases/att/Petition.pdf [hereinafter *Petition*].

[185] Order Granting Appeal to Ninth Circuit, Hepting v. AT&T Corp. *available at* http://www.eff.org/legal/cases/att/appealgranted.pdf.

[186] *Petition*, *supra* note 184, at 9.

[187] *See Reynolds*, 345 U.S. at 7.

[188] *See Hepting*, 439 F. Supp. 2d at 997.

[189] *Petition*, *supra* note 184, at 15–16.

[190] Brief of Appellant AT&T Corp. at 24, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. 06-17132), *available at* http://www.eff.org/legal/cases/att/att_opening_brief.pdf (citing Halkin v. Helms, 690 F.2d 977, 999–1000 (D.C. Cir. 1982)).

[191] *Id.* at 49.

[192] *Id.* at 31.

[193] *See Totten*, 92 U.S. at 107.

reveal specifics of the program that are properly privileged.[194] AT&T also claimed that the court below erred by assuming that the company had participated in an illegal surveillance program without actual proof.[195]

Since the case is currently ongoing, it is premature to speculate exactly how it will be decided. As aforementioned, courts often take an expansive view of the state secrets privilege and defer when the government invokes it.[196] However, the district court here has broken from that trend and decided that litigation should go forward. Furthermore, the Ninth Circuit has been "skeptical of and sometimes hostile" to the government's argument.[197] Still, it is unclear exactly how this case will be resolved. Nevertheless, the consequences are severe: AT&T could be liable for large sums of money and a huge government data-collection program could be exposed.

## IX. THE PROTECT AMERICA ACT OF 2007

Until recently, Congress was unable to agree on any legislation to deal with the surveillance and national security issues raised by *Hepting*. The Electronic Surveillance Modernization Act came close, making its way through the House of Representatives in September 2006,[198] only to die in the Senate without ever reaching a vote.[199]

---

[194] *Petition*, *supra* note 184, at 37.

[195] *Id.* at 40.

[196] Rapa, *supra* note 140, at 249.

[197] Adam Liptak, *U.S. Defends Surveillance Before 3 Skeptical Judges*, N.Y. TIMES, Aug. 16, 2007, at A13.

[198] Anne Broache, *House Votes to Expand Electronic Spying Powers*, CNET NEWS.COM, Sept. 29, 2006, http://news.com.com/House+votes+to+expand+electronic+spying+powers/2100-1028_3-6121474.html.

[199] H.R. 5825 109th (2006): Electronic Surveillance Modernization Act (GovTrack.us), http://www.govtrack.us/congress/bill.xpd?bill=h109-5825#votes (last visited Jan. 23, 2008). For more information on the Electronic Surveillance Modernization Act, see Elizabeth Bazan, CRS Report for Congress: H.R. 5825 109th (2006): "Electronic Surveillance Modernization Act," *available at* http://www.fas.org/sgpcrs/intel/RL33637.pdf; Opposition to H.R. 5835, the Electronic Surveillance Modernization Act (Sept. 28, 2006), *available at* http://www.cdt.org/security/20060928wilsonletter.pdf.

Then, on August 5, 2007, under strong pressure from the White House,[200] Congress passed the Protect America Act ("PAA") of 2007.[201] Introduced by Senator Mitch McConnell (R-KY) a mere four days earlier, this law passed through both houses with only a single amendment.[202] Despite the short deliberation, this bill made significant changes to the Foreign Intelligence Surveillance Act ("FISA")[203] and has serious implications for future lawsuits similar to *Hepting*.

The PAA's purpose was to modernize the law with regard to developments in technology that occurred since FISA was passed in 1978.[204] At the time FISA was passed, most international communications were conducted through wireless communications and domestic communications were primarily transmitted via wire.[205] Today, however, the situation has reversed and international communications once transmitted by satellite now use fiber optics.[206] Before the PAA, FISA excluded satellite communications from its regulations, but included fiber optic communications.[207] Thus, as originally conceived, FISA would have excluded most international communications from its scope, allowing foreign intelligence to be collected more easily, while regulating domestic communications and

---

[200] Radio Address, President George W. Bush, President's Radio Address, July 28, 2007, *available at* http://www.whitehouse.gov/news/releases/2007/07/20070728.html; Eric Lichtblau & Mark Mazzetti, *Broader Spying Authority Advances in Congress*, N.Y. TIMES, Aug. 4, 2007, at A8; Carl Hulse & Edmund L. Andrews, *House Approves Changes in Eavesdropping Program*, N.Y. TIMES, Aug. 5, 2007, at A1.

[201] Protect America Act, Public Law No 110-055, *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ055.110.pdf.

[202] The Library of Congress, http://thomas.loc.gov/cgi-bin/bdquery/z?d110:SN01927:@@@R (last visited, Jan. 23, 2008).

[203] FISA is codified at 50 U.S.C. §§ 1801–1811, 1821–1829, 1841–1846, 1861–62.

[204] House Permanent Select Committee on Intelligence, Hearing on the Protect America Act of 2007, Statement for the Record of J. Michael McConnell, Director of National Intelligence, Sept 20, 2007 *available at* http://www.dni.gov/testimonies/20070920_testimony.pdf [hereinafter *Hearing*].

[205] *Id.* at 5.

[206] *Id.*

[207] *Id.* at 5–6.

protecting people in the United States. However, because of the use of transnational fiber optics today, many communications that could be vital to foreign intelligence fell under the regulation of pre-PAA FISA.[208]

The PAA addressed this problem in its first amendment to FISA. Section 105A redefined "electronic surveillance" by removing from FISA's scope all "surveillance directed at a person reasonably believed to be located outside of the United States."[209] Since FISA regulates "electronic surveillance," this change in definition eliminates such surveillance from FISA's regulation.[210] Now, "if the government is monitoring someone outside the United States from a telecom switch in the U.S., it can listen in on the person's calls and read their e-mails without obtaining a FISA warrant first."[211]

The Director of National Intelligence ("DNI"), Michael McConnell, has called section 105A "the head of this legislation."[212] Prior to the PAA, the intelligence community was wasting time obtaining warrants for targets located outside of the United States.[213] "This process had little to do with protecting the privacy and civil liberties of Americans. These were foreign intelligence targets, located in foreign countries."[214] Thus, according to the DNI, the PAA was necessary to address the realities of today's foreign intelligence gathering.[215]

Section 105B(a) of the PAA empowers the DNI and the AG to authorize surveillance for up to one year on persons reasonably believed to be outside of the United States.[216] However, before such

---

[208] *Id.* at 6.

[209] Protect America Act of 2007 § 105A, Pub. Law. No. 110-055 (Aug. 5, 2007).

[210] EPIC, http://www.epic.org/privacy/terrorism/fisa (last visited Jan. 23, 2008).

[211] Posting of Orin Kerr to The Volokh Conspiracy, http://www.volokh.com/posts/1186332672.shtml (Aug. 5, 2007, 13:51 EST).

[212] *Hearing*, *supra* note 204.

[213] *Id.* at 9.

[214] *Id.*

[215] *Id.* at 3.

[216] Protect America Act § 105B(1). ELIZABETH B. BAZAN, CRS REPORT FOR CONGRESS: P.L. 110-55, THE PROTECT AMERICA ACT OF 2007: MODIFICATIONS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 5, (2007), *available at* www.fas.org/sgp/crs/intel/RL34143.pdf.

power can be executed, the DNI and the AG must certify in writing that there are procedures in place to determine that the surveillance concerns persons reasonably believed to be outside of the U.S.; it is not electronic surveillance (under its new definition); it involves obtaining information with the assistance of a communications service provider; a "significant purpose" of the surveillance is to obtain foreign intelligence; and there are minimization procedures in place to prevent information from being gathered about a person within the U.S.[217] If time does not permit a written certification, the DNI and the AG can authorize surveillance for up to 72 hours before a written certification is required.[218] When complete, the written certification must be sent to the FISA court and will remain sealed unless it is needed to assess the legality of the surveillance.[219]

The part of the Protect America Act that is likely most critical for telecos is the power of the AG and the DNI to compel telecos to turn over information seen as helpful to foreign intelligence.[220] If the teleco fails to cooperate, the AG may bring the company before the FISA court to force compliance.[221] "Failure to obey an order of the court may be punished" as contempt of court.[222] However, a teleco can challenge a surveillance directive in the FISA court, with the judge holding power to modify or set aside the directive if necessary.[223]

These new amendments also have serious implications for future lawsuits like *Hepting*. Section 105B(l) bars any cause of action against "any person for providing any information, facilities, or assistance in accordance with a directive under this section."[224] Thus, a case against a teleco could never be brought against surveillance done pursuant to FISA.

To prevent abuses, the PAA contains additional checks on this expanded surveillance power, but these checks are minimal. Section

---

[217] § 105B(a)(1)–(5).

[218] § 105B(a)

[219] § 105B(c).

[220] § 105B(e)

[221] § 105B(g).

[222] *Id.*

[223] § 105B.

[224] § 105B(l); BAZAN, *supra* note 216, at 9.

105C requires the AG to submit to the FISA court the procedures used by the government to confirm that intelligence will not constitute electronic surveillance within 120 days of when the law became active.[225] In these situations, the court will only overrule the government if it finds the order "clearly erroneous."[226] Furthermore, the AG must inform the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Judiciary Committees of both houses concerning acquisitions of foreign intelligence during the previous six months.[227] In this report to the Committees, the AG must describe any incidences of non-compliance by a teleco.[228] Interestingly, and perhaps paradoxically, the AG must also self-report any incidence during the prior six months during which the government did not ensure that surveillance was directed toward someone reasonably believed to be outside of the U.S.[229]

Not surprisingly, the PAA has spurred much debate from all sides of the political spectrum.[230] The day after the PAA passed, the White House released a "fact sheet" supporting the Act's amendments.[231] The PAA is important to the White House because it brings FISA in line with technological advances and allows foreign intelligence to be collected more effectively and efficiently.[232] Orin Kerr,[233] an Internet surveillance law expert, and Philip Bobbitt,[234] a constitutional law

---

[225] Protect America Act § 105C(a).

[226] *Id.* § 105C(c).

[227] *Id.* § 4.

[228] *Id.* § 4.

[229] *Id.* § 4; BAZAN, *supra* note 216, at 18.

[230] Beth Wellington, *Commentary: The Protect America Act and Legislation Related to the Domestic Surveillance Program*, LLRX.COM, Aug. 27, 2007, http://www.llrx.com/extras/nsa.htm.

[231] Press Release, White House, Fact Sheet: The Protect America Act of 2007 (Aug. 6, 2007), *available at* http://www.whitehouse.gov/news/releases/2007/08/20070806-5.html.

[232] *Id.*

[233] George Washington University, Orin S. Kerr, http://www.law.gwu.edu/Faculty/profile.aspx?id=3568 (last visited Jan. 23, 2008).

[234] University of Texas, Philip Bobbitt, http://www.utexas.edu/law/faculty/profile.php?id=pbobbitt (last visited Jan. 23, 2008).

scholar, also agree with the legislation. Kerr has stated that the "legislation on the whole seems relatively well done."[235] He noted that giving the government access to the communications of people outside the U.S., even if it forces telecos to cooperate, seems appropriate.[236] Bobbitt notes that "all sides agree that some legislative fix" to surveillance laws was needed "because of changes in telecommunications technology."[237] He writes that "in Robert M. Gates, the defense secretary, Mike McConnell, the director of national intelligence, and Gen[eral] Michael V. Hayden, the director of central intelligence, we have about as good a team as it is possible to imagine. Most people in Congress know that. Why not assume they are proposing a solution to a real problem?"[238]

The ACLU released its own "fact sheet" in response to the White House's version.[239] Calling the FISA amendment the "Police America Act," the ACLU argued the Act "allows for massive, untargeted collection of international communications without a court order or meaningful oversight by either Congress or the courts."[240] The ACLU doubts the protections that are built into the new law.[241] "The report to the court only need detail how the program is directed at people reasonably believed to be overseas—it does not require the AG to explain how it treats Americans' calls or emails when they are intercepted."[242] Yale Professor Jack Balkan has further criticized the FISA amendments, fearing that the United States is slowly moving toward becoming a surveillance state where the government is freed

---

[235] Posting of Orin Kerr, *supra* note 211.

[236] *Id.*

[237] Philip Bobbitt, *The Warrantless Debate Over Wiretapping*, N.Y. TIMES, Aug. 22, 2007, at A19.

[238] *Id.*

[239] American Civil Liberties Union, ACLU Fact Sheet on the "Police America Act," http://www.aclu.org/safefree/nsaspying/31203res20070807.html (last visited Jan. 23, 2008).

[240] *Id.*

[241] *Id.*

[242] *Id.*

from political control and accountability.[243] Even the conservative John Birch Society does not trust the law.[244]

## X. CONCLUSION

Perhaps something that all sides can agree on is that the debate is far from over. Indeed, one amendment made to the PAA was a sunset provision which stated that changes to FISA would only last six months.[245] While there is some question how effective this provision will be,[246] it is nevertheless clear that something more permanent is needed. As the White House pushes to make the PAA's changes permanent,[247] a presidential election looms, and *Hepting* is still being litigated. The only certainty is that issues related to the ECPA, the Stored Communications Act, and the Pen Register Statute will remain vitally important and widely debated.

---

[243] Posting of Jack Balkin to Balkinization, http://balkin.blogspot.com/2007/08/party-of-fear-party-without-spine-and.html (Aug. 5, 2007, 09:27 EST).

[244] Mary Benoit, Surveillance Program Signed into Law over Weekend, JOHN BIRCH SOCIETY, http://www.jbs.org/node/5057 (last visited Jan. 23, 2008).

[245] Protect America Act § 6(c).

[246] *See* ACLU, *supra* note 239; Aziz Huq, *Data-Mining Our Liberties*, THE NATION, Aug. 7, 2007, http://www.thenation.com/doc/20070813/huq2.

[247] Tom A. Peter, *Bush Wants Permanent Warrantless Wiretap Law*, CHRISTIAN SCI. MONITOR, Sept. 22, 2007, http://www.csmonitor.com/2007/0921/p99s01-duts.html.