View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Valparaiso University

ValpoScholar Valparaiso University Law Review

Volume 41
Number 4 *Symposium on Electronic Privacy in the Information Age*

*pp.*1481-1516

Symposium on Electronic Privacy in the Information Age

Liability for All, Privacy for None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World

Frederick M. Joyce

Andrew E. Bigart

Follow this and additional works at: https://scholar.valpo.edu/vulr

 Part of the Law Commons

Recommended Citation

Frederick M. Joyce and Andrew E. Bigart, *Liability for All, Privacy for None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World*, 41 Val. U. L. Rev. 1481 (2007).
Available at: https://scholar.valpo.edu/vulr/vol41/iss4/3

This Symposium is brought to you for free and open access by the Valparaiso University Law School at ValpoScholar. It has been accepted for inclusion in Valparaiso University Law Review by an authorized administrator of ValpoScholar. For more information, please contact a ValpoScholar staff member at scholar@valpo.edu.

Valparaiso University

LIABILITY FOR ALL, PRIVACY FOR NONE: THE CONUNDRUM OF PROTECTING PRIVACY RIGHTS IN A PERVASIVELY ELECTRONIC WORLD

Frederick M. Joyce and Andrew E. Bigart*

I. INTRODUCTION

Electronic communications technology in our nation is no longer merely pervasive, it is ubiquitous. We drive to work in automobiles that allow us to navigate via GPS, communicate with wireless phone systems, and, if faced with an emergency, contact an emergency help center at the push of a button. At the office, we spend our days sending emails or engaging in telephone conversations with employer-provided computers, hand-held devices, and wireless and wireline telephones. Back home, we relax by talking to friends and family on cellular phones, sending text messages, and editing Internet blog postings.

While the benefits of advanced communications technology are apparent, there is a dawning realization that the spread of these technologies at home and at work may have come at a price. The fact is that every time we venture into this ubiquitous electronic world, the odds are high that the government, or someone, may be monitoring or recording all of our communications and movements.

This Article examines how a wide array of federal laws such as the Wiretap Act,[1] the Communications Assistance for Law Enforcement Act[2] ("CALEA"), the Electronic Communications Privacy Act[3] ("ECPA"), the Stored Communications Act[4] ("SCA"), and the Foreign Intelligence

---

* Frederick "Rick" M. Joyce is chair of the Communications Group at Venable LLP law firm in Washington, D.C. His telecommunications work includes domestic and international telecom regulations and treaties, appellate and civil litigation matters, and state and federal communications legislation, with a particular emphasis on wireless communications and electronic media. Andrew E. Bigart is an associate in the Regulatory Group at Venable LLP.

1 Wire and Electronic Communications Interception and Interception of Oral Communications, ch. 119, Pub. L. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. § 2511 (2000)).

2 Communications Assistance for Law Enforcement Act, ch. 9, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 18 U.S.C. §§ 2510-2511; 47 U.S.C. § 1001 (2000)).

3 Electronic Communications Privacy Act of 1986, ch. 119, Pub. L. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. § 2510)).

4 18 U.S.C. § 2701.

Produced by The Berkeley Electronic Press, 2007

Surveillance Act[5] ("FISA"), not only permit the government to monitor and intercept electronic communications and data, but also place a duty on businesses to cooperate with these investigative efforts. These laws, originally intended to strike a reasonable balance between privacy rights and law enforcement needs, did not anticipate heightened "Homeland Security" concerns or the recent technological revolution. Consequently, the current state of the law has left government, businesses, and private citizens without a clear sense of their legal rights, obligations, and liabilities.

A. Privacy Risks in an Increasingly Electronic World

Over the past decade, U.S. courts have struggled to apply this complex array of electronic privacy laws to an equally complex if not bewildering array of communications technologies and applications. Previously, courts dealt mainly with conventional telephone wiretaps under these statutes; today, courts must apply decades-old law to a wide range of emerging technologies including cellular telephones, Internet communications, email, blogs, instant messaging, voice over internet protocol ("VOIP") communications, packet-sniffing systems, keylogging programs, and other emerging technologies.[6]

Businesses face similar dilemmas in trying to strike a reasonable balance between the obvious benefits of providing employees with comprehensive electronic communications tools, versus the risk that the electronic activities of their employees could lead to legal liability or network harm for the enterprise. Employers, not unlike modern courts, struggle to understand electronic privacy laws to the point where the purchase and deployment of ostensibly useful electronic devices can be constrained by concerns about potential legal liability.

This nascent conflict between electronic privacy laws and communications technology has led to two disturbing trends. First, without clear legal limits, the government has begun to expand its electronic surveillance operations to a degree not contemplated by the original laws or supported by the majority of U.S. citizens.[7] Second, this

---

[5] Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. § 1801 (2000)).

[6] *See e.g.*, Casey Holland, Note, *Neither Big Brother Nor Dead Brother: The Need for a New Fourth Amendment Standard Applying to Emerging Technologies*, 94 KY. L.J. 393, 394-95 (2005).

[7] David Jefferson, *NEWSWEEK Poll: American's Wary of NSA Spying*, Newsweek (Web Exclusive), May 14, 2006, http://www.msnbc.msn.com/id/12771821/site/newsweek. "According to the latest NEWSWEEK poll, 53 percent of Americans think the NSA's surveillance program 'goes too far in invading people's privacy,' while 41 percent see it as

confusing and uncertain legal landscape makes compliance with the law virtually impossible, to the extent that anyone who endeavors to comply with electronic privacy laws may nevertheless end up in court.

B. NSA Surveillance Cases Raise the Stakes

The recent ruckus over the National Security Agency's ("NSA") warrantless electronic surveillance program reflects a troubling escalation of this electronic privacy conflict. According to publicly available information, these NSA surveillance programs involved intercepting conversations or mining customer data without first obtaining court authority as arguably required by statute.[8] The first NSA program involved the monitoring of virtually all international telephone communications in order to identify potential terrorists.[9] The other program involved NSA requests to telephone carriers that they turn over all customer call records; the NSA would then sift through these records for links to terrorists.[10]

The litigation that these NSA programs spawned suggests that the increscent conflict between electronic privacy rights, law enforcement activities, and our outdated electronic privacy laws has reached nearly pandemic levels. Multiple cases have been filed throughout the U.S. in response to the NSA surveillance programs. The plaintiffs in these cases are not accused terrorists or bad guys, they are ordinary telephone customers. The defendants are not just the NSA and the government entities that authorized these surveillance programs; they include almost every major telecommunications carrier in the U.S. Moreover, although the U.S. Department of Justice recently decided to subject these NSA

---

a necessary tool to combat terrorism." *Id.* Further, the poll indicates that 57% of Americans believe that the White House went too far in expanding presidential power in light of the data mining revelation. *Id.*

8 *See, e.g.*, *Federal Court Strikes Down NSA Warrantless Surveillance Program*, ACLU, http://www.aclu.org/safefree/nsaspying/26489prs20060817.html (last visited Mar. 25, 2007) (noting that the warrantless surveillance program was in direct violation of FISA, which requires the executive branch to obtain a warrant before engaging in electronic surveillance of Americans).

9 *See, e.g.*, James Reisen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES, Dec. 21, 2005, at A1, http://www.nytimes.com/2005/12/21/politics/21nsa.html?ex=1292821200& en=91d434311b0a7ddc&ei=5088&partner=rssnyt&emc=rss (reporting that the president authorized the NSA to intercept communications where at least one end of the communication was outside of the United States.).

10 *See, e.g.*, Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY, May 10, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (reporting that the NSA used data provided by AT&T, Verizon, and BellSouth to analyze calling patterns).

surveillance programs to prior judicial review, the facts disclosed in these proceedings cast a disturbing light on the vast scope of electronic surveillance in the United States today and the relative ease with which it can be accomplished.

In some respects, public outrage over the NSA's surveillance activities,[11] particularly the lack of judicial oversight, misses a larger point that is the crux of this Article. New communications technologies raise new privacy concerns, concerns that are not well protected under the current statutory framework. A threat to privacy rights arises not only from an executive office or Department of Justice unchecked by judicial review, but also from the proliferation of new communications technologies that present the government, or private entities, with virtually unlimited opportunities to monitor communications and individual movements with or without judicial supervision. The federal framework of laws intended to prevent electronic technology from invading legitimate privacy interests is now rickety and unequal to the task.

To see how we arrived at this critical juncture, this Article examines the history and development of electronic privacy laws in the U.S. Then, this Article reviews recent case law to demonstrate how courts have struggled to apply electronic privacy laws to rapidly evolving electronic technology, comments on the need for congressional action, and offers suggestions for managing electronic information within the current state of the law.

II. THE EVOLUTION OF ELECTRONIC PRIVACY LAW

A. Common Law, the Constitution, and the Communications Act of 1934

A discussion of state electronic privacy laws and rights is well beyond the scope of this Article; nevertheless, it is useful to note that federal electronic privacy laws, and the courts' interpretations of them, have evolved from common law concepts of "invasion of privacy" and "intrusion upon seclusion."[12] For example, the common law concept of

---

11 Jefferson, *supra* note 7.

12 *See generally* Bartnicki v. Vopper, 532 U.S. 514 (2001); Heutche v. United States, 414 U.S. 898 (1973); Berger v. New York, 388 U.S. 41 (1967); Osborn v. United States, 385 U.S. 323 (1966); Lopez v. United States, 373 U.S. 427 (1963).

what constitutes a "reasonable expectation of privacy" is central to many court interpretations of electronic privacy rights.[13]

Although the Fourth Amendment protects persons from governmental searches and seizures, there is no express constitutional right of privacy.[14] Indeed, the U.S. Supreme Court initially refused to extend the Fourth Amendment's protections to private telephone communications.[15] It was not until *Katz v. United States* that the Court reversed prior decisions and recognized that individuals have legitimate privacy interests in telephone and electronic communications. According to *Katz*, "what [an individual] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[16] Nevertheless, because the Fourth Amendment operates primarily to protect citizens from government or state action, electronic privacy rights in most instances are governed by federal statutes, common law "invasion of privacy" claims, and, state privacy laws in those states that have adopted electronic privacy laws or constitutional privacy provisions.[17]

While it took the Court several decades to recognize legitimate privacy interests in electronic communications, Congress recognized the need to protect against interception of communications as early as 1912.[18]

---

13 47 U.S.C. § 705 (2000); *see also* Kyllo v. United States, 533 U.S. 27 (2001) (discussing thermal imaging in relation to reasonable expectation of privacy); United States v. Dunn, 480 U.S. 294 (1987) (discussing the use of electronic monitoring devices in tracking drug suspects); Katz v. United States, 389 U.S. 347 (1967) (discussing monitoring of telephone booth use).

14 *Katz*, 389 U.S. at 350.

15 *See* Olmstead v. United States, 277 U.S. 438, 478-79 (1928).

16 *Katz*, 389 U.S. at 351.

17 *See, e.g.*, Sarah DiLuzio, Comment, *Workplace E-Mail: It's Not as Private as You Might Think*, 25 DEL. J. CORP. L. 741 (2000); Kevin B. Kopp, Comment, *Electronic Communications in the Workplace: E-Mail Monitoring and the Right of Privacy*, 8 SETON HALL CONST. L.J. 861 (1998).

18 > What is known is that section 605 of the Federal Communications Act of 1934, prohibiting interception and disclosure of non-broadcast radio transmissions, was incorporated almost verbatim from section 27 of the Radio Act of 1927 [and] the prohibition on interception and disclosure contained in the Radio Act of 1927 [was] derived from section 4 of the Radio Act of 1912. . . . All three of these acts—1912, 1927, and 1934—prohibited disclosure of messages, not only by amateurs and others who might intercept radio transmissions, but also by employees of communications companies who, of necessity, have access to radio messages in the normal course of their jobs.

Kent R. Middleton, *Radio Privacy under Section 705(A): An Unconstitutional Oxymoron*, 9 ADMIN. L.J. AM. U. 583, 588-90 (1995).

It was then that Congress granted the Interstate Commerce Commission ("ICC") authority to prohibit unauthorized persons from intercepting and divulging the contents of radio communications.[19] The Communications Act of 1934 transferred the ICC's authority over communications to the Federal Communications Commission, including the power to prohibit unauthorized persons from intercepting communications.[20]

Over time, state and local law enforcement officials began to pay deference to federal electronic privacy statutes, even when it arguably was not required. In part, this was because of the Supremacy Clause and the larger body of law that had evolved over the years under federal electronic privacy statutes.[21] More recently, the USA PATRIOT Act empowered state and local prosecutors to use the federal laws in state court. As a practical matter, the desire to avoid liability under federal electronic privacy statutes motivates continued deference toward them.[22]

B. The Wiretap Act of 1968

The current federal framework for electronic surveillance and individual privacy is composed of several different statutes that separately govern the surveillance of domestic subjects and matters involving foreign intelligence. In the wake of the *Katz* decision, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Wiretap Act of 1968").[23] The Wiretap Act of 1968 set the blueprint for all subsequent privacy and surveillance laws by generally protecting the privacy of wire and oral communications while also permitting certain authorized interceptions. For example, the Wiretap Act of 1968 authorized interceptions by law enforcement officers acting pursuant to a court order.[24]

At the same time, the Wiretap Act of 1968 set unfortunate precedent for later electronic privacy laws by narrowly limiting the applicability of

---

[19] Radio Act of 1927, ch. 169, 44 Stat. 11621172 (1927) (as codified at 47 U.S.C. § 81 (2000)).

[20] Communications Act, ch. 5, 90 Pub. L. 351, 48 Stat. 1103 (1968) (as codified at 47 U.S.C. § 605 (2000)).

[21] AM. PROSECUTORS RESEARCH INST., THE ECPA, ISPS AND OBTAINING E-MAIL: A PRIMER FOR LOCAL PROSECUTORS (July 2005), *available at* http://www.ndaa-apri.org/pdf/ecpa_isps_obtaining_email_05.pdf.

[22] *Id.* at 7.

[23] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (1968).

[24] 18 U.S.C. § 2518 (2000).

the law to "wire" and "oral" communications, and, by failing to take into account available or looming technologies such as cordless telephones, cellular telephones, and other communication services. By this measure, the Wiretap Act of 1968 failed to heed Justice Brandeis's prophetic warning in *Olmstead v. United States* that "individual protection against specific abuses of power must have a . . . capacity of adaptation to a changing world," especially considering that "subtler and more far-reaching means of invading privacy have become available to the Government."[25]

C. Electronic Communications Privacy Act of 1986

By 1986, Congress recognized the need to upgrade the 1968 Wiretap Act and passed the ECPA to account for new computer and telecommunication technologies.[26] The ECPA, which continues to form the backbone of the current federal laws, extended wiretapping protections to cellular telephones, private networks, and intra-company communications while in transit or in storage. Although it was designed to address anticipated changes in the communications industry, the drafters of the ECPA evidently did not contemplate the rise of the Internet as a major communications device or the range of new communications technologies that would rapidly develop in the ensuing decade.[27]

Under current federal law, the interception of the contents of wire, oral, and electronic communications is regulated by the Wiretap Act of 1968, as amended by the ECPA (collectively "the Wiretap Act").[28] The Wiretap Act defines "interception" as "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."[29] "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in

---

25 Olmstead v. United States, 277 U.S. 438, 472-73 (1928).

26 Pub. L. No. 99-508, 100 Stat. 1848, 1860 (1986).

27 *See* Jonathan D. Barker, Note, *Society's Carnivores, Both Good and Bad. The Internet Wiretap*: *Why We Need it, and How it Should be Regulated*, 74 UMKC L. REV. 945, 948 (2006) (noting that although Congress did design the ECPA to distinguish between different stages of communication, the legislation nevertheless was designed for an "industry that was only in its infancy").

28 18 U.S.C. § 2511 (2000).

29 *Id.* § 2510(4).

part by a wire, radio, electromagnetic, photoelectronic or photooptical system."[30]

Generally, the Wiretap Act makes it unlawful to intentionally intercept any wire, oral, or electronic communication, or to intentionally disclose the contents of any such communication when there is reason to know that the information was obtained through unlawful interception.[31] Violators are subject to fines and imprisonment of not more than five years.[32] Moreover, any person whose wire, oral, or electronic communication is intercepted or disclosed in violation of the Wiretap Act may bring a civil action to recover from the person or entity that engaged in that violation.[33]

The statute defines an "electronic communications system" as any "wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[34] "Electronic storage" means any "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, or any storage of such communication by an electronic communications service for purposes of backup protection."[35]

The Wiretap Act permits the interception of communications using a pen register or a trap and trace device. Under the statute, the installation or use of a pen register or trap and trace device without first obtaining a court order is prohibited, unless the device is used by a provider of wire or electronic communication service (a) for the operation, maintenance, and testing of the service or the protection of the rights or property of the service provider; (b) to record the fact that the communication was initiated or completed in order to protect the service provider or another provider furnishing service toward the completion of the communications; or (c) where the consent of the user of that service has been obtained.[36] Pen registers are devices or processes used to record or decode dialing, routing, addressing, or signaling information of outbound wire or electronic communications. Similarly, trap and trace

---

30 *Id.* § 2510(12).
31 *Id.* § 2511(1).
32 *Id.* § 2511(4).
33 *Id.* § 2511(5).
34 *Id.* § 2510(14).
35 *Id.* § 2510(17).
36 *Id.* § 2511(2)(h).

devices or processes capture the electronic or other impulses that identify the originating number or other dialing, routing, addressing, and signaling information identifying the source of an incoming communication.

There are several exemptions to the Wiretap Act's prohibitions. For example, the "service provider exemption" states that it is not unlawful for an operator of a switchboard, or an officer, employee or agent of a provider of wire or electronic communications service whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity that is necessarily incident to the rendition of his service or the protection of the rights or property of the provider of that service.[37] There are also several exemptions that cover the interception of communications for law enforcement purposes, including § 2511(2)(a)(ii), which authorizes providers of wire or electronic communications services, landlords, custodians, and other persons to provide information, facilities, or technical assistance to law enforcement to intercept communications or conduct electronic surveillance pursuant to a court order or other written mandate from a government official, such as the U.S. Attorney General.

The "consent" exemption makes it lawful for a person "not acting under color of law" to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to the interception.[38] A number of states maintain more restrictive laws that require consent from all parties to a communication before interception is lawful.[39] In addition, the statute permits persons to intercept or access electronic communications made through an electronic communication system that is configured so that the electronic communications are "readily accessible to the general public."[40]

The "general public exemption" assumes that there are some forms of communication that have no "reasonable expectation of privacy."[41]

---

37 *Id.* § 2511(2)(a)(i). Except that a provider of wire communication service to the public may not utilize service observing or random monitoring except for mechanical or service quality control checks. *Id.*

38 *Id.* § 2511(2)(c).

39 *See e.g.*, CAL. PENAL CODE § 631(a); IND. CODE ANN. § 35-33.5-5-5 (requiring all party consent for intentionally interception of a communication)

40 18 U.S.C. § 2511(2)(g)(i).

41 A similar exemption for stored data that is available to the general public applies under the SCA, described below. In terms of communications open to the pubic, the

The legislative history of the Wiretap Act reflects congressional intent to make unlawful only the interception of communications that would reasonably be deemed "private."[42] This statutory exception creates problems for many modern forms of communications over "open" or shared networks, such as the Internet, that might not have been anticipated when the statute was drafted. Absent proof that electronic communications using shared networks or Internet-protocols would not be readily available to the general public, it may be left to the courts to determine whether these electronic communications are protected under the Wiretap Act.

D. The Stored Communications Act

Enacted as Title II to the ECPA, the SCA[43] makes it unlawful for a provider of an electronic communications service to knowingly divulge the contents of a communication while in electronic storage.[44] It also prohibits a person or entity providing remote computing services from knowingly divulging the contents of any communication which is carried or maintained on that service.[45] A "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communication system.[46]

However, there are several exemptions for disclosure of stored communications, including several exemptions that allow a service provider to divulge the contents of a communication. A service provider may divulge electronic communications with the lawful consent of the originator or an addressee or intended recipient of the communication.[47] Determining which persons or parties are the "addressee" or "intended recipient" can be difficult, as shown in the cases that have addressed the

---

Wiretap Act also states that it is not unlawful to intercept radio communications that are transmitted by any broadcasting station for use by the general public or for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service. 18 U.S.C. § 2511(g).

42 For a detailed history of the Wiretap Act and congressional intent, see *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005), which is discussed *infra* text accompanying notes 107-20.

43 Pub. L. 99-508, tit. II, 100 Stat. 1860, 201[1] (codified in 18 U.S.C. §§ 2701-2712).

44 18 U.S.C. § 2702(a)(1).

45 *Id*. § 2702(b)(2).

46 *Id*. § 2711(2).

47 *Id*. § 2702(b)(1).

issue, particularly with respect to personal emails sent to or from employees.[48]

Other exemptions: a service provider may disclose a stored electronic communication to an employee, to a person who is authorized to view the communication, to a person whose facilities are used to forward the communications to its destination, or to any person as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the service provider.[49] A service provider may disclose a stored electronic communication in the normal course of business while engaged in any activity which is necessarily incident to the rendition of service or to protect the rights or property of the provider.[50]

Additionally, a service provider must disclose electronic communications to a governmental entity pursuant to a warrant for communications stored for six months; for communications stored longer than six months, the service provider must disclose the communications to a governmental entity with a warrant or if the government entity provides prior notice to the subscriber and either (1) uses an administrative subpoena authorized by a federal or state statute or a federal or state grand jury; or (2) obtains a court order for the disclosure.[51] The service provider must disclose such information to a law enforcement agency if the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime, pursuant to provisions of the Crime Control Act, or if the provider reasonably believes that an emergency involving danger of death or serious injury to any person requires disclosure of the information with delay.[52]

E. The Communications Assistance for Law Enforcement Act

In 1994, Congress passed CALEA to aid law enforcement in its effort to conduct surveillance of citizens via digital telephone networks.[53] The

---

48 *See generally* Reno v. ACLU, 521 U.S. 844 (1997); Bartnicki v. United States, 532 U.S. 514 (2001).

49 18 U.S.C. § 2702(b).

50 *Id.* § 2702(b)(5) (except that the provider cannot use random monitoring except for mechanical or quality control checks).

51 *Id.* § 2703.

52 *Id.*

53 Pub. L. 103-414, tit. I, 108 Stat. 4279 (1994). The purpose, in part, is "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes." *Id.*

Produced by The Berkeley Electronic Press, 2007

Act obliges telephone companies to enable law enforcement agencies to tap any phone conversations carried out over their networks and to make available call detail records.[54] CALEA also stipulates that it must not be possible for a person to detect that a conversation is being monitored.[55]

Additionally, CALEA requires telecommunication carriers to ensure that all of their equipment, facilities, and services are capable of allowing government agents to intercept customer or subscriber communications.[56] Specifically, CALEA requires carriers to maintain equipment that: (1) permits the government, pursuant to court order, to intercept all wire or electronic communications carried by the carrier; (2) permits the government to access call-identifying information; (3) delivers the intercepting communications or call-identifying information to the government; and (4) facilitates such interceptions and access to call-identifying information unobtrusively and with a minimum of interference.[57] CALEA does not apply to information services, that is, services that generate, store, or process information including electronic publishing and electronic messaging services.[58] Telecommunications carriers that fail to honor the statute's requirements face civil fines of up to $10,000 a day.[59]

F. Customer Proprietary Network Information

Customer proprietary network information ("CPNI") is the data collected by telecommunications carriers about a customer's telephone calls.[60] "It includes the time, date, duration and destination number of

---

54 47 U.S.C. § 1002 (2000).

55 *Id.* § 1002(a)(4).

56 *Id.* § 1002(a).

57 *Id.* § 1002(a). "The term 'call-identifying information' means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." *Id.* § 1001(2).

58 *Id.* § 1002(b).

59 18 U.S.C. § 2522(c) (2000).

60 47 U.S.C. § 222(h)(1).

> The term 'customer proprietary network information' means (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer or carrier.

Id.

each call, the type of network a consumer subscribes to, and any other information that appears on the consumer's telephone bill."[61] For a long time, telecommunications companies were able to sell this data to third party companies for marketing purposes.[62] Faced with growing complaints about unwanted telephone solicitations and other marketing activities, in the Telecommunications Act of 1996, Congress adopted amendments to the Communications Act to require telecommunications companies to obtain customers' approval prior to sharing their CPNI with third parties.[63]

Section 222 of the Communications Act, which contains the CPNI provisions, requires telecommunications carriers "to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."[64] The original impetus for § 222 was consumer protection; it was intended to cut down on unwanted marketing and advertising solicitations of telephone customers.[65] Nevertheless, the NSA surveillance programs have thrust § 222 of the Communications Act squarely into the electronic privacy debate, as it appears that some of the surveillance activities involved the culling and screening of CPNI data.

G. The Foreign Intelligence Surveillance Act and the USA PATRIOT Act

In 1978, Congress enacted FISA and authorized the government to conduct electronic surveillance of foreign agents within the United States.[66] FISA also created an exclusive court of review which has jurisdiction over applications for electronic surveillance of foreign agents within the United States.[67] The court has jurisdiction to review the

---

61 Electronic Privacy Information Center (EPIC), CPNI, http://www.epic.org/privacy/cpni/ (last visited Mar. 25, 2007).

62 *Id.* The Telecommunications Act of 1996 required customers to "opt-in" before their CPNI was sold to marketing companies; however, there was debate over whether "opt-out" was a permissible option instead of the "opting-in" interpretation of the Act. *Id.*

63 47 U.S.C. § 222.

64 *Id.* § 222(a).

65 S. 652, 104th Cong. (1996). The purpose of the bill was "[t]o promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies." *Id.*

66 50 U.S.C. §§ 1801-1811 (2000).

67 *Id.* § 1803(a).

denial of any application for authority to conduct electronic surveillance.[68]

In 2001, in response to the September 11 terrorist attacks, Congress passed the USA PATRIOT Act of 2001, which amended FISA to account for new technologies and increased threats.[69] In particular, the USA PATRIOT Act expanded the pen register and trap and trace laws to include Internet communications and software programs in addition to telephone communications.[70] The USA PATRIOT Act permits the government to use pen registers to capture a vast amount of information, including telephone numbers, comprehensive "dialing, routing, addressing, or signaling information," and potential Internet-related information such as email and IP addresses.[71] In addition, the USA PATRIOT Act permits the government, without court approval, to share the contents of intercepted electronic communications among federal law enforcement and intelligence personnel.[72] In essence, the Act has enlarged the scope of surveillance statutes, expanded the coverage of those statutes to include new targets, lowered the government's threshold to engage in surveillance, and placed additional responsibilities on communications providers.[73]

As examined in this Article, one view of the NSA surveillance program is that it involved the crashing together of all of these statutes in a very public and unfortunate way. As best as can be told from the public record, the NSA program was not limited to "foreign agents"; instead, it culled electronic communications and records of thousands of telephone customers who were never considered threats to our national interests. We now know that the FISA procedures, which were intended to be a check on this type of government surveillance, were never

---

68 *Id.* § 1803(b). The FISA Court of Review is composed of three judges from the U.S. District Courts or Circuit Courts, appointed by the Chief Justice of the Supreme Court. *Id.*

69 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, 107 Pub. L. No. 56, 115 Stat. 212 (2001). The majority of the provisions of the PATRIOT Act that were due to end were renewed in March 2006. *See* USA PATRIOT Act Improvement Reauthorization Act of 2005, Pub. L. No. 109-77, 120 Stat. 192 (2006) (codified as amended in scattered sections and titles of the United States Code).

70 *See, e.g.*, United States v. Focarile, 340 F. Supp. 1033, 1039-40 (D. Md. 1972); *Administration's Draft Anti-Terrorism Act of 2001*: *Hearing Before the H. Comm. on the Judiciary*, 107th Cong. 50 (2001).

71 *Administration's Draft Anti-Terrorism Act of 2001*: *Hearing Before the H. Comm. on the Judiciary*, 107th Cong. 50 (2001).

72 18 U.S.C. § 2517 (2000).

73 Jaime S. Gorelick, John H. Harwood & Heather Zachary, *Navigating Communications Regulation in the Wake of 9/11*, 57 FED. COMM. L.J. 351, 354 (2005).

invoked.[74] Despite all of Congress's efforts over the decades to balance law enforcement needs with reasonable expectations of privacy, from the plaintiffs' point of view, the NSA surveillance programs ran roughshod over the privacy rights of thousands of U.S. citizens.

III. NEW TECHNOLOGIES CHALLENGE THE EXISTING LEGAL FRAMEWORK

It is the central premise of this Article that the federal framework of electronic privacy laws is sorely in need of an overhaul in light of today's ubiquitous communications technologies. A random sampling of cases involving alleged violations of the ECPA and other electronic privacy laws reveals a crazy-quilt of fact-specific outcomes. There is no unitary theme to these case precedents; they offer little practical guidance to those who engage in electronic communications and to those who are entrusted to protect electronic communications and records.

A. Electronic Messaging Services

A recurring theme in ECPA jurisprudence is the difficulty of courts in determining whether electronic communications are "in transit" and thus subject to the more strenuous provisions of the Wiretap Act, or, "stored communications" subject to the less burdensome SCA provisions. Given the widespread and expanding use of various forms of online communications, this is a statutory interpretation problem that is unlikely to go away absent revisions to federal law.

In *Quon v. Arch Wireless Operating Co., Inc.*, a California federal district court engaged in one of the most comprehensive discussions of "the legal boundaries of . . . privacy in this interconnected, electronic-communication age, one in which thoughts and ideas that would have been spoken personally and privately in ages past are now instantly text-messaged to friends and family via hand-held, computer assisted electronic devises[.]"[75] The *Quon* case arose from an internal investigation by the Ontario Police Department into the allegedly personal and illegal use of department-issued pagers by several employees.[76] The department had previously entered into a contract with Arch Wireless Operating Company, Inc. to provide its employees

---

[74] See Dan Eggen, *Records on Spy Program Turned Over to Lawmakers*, Wash. Post, Feb 1, 2007, at A02, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/01/31/AR2007013100921_pf.html (noting the administration's decision, in light of congressional and public pressure, to replace the controversial NSA warrantless surveillance program with a program subject to the FISA secret court).

[75] 445 F. Supp. 2d 1116, 1121 (C.D. Cal 2006).

[76] *Id.* at 1121-22.

with pagers and other wireless communication devices.[77] The department required that all of its employees review and sign the department's equipment use policy which applied to "the use of any city-owned computer equipment, computer peripherals, city networks, the Internet, e-mail services or other city computer related services."[78] The policy further stated that the department recorded and reviewed access to all Internet sites and that the department reserved the "right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources."[79]

At various times, the department informed Quon, one of the plaintiffs in the case, that the department's pagers were considered to be e-mail messages that fell within the department's policy and were therefore subject to audit.[80] The department, however, "had an unstated policy of agreeing not to audit the use of the pagers whenever overages existed so long as the personnel in question paid the department for the overage."[81] In any case, the department did not have the ability to review pager messages without first contacting Arch Wireless and requesting that they generate a transcript of the messages.[82] Eventually, the department decided to change its informal policy and audited the pager transcripts to determine to what extent the overages were caused by personal use and contacted Arch Wireless for copies of the pagers' transcripts.[83] Prior to providing the department with the transcripts, Arch Wireless "confirmed that the pagers were owned by the city and that the request came from the designated contact person. After satisfying itself of these two points, Arch Wireless provided transcripts of the contents of the messages sent and received by the pagers during the time in question."[84]

Upon reviewing the transcripts, the department determined that Quon had been using his pager for personal reasons, including the transmission of sexually explicit messages to his wife and girlfriend.[85] The transcripts were turned over to Internal Affairs who took action

---

77 *Id.* at 1122-23.
78 *Id.* at 1123.
79 *Id.*
80 *Id.* at 1124.
81 *Id.*
82 *Id.*
83 *Id.* 1125-26.
84 *Id.* at 1126.
85 *Id.*

against the plaintiffs.[86] The collective plaintiffs, in turn, filed suit against the department and Arch Wireless, asserting violation of the SCA.[87]

In defense, Arch Wireless argued that 18 U.S.C. § 2702(b)(3) permits a carrier to disclose the contents of a stored electronic communication when done "'with the lawful consent of the originator or an addressee or intended recipient of such communication [in the case of an electronic communication service], or the subscriber in the case of remote computing service.'"[88] The key issue focused on whether "the service provided by Arch Wireless—that is, of being able to retrieve for its subscribers text messages that have been sent over its communication network and are held in long-term storage on its computers—constitutes a remote computing service, or, rather, is more properly characterized as an electronic communication service."[89] According to the court, the classification of Arch Wireless's service would determine whether Arch Wireless was exempt under the statute.[90]

Arch Wireless argued that because it stored the messages on a computer, the service was akin to e-mail and therefore a remote computing service. But the court noted that unlike email, which permits the original sender to access the message even when stored, the text-messages could not be retrieved without Arch Wireless's assistance.[91] As such, the court addressed whether such a "direct-accessibility feature" was a necessary component of a remote computing service.[92] Although the plaintiffs argued that interconnectivity was a key element of a remote computing service, the court found that the statute's language did not specifically require or even address interconnectivity.[93] According to the court, "[u]nder the SCA, the centrality a computer plays in facilitating the communication is key to Congress' definition of a remote computing service."[94] The court found this definition no longer particularly relevant considering the ubiquity of computers as forms of electronic communication.[95] For example, the transmission of text messages

---

86 *Id.*

87 *Id.* at 1128. Quon also asserted violations of the Fourth Amendment and state law claims for violations of the California Constitution, California Penal Code, invasion of privacy, and defamation. *Id.*

88 *Id.* at 1130 (quoting 18 U.S.C. § 2702(b)(3)).

89 *Id.*

90 *Id.*

91 *Id.* at 1131.

92 *Id.*

93 *Id.*

94 *Id.* at 1132.

95 *Id.* at 1133.

probably satisfied the definition of an electronic communication whereas the long-term storage of such messages might qualify as a remote computing service.[96] Acknowledging that Arch Wireless's services incorporated elements of both types of services, the court held that given that the retrieval of messages in long-term storage was at issue, § 2702(b)(3)'s subscriber exception applied.[97]

Next, the court addressed whether the department had violated Quon's reasonable expectation of privacy by reviewing his messages.[98] According to the court, the department failed to provide Quon with fair notice that the pager communications were open to public view because of its contradictory official and informal policies.[99] The court found that the department's informal policy of not reviewing the contents of messages so long as the user paid the overage charges undercut the formal policy provision allowing the department to review and monitor all pager messages.[100] Specifically, the court noted that

> it is unreasonable to expect that an employee would assume that some other unstated norm should inform their opinion on how much privacy to expect in using an employer's equipment once that employer expressly informs his or her employees of an actual policy regarding the use of that very equipment.[101]

Since Quon had a reasonable expectation of privacy in the messages the department's audit was not justified.[102] The outcome of the claim depended largely on whether the department read the transcripts in order to discover misconduct or to improve efficiency.[103] As such, the court denied the defendant's motion for summary judgment so that a jury could determine the purpose of the audit.[104]

---

96 *Id.* at 1136-37.
97 *Id.* at 1137.
98 *Id.* at 1140.
99 *Id.*
100 *Id.* at 1141.
101 *Id.* at 1142.
102 *Id.* at 1143-44.
103 *Id.* at 1146.
104 *Id.*

B. Internet-Based Communications

Email has largely supplanted the telephone as the main form of communications in the business world.[105] From the law enforcement perspective, an agent can examine email by "acquiring a Title I content warrant, a Title II store communications order, a Title III pen register order, or a FISA warrant . . . ."[106] Perhaps paradoxically, given the ubiquitous nature of email and the use of Internet-based message services, the courts continue to grapple with statutory definitions for these technologies. Defining these technologies is a critical predicate to determining the extent to which they are entitled to privacy protection under federal law.

The recent case of *United States v. Councilman* underscores the difficulty of squeezing twenty-first-century technology into twentieth-century laws.[107] In *Councilman*, defendant Bradford C. Councilman was the vice-president of "an online rare and out-of-print book listing service" called Interloc.[108] In addition to the book listing service, Interloc provided customers with email accounts and acted as a service provider for these accounts.[109] To better target customers and respond to growing competition from Amazon.com, Interloc intercepted and copied email communications sent from Amazon.com to its customers before delivering the messages into customer email accounts.[110] The government charged Councilman with Wiretap Act violations due to his intercepting emails.[111] In defense, Councilman argued that the intercepted e-mails were in electronic storage at the time and therefore not subject to the Wiretap Act's prohibition against intercepting electronic communications.[112] The district court dismissed the indictment, a divided panel of the First Circuit affirmed; an en banc panel reversed and remanded.[113]

---

105 Ferris Research, http://www.ferris.com/research-library/industry-statistics/ (last visited Mar. 25, 2007). Industry statistics show that in 2006, business email users sent over 6 trillion non-spam e-mail messages. *Id.* Every day, approximately 25 billion non-spam e-mail messages are sent. *Id.*

106 Holland, *supra* note 6, at 407.

107 418 F.3d 67 (1st Cir. 2005).

108 *Id.* at 70.

109 *Id.*

110 *Id.*

111 *Id.* at 70-71.

112 *Id.* at 71.

113 *Id.* at 69, 85.

On rehearing, the First Circuit disagreed with Councilman's assertion and found that the e-mail messages were electronic communications.[114] The crux of the analysis focused on the definition of electronic communication and whether communications that went into momentary electronic storage qualified as electronic communications.[115] Accordingly, the court began its analysis by reviewing the language of the Wiretap Act, concluding that the "ECPA's plain text does not clearly state whether a communication is still an 'electronic communication' within the scope of the Wiretap Act when it is in electronic storage during transmission. Applying canons of construction does not resolve the question. Given this continuing ambiguity, we turn to the legislative history."[116] Based on the Act's legislative history, the court found that there was no evidence that Congress intended to exclude the temporary storage of an electronic communication during transmission from the scope of the Wiretap Act.[117] As a result, the court concluded that the term "electronic communication" as used in the Wiretap Act included the temporary storage of electronic communications.[118]

The First Circuit reached its ultimate decision based primarily on its interpretation of the Wiretap Act's legislative history, rather than on an analysis of the statute itself. Given the election to steer around the plain language of the statute, it is perhaps not surprising that other courts have reached different conclusions with respect to their treatment of email under the Wiretap Act.[119] Similarly, several courts interpreting state statutes similar to ECPA have found that email is a recorded medium in which the communication is sent to other computers and is therefore subject to interception since the sender would not have a reasonable expectation of privacy.[120]

---

114 *Id.* at 79.

115 *Id.* at 72-79.

116 *Id.* at 76.

117 *Id.* at 76-79.

118 *Id.* at 79.

119 *See* Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994) (holding that the interception of a private electronic email which was stored on a bulletin board did not fall within the scope of the Wiretap Act); *see also* Konop v. Hawaiian Airlines, 302 F.3d 868, 872 (9th Cir. 2002) (endorsing the *Steve Jackson* view that communications cannot be intercepted while in electronic storage).

120 *See* Commonwealth v. Proetto, 771 A.2d 823 (Pa. Super. Ct. 2001) (standing for the proposition that the sender has no privacy interest in the email communication because the recipient's computer would record the email); Holland, *supra* note 6, at 409-10 (discussing State v. Townsend, 57 P.3d 255 (Wash. 2002)).

Courts have also struggled to determine where web sites and Internet "bulletin boards" fit within the Wiretap Act's statutory framework. In *Konop v. Hawaiian Airlines*, an airline employer had used access codes given by Konop, an employee, to other individuals to access Konop's website, where unfavorable comments about the employer had been posted.[121] Konop claimed that the airline had unlawfully intercepted private electronic communications in violation of the Wiretap Act.[122]

The *Konop* court considered whether the airline had violated an employee's privacy rights by accessing his private website.[123] The court noted that the intersection of the ECPA and SCA was a "convoluted[ ] area of the law" and that "[c]ourts have struggled to analyze problems involving modern technology within the confines of this statutory framework . . . ."[124] After reviewing the legislative history, the court concluded that Congress's intent in enacting the ECPA was to protect private electronic communications.[125] Nevertheless, the Internet makes it almost impossible to determine the identity of web visitors or to determine whether a visitor was actually eligible to view a given website.[126] The Ninth Circuit held that the website qualified as an electronic communication under the Wiretap Act, but that websites can only be intercepted under the Wiretap Act during active transmission and not while a message is in electronic storage.[127] Consequently, the *Konop* court found that the airline had not violated the Wiretap Act.

Next, the *Konop* court considered whether the airline had violated the SCA by accessing the employee's website without proper authorization.[128] The SCA exempts from its requirements persons who are users of the service or who are the intended recipients of the communication.[129] Finding that the airline was not an authorized user of the website, the court dismissed the airline's motion for summary judgment.[130] The *Konop* court recognized that "until Congress brings the laws in line with modern technology, protection of the Internet and

121 302 F.3d at 872.
122 *Id.* at 873.
123 *Id.* at 874.
124 *Id.*
125 *Id.* at 875.
126 *Id.*
127 *Id.* at 875-76, 878.
128 *Id.* at 879.
129 *Id.* at 880.
130 *Id.*

websites such as Konop's will remain a confusing and uncertain area of the law."[131]

The courts and government have strained to fit other Internet-based communications technologies, such as VOIP and instant messaging, into the existing federal privacy law framework.[132] VOIP technology allows users to place what appear to be traditional telephone calls, but instead the voice data is transferred via Internet protocol (where multiple packets of unrelated voice data are essentially "streamed" together over broadband connections, and then reassembled on the receiver's end of the communication) rather than dedicated telephone circuits.[133] Internet-based communication technologies strain the existing legal system because courts have often refused to "recognize a 'reasonable expectation of privacy' in Internet electronic communications reasoning that, as the Internet is public in nature, communications therein should receive a disfavored privacy protection status."[134]

Although VOIP services are not considered "telecommunications common carrier" services, such as conventional telephone service, the FCC recently concluded, after considerable coaxing from the FBI, that CALEA applies to facilities-based broadband Internet access services and interconnected VOIP.[135] According to the Commission, Congress intended the term "telecommunications carrier" in CALEA to apply to a broader group of entities than in the Communications Act.[136] "In today's technological environment, where IP-based broadband networks are rapidly replacing the legacy narrowband circuit-switched network, various types of packet-mode equipment are increasingly being deployed to 'originate, terminate, or direct communications' to their intended destinations."[137]

---

131 *Id.* at 874.

132 A report in 2004 by the Pew Institute indicates that over 53 million Americans use instant messaging and that over 11 million employees use instant messaging at work. EULYNN SHIU & AMANDA LENHART, PEW INTERNET & AMERICAN LIFE PROJECT, HOW AMERICANS USE INSTANT MESSAGING i, ii (2004), *available at* http://www.pewinternet.org/pdfs/PIP_Instantmessage_Report.pdf.

133 Barker, *supra* note 27, at 952-53.

134 Daniel B. Garrie, Matthew J. Armstrong & Donald P. Harris, *Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected*, 29 SEATTLE U. L. REV. 97, 122-23 (2005).

135 In the Matter of Communications Assistance for law Enforcement Act and Broadband Access and Services, First Report and Order and Further Notice of Proposed Rulemaking, FCC 05-153, ¶ 8 (Sept. 23, 2005).

136 *Id.* ¶ 10.

137 *Id.* ¶ 11.

The Commission concluded that CALEA covers all facilities-based providers of broadband Internet access including wireline, cable modem, satellite, wireless, fixed wireless, and broadband via powerline providers.[138] Specifically, the Commission found that that CALEA created three categories of telecommunication services to cover pure telecommunications (fully covered by CALEA), pure information (not covered by CALEA), and hybrid services (partially covered by CALEA).[139] According to the Commission, broadband and VOIP services fall within the hybrid services tier and are therefore partially covered by CALEA.[140]

Privacy groups attacked the Commission's decision as contrary to CALEA's statutory provisions and a threat to individual privacy.[141] However, in *American Council on Education v. FCC*, the D.C. Circuit denied a petition for review based on a *Chevron* deference analysis of the Commission's Report and Order.[142] The plaintiff had challenged the FCC's decision on the grounds that the Commission, in proceedings implementing the Telecommunications Act of 1996, had previously classified broadband Internet access as information services.[143] The court dismissed the plaintiff's argument, citing differences between the two statutes and finding that the Commission's decision to classify broadband Internet access under CALEA as a hybrid service was a "reasonable policy choice" under *Chevron*.[144] In essence, the FCC is treating VOIP communications as akin to "common carriage" for purposes of CALEA's law enforcement mandates; however, it may be up to the courts to determine whether VOIP communications will be afforded privacy protection under federal electronic privacy laws.

C. Cellular Telephone Interceptions and Surveillance

Another example of how technology has outgrown the existing legal framework is the use of "roving bugs" by law enforcement officials. A "roving bug" occurs when a government agent, "with court approval and mobile-phone carrier assistance required by law[,] can exploit mobile phones over the air in such a way that microphones in handsets are activated and nearby conversations picked up by federal

---

138 *Id.* ¶ 24.
139 *Id.* ¶ 16-18.
140 *Id.* ¶ 24-45.
141 Jay Lyman, *FCC Criticized for VoIP Tapping Requirements*, TECHNEWSWORLD, Aug. 11, 2005, http://www.technewsworld.com/story/45416.html.
142 451 F.3d 226 (D.C. Cir 2006).
143 *Id.* at 227-28.
144 *Id.* at 228-36.

investigators."[145] In order to initiate the microphone in a mobile phone the carrier must first place the phone into a diagnostic mode. Once this occurs, the microphone can pick up conversations in the area around the phone without the user knowing that the phone is recording.

Although "roving bugs" have been recognized as legitimate surveillance tools for several years, a recent New York case demonstrates how the cellular telephone has expanded the scope, effectiveness, and invasiveness of such surveillance tools.[146] In *United States v. Tomero*, the FBI requested and received court authorization to use roving bugs to record the conversations of several individuals associated with an organized crime family.[147] The FBI used this authorization to record hundreds of hours of conversations through several cell phones, regardless of whether the phones were turned on or off.[148] The court rejected all of the defendant's constitutional and non-constitutional defenses.[149] First, the court rejected the defendant's claim that the use of roving bugs was unconstitutional under the Fourth Amendment because the warrant did not limit the search to a particular place.[150] Second, the court held that the FBI's warrant applications satisfied 18 U.S.C. § 2518 because they indicated that alternative methods were unlikely to succeed, they targeted conversations that included at least one known subject, and because the government was only required to show "that the defendants moved often enough that the regular procedures for obtaining a warrant would inhibit the interception of some conversations needed for the investigation."[151]

In *United States v. Forest*, two defendants challenged their arrests for cocaine possession, claiming statutory and constitutional violations arising from data intercepted from their cellular phones by law enforcement officials who had previously obtained court authorization

---

145 Jeffrey Silva, *Roving Bugs*: *Wiretap Law Can Turn Cell Phone into Microphone*, RCR WIRELESS NEWS, Dec. 16, 2006, at 1.

146 *See, e.g.*, United States v. Bianco, 998 F.2d 1112, 1122-24 (2d Cir. 1993) (upholding the constitutionality of "roving bugs" for interception of oral communications that are not transmitted via wire or electronic means); *see also* United States v. Gaytan, 74 F.3d 545. 553 (5th Cir. 1996) (upholding the constitutionality of "roving bugs" for the interception of oral communications that are not transmitted via wire or electronic means); United States v. Petti, 973 F.2d 1441 (9th Cir. 1992), *cert. denied*, 507 U.S. 1035 (1993).

147 462 F. Supp. 2d 565 (2006).

148 *Id.* at 566-57.

149 *Id.* at 572.

150 *Id.* at 569.

151 *Id.* at 572.

to intercept the conversations.[152] The authorization also required the cellular provider to disclose to the government defendants' subscriber information, toll records, and other relevant information.[153] Based on information received through the cellular phone interceptions, law enforcement officials began conducting physical surveillance of the defendants, but found that they were unable to maintain constant visual contact.[154] "In order to reestablish visual contact, a DEA agent dialed [defendant's] cellular phone (without allowing it to ring) several times that day and used Sprint's computer data to determine which cellular transmission towers were being 'hit' by [defendant's] phone. This 'cell-site data' revealed the general location of [defendant]."[155] The officers repeated this procedure in order to maintain their physical surveillance of the defendants.[156]

On appeal, defendants argued that the government's use of their cell phone data turned their phones into tracking devices in violation of the Wiretap Act and the Fourth Amendment.[157] But the Sixth Circuit agreed with the district court's finding that the cellular phone data was an electronic communication rather than a wire or oral communication.[158] As a result, the Circuit Court dismissed defendant's request to suppress the evidence under the Wiretap Act because the Act only permitted suppression of wire or oral communications.[159] Next, the court addressed defendant's claim that the government's use of his cellular phone as a tracking device violated 18 U.S.C. § 3117(a), governing the use of mobile tracking devices, and determined that § 3117 did not provide for suppression as a remedy to the government's actions.[160] The court also addressed the defendants' argument that the government's use of their cellular phones as tracking devices violated their Fourth Amendment rights, but held that defendants did not have a claim because their data was intercepted only while they traveled on public

---

152 355 F.3d 942, 946-47 (6th Cir. 2004).

153 *Id.*

154 *Id.*

155 *Id.*

156 *Id.* at 947-48.

157 *Id.* at 948. Another interesting issue is whether the location information obtained from the defendant's cellular phones even qualifies as "call-identifying" data under CALEA. For a further discussion of this issue, see *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 315 (2004).

158 *Forest,* 355 F.3d at 948-49. The court acknowledged that there was a strong argument that "cell-site data is not a form of *communication* at all." *Id.* at 949.

159 *Id.*

160 *Id.* at 949-50.

highways.[161] Instead, the court noted that the cell-site data was "simply a proxy for [defendant's] visually observable location."[162]

Tomero and *Forest* reveal how the government can easily intercept conversations or track individuals' movements through cellular phones. In addition, some cellular phone carriers and private companies have begun offering products that allow cellular phone users to track the movements of other cellular phone users. In late 2006, Boost Mobile, a pre-paid cellular phone service owned by Sprint, introduced a mobile-tracking system service that allows users to track the whereabouts of friends.[163] Loopt, the company that created the system, claims to have "developed safeguards to ensure that mobile-phone users are tracked only by people they know and only when they want to be found."[164] Other cellular phone carriers have hesitated to implement similar systems because of privacy and safeguard concerns. Verizon Wireless for example, has stated "concerns about making sure a tracking service is done right, . . . The last thing we want to do is let a genie out of a bottle and find that the service is misused."[165]

D. Automobile Communications Surveillance

Over the past few years, automobile manufacturers have begun to equip their vehicles with telecommunication devices that provide drivers with on-board services such as navigation, information services, emergency services, and road-side assistance. These services generally operate through a combination of cellular and global positioning system technologies. General Motors has incorporated this technology into at least 50 of its 2007 models.[166] Although these systems provide drivers with important, and at times life-saving services, they also provide law enforcement officials with a powerful and tempting "roving bug" surveillance tool.

As these services have become widespread, it has been left to the courts to determine whether they are covered under federal wiretap and surveillance laws. In *The Company v. United States*, the Ninth Circuit considered "whether the statute governing private parties' obligations to

---

161 *Id.*

162 *Id.* at 951.

163 Marguerite Reardon, *Mobile Phones that Track Your Buddies*, Nov. 14, 2006, http://news.com.com/Mobile+phones+that+track+your+buddies/2100-1039_3-6135209.html.

164 *Id.*

165 *Id.*

166 Onstar, 2007 Onstar Equipped Vehicles, http://www.onstar.com/us_english/jsp/equip_vehicles/07_vehicles.jsp (last visted Mar. 28, 2007).

assist the federal government in intercepting communications" required one such service provider to assist the government in intercepting conversations through the service.[167] In that case, the FBI sought to use the Company's auto service as a "roving bug" and obtained several court orders requiring the Company to help the FBI intercept conversations through the system.[168] The lower court that granted the FBI's requests determined that the service provider was a "telecommunications carrier" and "provider of wire or electronic communication service" under 18 U.S.C. § 2518(4) and § 2522.[169] Objecting to the use of its product for surveillance purposes, the Company expressed concern that "if no operator is on the line and only the FBI is listening in, there will be no response to the subscriber's emergency signaled by the transmitted tone."[170]

On review, the Ninth Circuit considered the key question: "When may a company, not a common carrier but possessing a unique ability to facilitate the interception of oral communications, be required to assist law enforcement in intercepting such communications?"[171] Comparing the facts of the case to the ECPA's statutory requirements, the court found that the conversations intercepted through the system qualified as "oral communications" under § 2510(3) because the occupants of the vehicle reasonably expected that their conversations were private and not subject to interception.[172] Next, the court addressed whether the Company had an obligation to assist the FBI in intercepting the communications.[173] In order to answer this question, the court had to determine whether the Company was a "provider of wire or electronic communication service, landlord, custodian, or other person" as required by § 2518(4).[174] The Company claimed that it was not a provider of such a service because it did not operate the cellular service incorporated into the system.[175] After analyzing the statute's language, the court determined that the Company qualified as a "provider of wire or electronic communication service" because the Company billed the customers directly for the service and because the customers had no

---

167 349 F.3d 1132, 1134 (9th Cir. 2003).

168 *Id.*; *see* Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 223 n.30 (2006).

169 *The Company*, 349 F.3d at 1134.

170 *Id.* at 1135.

171 *Id.* at 1137.

172 *Id.* at 1138.

173 *Id.*

174 *Id.* at 1139.

175 *Id.*

contact with the cellular telephone company.[176] According to the court, "[t]he service-providing structure here is very much akin to circumstances in which an established long distance telephone carrier offers *local* phone service even though it does not own or operate any of the local infrastructure."[177] The court concluded that for purposes of § 2518(4), the statute does distinguish between "those service providers that furnish their own facilities, and those service providers like the Company that do not."[178]

The court also held that the Company qualified as an "other person" under § 2518(4), noting that the term "other person" includes individuals or entities that provide a service to the targets of electronic surveillance and who are uniquely able to assist law enforcement officials in intercepting communications through their facilities or service.[179] Specifically, the court found that "The Company [was] uniquely situated to facilitate the interception of the oral communications within the vehicle . . . ."[180] The court held that the Company qualified as an "other person" and fell within the purview of § 2518(4)'s requirements.[181]

Having determined that the Company was required to comply with the ECPA's provisions, the court addressed whether the FBI's requests went too "far in interfering with the service provided by the Company" under § 2518, which required that the assistance be provided with a "minimum of interference with the services" of the provider.[182] Although the court recognized that § 2518 permits a certain level of interference, the court found under the facts of the case that the FBI's requests were too obtrusive because they completely shut down the provider's service.[183] The court concluded that although the Company fell within the purview of § 2518(4) as both a "provider" and an "other person," the district court erred by granting the FBI's requests because

---

176 *Id.* at 1140.
177 *Id.*
179 *Id.*
179 *Id.* at 1141-42.
180 *Id.* at 1143.
181 *Id.*
182 *Id.* at 1144.
183 *Id.* at 1146. *See* Dorothy L. Glancy, *Privacy on the Open Road*, 30 OHIO N.U. L. REV. 295, 318 n.90 (2004); Eva Marie Dowdell, Note & Comment, *You are Here! Mapping the Boundaries of the Fourth Amendment with GPS Technology*, 32 RUTGERS COMPUTER & TECH. L.J. 109, 116 n.60 (2005).

the Company "could not assist the FBI without disabling the System in the monitored car."[184]

A dissenting judge opined that the FBI's actions were in compliance with the federal statutes, and was not particularly swayed by the potential harm that this surveillance program could cause to the Company's "emerging business . . . because people might not subscribe to its service if they become aware of [the] potential for court-ordered eavesdropping[.]"[185] Of course, that was presumably why the service provider prosecuted this appeal: to avoid having its safety and convenience product from intentionally becoming a primary tool for law enforcement activities.

IV. THE NSA SURVEILLANCE PROGRAM AND FEDERAL PRIVACY LAW

In adopting the ECPA, CALEA, and FISA, Congress intended to strike a balance between individual privacy interests and legitimate law enforcement needs. Recent revelations about the NSA's secret surveillance programs suggest that these statutes may no longer be capable of balancing these competing interests. And, as discussed above, the proliferation of new technologies has given law enforcement new surveillance tools that further strain the existing legal framework and place increasing burdens on the judicial system to strike the appropriate balance.

The foundation for *Hepting* and other related NSA surveillance cases was laid by the press.[186] On December 16, 2005, *The New York Times* reported that President Bush had previously authorized the NSA to engage in the covert, warrantless wiretapping of U.S. citizens.[187] The story immediately caused a public uproar that forced the government to defend its action as a key weapon in the fight against terrorism.

In its defense, the government revealed select details about the program, including that: (1) the program performed wiretaps on international communications between U.S. citizens and foreign entities; (2) the program was implemented by non-judicial "career professionals" at the NSA when they had reasonable grounds to suspect that a party to a communication was a member of a foreign terrorist organization; (3)

---

184 *The Company*, 349 F.3d at 1146.

185 *Id.* at 1149.

186 *See infra* text accompanying notes 207-15 (discussing *Hepting*).

187 Eric Lichtblau & James Risen, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

Produced by The Berkeley Electronic Press, 2007

the wiretaps targeted U.S. citizens; and (4) the government did not seek FISA or any other judicial warrants prior to beginning its surveillance.[188] Not surprisingly, litigation ensued.

Similarly, in *ACLU v. NSA*, a group of citizens filed suit against the NSA challenging the constitutionality of the program under the Fourth Amendment.[189] The plaintiffs consisted of individuals whose international telephone and internet communications were intercepted and recorded by the government.[190] Engaging in a lengthy review of the judicial precedent concerning government electronic surveillance, the federal district court focused the bulk of its analysis on whether the executive branch had exceeded the scope of its constitutional powers and taken on a role traditionally reserved for the judiciary and Congress under the separation of powers. For example, the court noted that in *United States v. United States District Court*,[191] the Supreme Court established that the Fourth Amendment requires the government to seek a warrant prior to engaging in domestic security surveillance.[192] The court went on to cite Justice Powell's opinion for the proposition that the executive branch's duty is to "enforce the laws, to investigate, and to prosecute . . . . But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks."[193]

In addition, the court noted that Congress designed FISA to provide the executive branch with a clear and well-defined framework for engaging in electronic surveillance for foreign intelligence.[194] Further, the court noted that in enacting FISA, Congress had "made numerous concessions to stated executive needs." The problem identified by the court is that post-911, the government no longer seems satisfied to limit its operations as required under the current legal framework. It seems that the executive branch implemented the NSA without regard to FISA or the Fourth Amendment.[195] "The President of the United States, a creature of the same Constitution which gave us these Amendments, has undisputedly violated the Fourth in failing to procure judicial orders as

---

188 Fletcher N. Baldwin, Jr. & Robert B. Shaw, *Down to the Wire: Assessing the Constitutionality of the National Security Agency's Warrantless Wiretapping Program: Exit the Rule of Law*, 17 J. LAW & PUB. POL'Y 429, 432 (2006).

189 438 F. Supp. 2d 754, 758 (E. D. Mich 2006).

190 *Id.*

191 407 U.S. 297 (1972).

192 *ACLU*, 438 F. Supp. 2d at 772.

193 *Id.* at 775.

194 *Id.* at 773.

195 *Id.* at 775.

required by FISA, and accordingly has violated the First Amendment Rights of these Plaintiffs as well."[196]

The government argued that it had not violated the Constitution because Congress had granted the president the power to use all necessary and appropriate force to prevent future terrorist attacks in the Authorization for Use of Military Force ("AUMF") passed shortly after 9/11.[197] The court dismissed this argument because the AUMF does not address intelligence or surveillance, and, because FISA and the ECPA clearly state that surveillance may only be conducted pursuant to prior warrants.[198] Additionally, the court also dismissed the government's claim that the president's inherent powers were sufficient to authorize the NSA program; in the end, the court granted the plaintiff's request for a permanent injunction.[199]

In response, the government filed an appeal with the Sixth Circuit.[200] In addition, approximately six months after the *ACLU v. NSA* opinion, the government voluntarily changed the NSA surveillance program so that the FISA court would review each surveillance request.[201] Although many privacy advocates cheered the government's decision and characterized the change as a "retreat," the government continues to defend the president's authority to engage in unauthorized wiretapping.[202] At the same time, the government moved the Sixth Circuit to dismiss the lawsuit since it had subsequently placed the NSA program under FISA review.[203] In its filing, the government stated that the plaintiffs' challenge was moot because the challenged surveillance activity no longer existed.[204] However, in a public statement the ACLU

---

196 *Id.* at 776.

197 *Id.* at 779.

198 *Id.*

199 *Id.* at 780-82.

200 Dan Eggen, *Court Will Oversee Wiretap Program,* WASH. POST, Jan. 18, 2007, at A01.

201 *Id.*

202 *See id.* Eggen noted:

> White House and Justice officials said the president was not retreating from his stance that he has the constitutional and legislative authority to order warrantless surveillance on international calls but [that] the new rules promulgated by the surveillance court have satisfied concerns about whether the FISA process can move quickly enough to authorize surveillance.

Id. Further, the Justice Department has continued to argue that federal judges are not qualified to decide terrorism issues. *Id.*

203 Dan Eggen, *Dismissal of Lawsuit Against Warrantless Wiretaps Sought*, WASH. POST, Jan. 26, 2007, at A05.

204 *Id.*

stated that "'[t]he FISA court didn't reach out on its own to do something; the government asked it to do something, . . . And absent a ruling, they are free to return to their illegal conduct again.'"[205]

The NSA program launched a slew of lawsuits against the companies that cooperated with the government by providing access to customer information. Although most of these cases remain in litigation, they nevertheless demonstrate that companies that cooperate with the government cannot necessarily rely on the statutory safe harbors for protection from angry customers. For example, in *Hepting* and *Terkel v. AT&T*, two district courts reached two different conclusions about the legality of the NSA programs despite many common facts.

In *Hepting*, plaintiffs filed suit against AT&T for essentially collaborating with the NSA wiretap program.[206] AT&T immediately moved to dismiss the case alleging that the plaintiffs lacked standing.[207] In addition, the government moved to intervene as a defendant and moved to dismiss the claim based on the state secrets privilege.[208] However, according to the *Hepting* court, the government could not claim the state secrets privilege because it had disclosed significant information to the public about the program; as a result, the court rejected the government's motion to dismiss.[209] In support, the court noted that "the very subject matter of this action is hardly a secret . . . public disclosures by the government and AT&T indicate that AT&T is assisting the government to implement some kind of surveillance program."[210]

For its part, AT&T argued that plaintiffs lacked standing and that AT&T was entitled to statutory, common law, and qualified immunity.[211] More specifically, ATT argued that under 18 U.S.C. § 2511(2)(a)(ii)(B), "telecommunications providers are immune from suit if they receive a government certification authorizing them to conduct electronic surveillance."[212] The court found that it did not need to address AT&T's claim because the plaintiffs pled that AT&T acted outside the scope of government certification.[213] In essence, the *Hepting* court held that the

---

205 *Id.*
206 439 F. Supp. 2d 974, 978 (N.D. Cal. 2006).
207 *Id.* at 979.
208 *Id.*
209 *Id.* at 986-94 (dismissing the case based on the Toten/Tenent bar).
210 *Id.* at 994.
211 *Id.* at 999.
212 *Id.* at 1001.
213 *Id.* at 1002.

issue of whether the government authorized AT&T to disclose customer records was an issue that warranted further litigation.[214]

To further confuse matters, in *Terkel*, another district court addressing similar claims against AT&T reached virtually opposite conclusions. In *Terkel*, the district court addressed a challenge to AT&T's disclosure of records of customer communications.[215] Plaintiffs alleged that AT&T had violated 18 U.S.C. § 2702(a)(3) by releasing records to the NSA.[216] Although the court denied AT&T's motion to dismiss, the court did grant the government's motion to dismiss because "in contrast to the alleged content monitoring that is a key focus of the *Hepting* case, there have been no public disclosures of the existence or non-existence of AT&T's claimed record turnover—the sole focus of the current complaint in the present case—that are sufficient to overcome the government's assertion of the state secrets privilege."[217] The court concluded that § 2702(a)(3) provides private individuals with enforceable rights against carriers that disclose communication records to third parties; having found that plaintiffs alleged a sufficient injury under the statute, the court denied AT&T's motion to dismiss.[218]

Nevertheless, the government convinced the court to dismiss the case based on the state secrets doctrine.[219] After engaging in a lengthy review of the state secrets doctrine precedent, the court concluded that "based on the government's public submission, the Court is persuaded that requiring AT&T to confirm or deny whether it has disclosed large quantities of telephone records to the federal government could give adversaries of this county valuable insight into the government's intelligence activities."[220] Because the plaintiffs could not establish standing without such information from AT&T, the court granted the government's motion to dismiss.[221]

V. LESSONS LEARNED AND THE WAY FORWARD

Although the NSA surveillance litigation is ongoing, it is not too early to draw conclusions from the courts' initial decisions. Likewise, court decisions that have attempted to apply federal electronic privacy

---

214 *Id.* at 1003.
215 441 F. Supp. 2d 899, 900 (N. D. Ill 2006).
216 *Id.* at 901.
217 *Id.*
218 *Id.* at 904.
219 *Id.*
220 *Id.* at 917.
221 *Id.*

law to cellular phones, Internet-based services, and other new technologies provide perhaps unintended lessons. The clear implication from all of these hotly contested cases is that an understanding of electronic privacy law has become critical whether you are a business, a government agent, or a private citizen, given the ubiquitous nature of the communications services we use every day.

From the perspective of an employer, corporation or enterprise, even those that are not technically "communications service providers," the early lessons from the NSA cases are fairly apparent, the main one being: ask for a court order before participating in any law enforcement surveillance activity. It may be hard to say "no" to law enforcement officials, and, public safety is obviously a collective concern. Still, if an electronic surveillance program is legitimate, it's difficult to imagine why the government would be unable to get a court order to enforce it. Indeed, the Department of Justice's recent capitulation to FISA oversight for the NSA surveillance programs begs the question as to why they didn't get a court order in the first place.

There may be various exemptions and protections for compliance with electronic surveillance programs, but, it is unwise for any business to invite a judicial proceeding to determine whether those exemptions apply to their particular actions. All businesses, and in particular communications businesses, should have in place well-defined procedures and protocols for dealing with law enforcement surveillance requests.[222]

With respect to electronic privacy issues in general, and the cases reviewed herein that have struggled to interpret relevant law, it is difficult to create simple or comprehensive plans and procedures to govern all forms of advanced communications technology. Fundamentally, all businesses and workplaces ought to have clearly defined internal rules and procedures for handling every form of electronic communications available throughout their enterprises. These electronic communications policies need to be in writing, they need to be explained to all employees, employees need to read them, these policies need to be routinely honored and enforced, and they need to be revised whenever new laws, cases, technologies, or situations warrant their reconsideration.

---

[222] For example, surveillance statutes now also apply to cable operators who have never previously faced requests for surveillance cooperation. Gorelick et al, *supra* note 73, at 361. Cable operators must develop internal protocols and procedures to comply with such requests while still meeting their customer's needs and privacy expectations.

From an individual's perspective, citizens need to understand that almost any electronic communications device or service these days may be fair game for electronic surveillance, some lawful, some not. Given the somewhat archaic nature of our electronic privacy laws, we are largely left to do what we can to safeguard the privacy of our own electronic information. Questions remain as to whether the data we transmit over the Internet will be afforded a "reasonable expectation of privacy" under electronic privacy laws should it fall into inappropriate hands.

Finally, Congress must determine how far it wants to allow the law enforcement community to push the electronic surveillance envelope in the name of national security and public safety. The time has come for Congress to address the increscent conflict between our outdated electronic privacy laws, modern communications technology, individual privacy rights, and legitimate law enforcement needs. Without relevant changes in legislation to fit present day technology, courts will continue to render their own interpretations of federal laws, resulting in an uncertain and inconsistent legal landscape in which bad facts will increasingly dictate individual privacy rights. This confusing and uncertain legal landscape makes compliance with the law difficult if not impossible.[223] Absent legislative guidance, law enforcement officials may establish the standards for us, continuing to expand electronic surveillance activities to a degree not contemplated by the original laws or supported by the majority of the people.

---

[223] *See id*. at 367 ("A provider's subjective good-faith belief that its actions are lawful is not enough to immunize it from liability."). In addition, even when the surveillance statutes and company privacy policies clearly permit a communications provider to release information voluntarily, there may be some unwanted consequences of doing so. *Id.* "No provision in the statutes entitles companies to 'uninvite' the government after an investigation has begun." *Id.* at 372.

Produced by The Berkeley Electronic Press, 2007