# COMMUNICATIONS PRIVACY IN THE DIGITAL AGE: REVITALIZING THE FEDERAL WIRETAP LAWS TO ENHANCE PRIVACY

*James X. Dempsey**

TABLE OF CONTENTS



* Senior Staff Counsel, Center for Democracy and Technology, Washington, D.C. <www.cdt.org>. I am grateful to Jerry Berman, Joel Bernstein, Emilio Cividanes, Geoff Feiss, Wallace Henderson, Kate Martin, Lynn McNulty, Ronald Plesser, and Daniel Weitzner, who provided valuable comments on an earlier version of this article, and to Adam White Scoville, for able research assistance. For a lifetime's worth of inspiration, I am indebted to former Rep. Don Edwards, longtime chairman of the Subcommittee on Civil and Constitutional Rights of the House Judiciary Committee, for whom I had the privilege to work as assistant counsel for a decade as he endeavored to enhance the civil rights and civil liberties of all Americans.

*That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.*[1]

## I. INTRODUCTION

The ongoing worldwide revolution in communications technology is fundamentally changing the way people conduct their business and private lives. These changes are producing challenges for both privacy and law enforcement interests, stretching the limits of existing legal rules. Striking the proper balance between privacy and law enforcement in the electronic realm has always been a complex endeavor. Changes in communications technology have required periodic reexamination of privacy protections and law enforcement capabilities. It is time again for such a review.

There are broad grounds for concern that modern systems of communication are not private. Despite the convenience and the widespread popularity of cellular and other wireless telephones, they are notoriously insecure.[2] The open, networked nature of the Internet, while the source of its power as a medium, also makes it uniquely vulnerable.[3] Electronic communications systems generate vast quantities of transactional data that can be readily collected and analyzed.[4] The globalization of communications infrastructures threatens to turn the Bill of Rights into a local ordinance.

Meanwhile, law enforcement agencies, particularly at the federal level, are putting increasing emphasis on electronic surveillance.[5] The use of year-long wiretaps on multiple individuals in the "Pizza Connection" drug trafficking case, the "Ill Wind" defense procurement fraud investigation, and the "Operation

---

[1] Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[2] Adam Clymer, *Gingrich Is Heard Urging Tactics in Ethics Case*, N.Y. TIMES, Jan. 10, 1997, at A1. *See also Cellular Privacy: Is Anyone Listening? You Betcha: Oversight Hearing before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the House Comm. on Commerce*, 105th Cong. Feb. 5, 1997 [hereinafter *Cellular Privacy Hearing*].

[3] COMMITTEE TO STUDY NATIONAL CRYPTOGRAPHY POLICY, NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY (Kenneth W. Dam & Herbert S. Lin eds. 1996) [hereinafter NRC REPORT].

[4] *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195 (1992).

[5] Jim McGee, *Wiretapping Rises Sharply Under Clinton*, WASH. POST, July 7, 1996, at A1.

Polar Cap" money laundering investigation is seen as representing the future of law enforcement.[6] Louis Freeh, Director of the Federal Bureau of Investigation (FBI), has called wiretapping "one of law enforcement's most valuable investigative techniques."[7] Freeh argues that wiretapping is crucial to the investigation of cases involving terrorism, espionage, organized crime, drug trafficking, public corruption, and violent crime.[8] Without this technique, Freeh has testified, "law enforcement at the Federal, State, and local levels will be crippled."[9] Not surprisingly, therefore, a number of public policy debates in recent years have centered around law enforcement proposals to preserve or expand government surveillance capabilities in light of technological developments.

This article addresses the privacy issues raised by new communications and computer technologies and the needs of law enforcement. Section II summarizes the principles underlying the federal wiretap laws and questions whether those laws currently provide adequate protection to privacy in light of judicial interpretations and technological enhancements in surveillance capabilities. Section III addresses some of the broad implications of ongoing changes in communications technology for privacy and law enforcement and identifies five trends that should guide the development of privacy protections for the digital age. Sections IV through IX apply these themes to specific policy issues: (Section IV) the legal status of Internet communications and records stored digitally in cyberspace; (Section V) implementation of the 1994 federal legislation imposing surveillance assistance requirements

---

[6] *See* U.S. DEP'T OF JUSTICE & FBI, REPORT ON A STUDY OF THE USE OF ELECTRONIC SURVEILLANCE PREPARED BY THE UNITED STATES DEPARTMENT OF JUSTICE AND THE FEDERAL BUREAU OF INVESTIGATION, AS REQUIRED BY SECTION 810 OF THE ANTITERRORISM AND EFFECTIVE DEATH PENALTY ACT OF 1996, SUBMITTED TO THE UNITED STATES HOUSE OF REPRESENTATIVES AND THE UNITED STATES SENATE 21-22 (July 1996) [hereinafter JULY 1996 ELECTRONIC SURVEILLANCE REPORT TO CONGRESS].

[7] *Encryption, Key Recovery, and Privacy Protection in the Information Age: Hearings Before the Senate Comm. on the Judiciary*, 105th Cong. (June 4, 1997) (testimony of Louis J. Freeh).

[8] *See id.* at 9-10.

[9] *See Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 103rd Cong. 6 (1994) [hereinafter *Digital Telephony Hearings*] (testimony of Louis J. Freeh).

on telecommunications carriers;[10] (Section VI) the role of encryption; (Section VII) protection of wireless communications; (Section VIII) revisions, including those sought by the Clinton Administration, in the laws governing wiretaps, pen registers and "trap and trace" devices; and (Section IX) emerging issues concerning law enforcement cooperation and privacy protection in the international arena. Each of Sections IV through IX includes recommendations for strengthening privacy protections while preserving necessary law enforcement capabilities.

The focus of this article is limited to government access to communications and stored electronic data and attendant issues, deferring to others the consideration of important questions concerning the disposition of control over personal information as between employers and employees or between businesses and customers.[11]

## II. Electronic Surveillance and the Need for Strong Privacy Protections

*The tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques . . . Both proponents and opponents of wiretapping and electronic surveillance agree that the present state of the law in this area is extremely unsatisfactory and that the Congress should act to clarify the resulting confusion.*[12]

### A. *The Legal Framework*

In important ways, electronic surveillance has always posed greater threats to privacy than the physical searches and seizures

---

[10] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. § 1001-1010 and scattered sections of 18 U.S.C. and 47 U.S.C.) [hereinafter CALEA].

[11] *See* David N. King, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap,"* 67 S. Cal. L. Rev. 441 (1994). *See also* Sandra Petersen, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?,* 48 Fed Comm. L.J. 163 (1995); Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values?,* 72 Chi.Kent L. Rev. 271 (1996); Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace,* 1996 U. Chi. Legal F. 77 (1996); Thomas R. Greenberg, Comment, *E-Mail And Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 Am. U. L. Rev. 219 (1994).

[12] S. Rep. No. 90-1097, at 67 (1968) (Omnibus Crime Control and Safe Streets Act).

that the Fourth Amendment was originally intended to cover.[13] To begin with, "electronic surveillance is almost inherently indiscriminate."[14] Interception of a telephone line provides to law enforcement all of the target's communications, whether they are relevant to the investigation or not, raising concerns about compliance with the particularity requirement in the Fourth Amendment and posing the risk of general searches.[15] In addition, electronic surveillance involves an on-going intrusion in a protected sphere, unlike the traditional search warrant, which authorizes only one intrusion, not a series of searches or a continuous surveillance.[16] Officers must execute a traditional search warrant with dispatch, not over a prolonged period of time. If they do not find what they were looking for in a home or office, they must leave promptly and obtain a separate order if they wish to return to search again.[17] Electronic surveillance, in contrast, continues around-the-clock for days or months. Finally, the usefulness of electronic surveillance depends on lack of notice to the suspect.[18] In the execution of the traditional search warrant, an announcement of authority and purpose ("knock and notice") is considered essential so that the person whose privacy is being invaded can observe any violation in the scope or conduct of the search and immediately seek a judicial order to halt or remedy any violations.[19] In contrast, wiretapping is conducted surreptitiously.

In 1967, in the landmark *Berger* and *Katz* cases, the Supreme Court ruled that electronic surveillance was a search and seizure covered by the privacy protections of the Fourth Amendment.[20] In *Berger*, the Court condemned lengthy, continuous or indiscriminate electronic surveillances, but in *Katz*, the Court indicated that a short surveillance, narrowly focused on interception of a few

---

[13] "[T]he 'indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments,' and imposes 'a heavier responsibility on this Court in its supervision of the fairness of procedures' . . . ." Berger v. New York, 388 U.S. 41, 56 (1967) (quoting Osborn v. United States, 385 U.S. 323, 329, n. 7 (1966)).

[14] Lopez v. United States, 373 U.S. 427, 463 (1963) (Brennan, J., dissenting).

[15] *See id.*; STANDARDS RELATING TO ELEC. SURVEILLANCE, AM. BAR ASS'N PROJECT ON MINIMUM STANDARDS FOR CRIMINAL JUSTICE, 87-95 (Approved Draft, 1971).

[16] *See Berger*, 388 U.S. at 57, 59.

[17] *See id.* at 57.

[18] *See Lopez*, 373 U.S. at 463-64 (Brennan, J., dissenting).

[19] The Supreme Court has recently reaffirmed the centrality of knock and notice to the Fourth Amendment's protective scheme. *See* Richards v. Wisconsin, 117 S. Ct. 1416 (1997); Wilson v. Arkansas, 514 U.S. 927 (1995).

[20] *See Berger*, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967).

conversations, was constitutionally acceptable if approved by a judge in advance and based on a special showing of need.[21]

Responding to the Supreme Court's *Berger* and *Katz* opinions and to the arguments of law enforcement that wiretapping was a vital weapon in the efforts against organized crime,[22] Congress, in 1968, authorized law enforcement wiretapping under a system of protections intended to compensate for the uniquely intrusive aspects of electronic surveillance.[23] According to the Senate report, the legislation had "as its dual purpose (1) protecting the privacy of wire and oral communications and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized."[24] The wiretap provisions were enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, so the federal wiretap law is still referred to sometimes as "Title III."[25]

In brief, the legislation Congress enacted in 1968 had the following components: the content of wire communications could be seized by the government in criminal cases pursuant to a court order issued upon a finding of probable cause;[26] wiretapping would be otherwise outlawed;[27] wiretapping would be permitted

---

[21] *See Berger*, 388 U.S. at 59; *Katz*, 389 U.S. at 354-59.

[22] *See Controlling Crime Through More Effective Law Enforcement: Hearings on S. 300, S. 552, S. 580, S. 674, S. 675, S. 678, S. 798, S. 824, S. 916, S. 917, S. 992, S. 1007, S. 1094, S. 1194, S. 1333, and S. 2050 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary*, 90th Cong. *passim* (1967).

[23] Pub. L. No. 90-351, tit. III, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-22 (1996)).

[24] S. REP. NO. 90-1097, at 66 (1968).

[25] States may authorize wiretapping under restrictions at least as strict as the federal law, and most have done so. *See* 18 U.S.C. § 2516(2). As of December 31, 1996, forty-five jurisdictions (including the District of Columbia, Puerto Rico, and the Virgin Islands) had laws on the books authorizing wiretapping, while eight states (Alabama, Arkansas, Kentucky, Maine, Michigan, Montana, South Carolina, and Vermont) did not allow wiretapping by state and local police. *See* Statistics Div., Admin. Office of the United States Courts, 1996 WIRETAP REP. at 13 (1997) [hereinafter 1996 WIRETAP REP.]. Every year, about half of the states that do authorize wiretapping report not a single use of it by state and local law enforcement agencies, according to the annual Wiretap Reports of the Administrative Office of the United States Courts. In 1995, for example, over half of the states that authorized wiretapping (22 out of 40) did not utilize the technique (including, e.g., such large states as Illinois, Ohio, Oregon, Virginia, and Wisconsin). Statistics Div., Admin. Office of the United States Courts, 1995 WIRETAP REP. at 12 (1996).

[26] 18 U.S.C. § 2518(3) (1996).

[27] 18 U.S.C. § 2511 (1996).

only for specified crimes;[28] it would be authorized only as a last resort, when other investigative techniques would not work;[29] surveillance would be carried out in such a way as to "minimize" the interception of innocent conversations;[30] notice would be provided after the investigation had been concluded;[31] and there would be an opportunity prior to introduction of the evidence at any trial for an adversarial challenge to both the adequacy of the probable cause and the conduct of the wiretap.[32] "Minimization" was deemed essential to satisfy the Fourth Amendment's particularity requirement, compensating for the fact that law enforcement was receiving all of the target's communications, including those that were not evidence of a crime.[33] The showing of a special need, in the form of a lack of other reasonable means to obtain the information, was viewed as justification for the failure to provide advance or contemporaneous notice of the search.[34]

In 1978, Congress regulated wiretapping in national security cases through another statute, the Foreign Intelligence Surveillance Act (FISA).[35] This law authorizes the government to carry out electronic surveillance in the United States upon obtaining a judicial order (from one of a panel of Article III judges designated by the Chief Justice) based upon a probable cause finding that the target is a foreign power or an agent of a foreign power.[36] FISA was intended to be used primarily in foreign intelligence and counter-intelligence cases and therefore did not offer some of the protections required under Title III.[37] Most significantly, FISA does not require that the target ever be given notice of the surveil-

---

[28] 18 U.S.C. § 2516(2) (1996).

[29] 18 U.S.C. § 2518(3)(c) (1996).

[30] 18 U.S.C. § 2518(5) (1996).

[31] 18 U.S.C. § 2518(8)(d) (1996).

[32] 18 U.S.C. § 2518(9), (10) (1996).

[33] CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 14.5, at 14-11 to 14-12 (2d ed. 1995) [hereinafter FISHMAN & MCKENNA]; JAMES G. CARR, THE LAW OF ELECTRONIC SURVEILLANCE § 5.7(a), at 5-28 to 5-31 (1986). *See also* Clifford S. Fishman, *The "Minimization" Requirement in Electronic Surveillance: Title III, the Fourth Amendment, and the Dred Scott Decision*, 28 AM. U. L. REV. 315 (1979).

[34] S. REP. NO. 90-1097, at 66 (1968).

[35] Pub. L. No. 95-511, tit. I, § 101, 92 Stat. 1783 (1983) (codified at 50 U.S.C. § 1801-11 (1996)).

[36] 50 U.S.C. § 1805(a)(3)(a).

[37] *Foreign Intelligence Surveillance Act: Oversight Hearings before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary*, 98th Cong. 2-18 (1983) (testimony of Mary Lawton).

lance, even after the investigation is closed, unless the government seeks to use the results in a criminal prosecution.[38] In addition, for individuals who are not U.S. citizens or permanent resident aliens, the statute does not require probable cause to believe that the target is engaged in criminal conduct. Rather, it is enough that the target is an agent of a foreign power.[39] Even for U.S. citizens, the statute allows surveillance where there is probable cause to believe that the person is engaged in clandestine intelligence activities on behalf of a foreign power, "which activities involve *or may involve* a violation of the criminal statutes of the United States."[40]

A third major piece of legislation regulating electronic surveillance was enacted in 1986, when Congress made an initial response to the emergence of wireless services and the digital era with the adoption of the Electronic Communications Privacy Act (ECPA).[41] Title III had been limited to voice communications, whether face-to-face or over a wire. ECPA extended Title III to include wireless voice communications and electronic communications of a non-voice nature, such as e-mail or other computer-to-computer transmissions.[42] ECPA was intended to reestablish the balance between privacy and law enforcement, which Congress found had been upset, to the detriment of privacy, by the development of communications and computer technology and changes in the structure of the telecommunications industry. Among the developments noted by Congress were "large-scale electronic mail operations, cellular and cordless phones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of

---

[38] *Cf.* 50 U.S.C. § 1806(c).

[39] 50 U.S.C. § 1801(b)(1) (defining an "agent of a foreign power").

[40] *Id.* at § 1801(b)(2)(A) (emphasis added).

[41] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in sections of 18 U.S.C. including §§ 2510-21, 2701-10, 3121-26).

[42] ECPA, in fact, did not extend all of Title III's protections to electronic communications. The court order authorizing the interception of electronic communications can be based upon suspected violations of any federal felony, rather than the limited list of crimes that can serve as a predicate for telephone interceptions. *See* 18 U.S.C § 2516(3) (1996). In addition, no statutory exclusionary rule applies to non-voice interceptions that violate the procedures in the law. *See* 18 U.S.C. § 2515 (1996) (exclusionary rule only refers to wire or oral communications, not electronic communications).

digitized networks."[43] Privacy, Congress concluded, was in danger of being gradually eroded as technology advanced.[44]

In addition to the twin goals of privacy and law enforcement, ECPA sought to advance a third goal: supporting the development and use of these new technologies and services.[45] Congress affirmatively wanted to encourage the proliferation of new communications technologies, but it recognized that consumers would not trust new technologies if the privacy of those using them was not protected.[46]

ECPA made it a crime to knowingly intercept wireless communications and e-mail, but authorized law enforcement to do so with a warrant issued on probable cause.[47] In ECPA, Congress also began to recognize the privacy implications of transactional data generated by communications systems. ECPA established rules for the use of pen registers, which capture numbers identifying outgoing calls, and for trap and trace devices, which capture numbers identifying incoming calls.[48] In addition, it set rules for law enforcement access to information identifying a subscriber of an electronic communications service.[49] ECPA also eased certain procedural requirements for interception of wire communications by federal law enforcement officers.[50]

When law enforcement officials discuss wiretapping today, they often hasten to emphasize how stringent are the privacy protections of the legal framework established between 1968 and 1986: that wiretaps are available only for the most serious cases;[51] that authorization to conduct a tap is sought only when all other investigative techniques have failed;[52] that applications are subject to

---

[43] H.R. REP. No. 99-647, at 18 (1986).

[44] S. REP. No. 99-541, at 2-3, 5 (1986); H.R. REP. No. 99-647, at 16-19 (1986). *See also* H.R. REP. No. 99-647, at 18 (stating that "[l]egal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology.").

[45] *See* S. REP. No. 99-541, at 5 (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems").

[46] S. REP. No. 99-541, at 5 (1986); H.R. REP. No. 99-647, at 19 (1986).

[47] 18 U.S.C. § 2701-03 (1996).

[48] 18 U.S.C. § 3121-27 (1996).

[49] 18 U.S.C. § 2703(c).

[50] Pub. L. No. 99-508, § 106, 100 Stat. 1848, 1856-57 (1986) (amending 18 U.S.C. § 2518).

[51] *See Digital Telephony Hearings, supra* note 9, at 6, 8, 16-20 (testimony of Louis J. Freeh).

[52] *See id.* at 6, 8, 16, 22, 123.

rigorous judicial scrutiny;[53] that wiretaps are conducted in such a manner as to minimize the interception of innocent conversations;[54] and that parties whose conversations are intercepted are entitled to obtain after-the-fact judicial review of the authorization and conduct of wiretaps.[55] Law enforcement officials cite these protections as a way of reassuring legislators and the public that the intrusiveness of electronic surveillance is well regulated.

### *B. Erosion of the Wiretap Laws' Protective Scheme*

There is substantial evidence, however, technological developments aside, that the protections initially established in 1968 and reaffirmed in 1986 are not working as intended. It appears increasingly apparent that components of the balanced legislative scheme have been watered down by Congress itself and by the judiciary:

(1) Wiretapping is no longer confined to violent and major crimes. Although Congress recognized in 1968 that wiretapping was an extraordinary technique that should be used only for especially serious crimes, the list of offenses for which wiretapping is permitted has been expanded steadily ever since — from the original 26 in 1968 to 95 in 1996.[56] The original list was largely limited to espionage and treason, violent crimes, and offenses typically associated with organized crime. The current list has been so expanded that wiretapping is now authorized for cases involving false statements on passport applications and loan applications or involving "any depredation" against any property of the United States.[57] Further expansions are promoted in response to each new law enforcement concern that receives legislative attention. Wiretapping is used only rarely in cases involving homicide, kidnapping, or terrorism. In 1996, 71% of wiretaps nationwide were in drug cases.[58]

(2) The yearly number of federal, state and local law enforcement wiretaps has gone up steadily, from 564 in 1980 to 1,149 in 1996. Wiretaps increased 9% in 1996 alone.[59] Judges rarely deny wiretap applications. In 1996, only one wiretap application was

---

[53] *See id.* at 16, 22.
[54] *See id.* at 22, 24.
[55] *See id.* at 16.
[56] 18 U.S.C. § 2516 (1996).
[57] *Id.*
[58] 1996 WIRETAP REP., *supra* note 25, at 8.
[59] *Id.* at 7.

denied; 1,149 were approved.[60] For seven years in a row, 1989 through 1995, no judge, state or federal, denied a single government request for wiretapping.[61] In that period, judges approved 6,598 wiretap orders in criminal cases.[62] There has been equally dramatic growth in the use of pen registers and trap and trace devices. In 1995, the law enforcement agencies of the federal Justice Department alone executed 3,414 pen register orders covering the telephone facilities of 7,899 persons and 1,558 trap and trace orders affecting the telephones of 3,902 persons.[63] No judge has ever been known to deny an application for a pen register or trap and trace device, because the law states that a judge *must* approve any application signed by an Assistant United States Attorney (or higher-ranking government attorney) who certifies that the information likely to be obtained is relevant to an ongoing criminal investigation.[64]

(3) While *Katz* indicated approval of wiretaps of short duration, the longest wiretap in 1996 lasted 420 days.[65] The average length of intercepts has increased steadily, from an average of 21 days in 1980, to an average of 38 days in 1996.[66] The average number of calls intercepted per wiretap has also increased steadily, from 1,058 per intercept in 1980 to 1,969 in 1996.[67]

(4) The courts authorize electronic surveillance even when law enforcement agencies have not exhausted all other reasonably available techniques.[68] In *United States v. Garcia*,[69] for example, the Eighth Circuit held that electronic surveillance approval does

---

[60] *Id.*

[61] *Id.* at 29.

[62] *Id.*

[63] Report on the Use of Pen Registers and Trap and Trace Devices by the Law Enforcement Agencies/Offices of the Department of Justice for Calendar Year 1995, Report submitted to the House and Senate Judiciary Committees, April 30, 1996 [hereinafter PEN REGISTER REPORT].

[64] 18 U.S.C. § 3123(a) (1996).

[65] 1996 WIRETAP REP., *supra* note 25, at 8.

[66] *See* Statistics Div., Admin. Office of the United States Courts, 1990 WIRETAP REP. at 29 (1991); 1996 WIRETAP REP., *supra* note 25, at 29.

[67] *Id.*

[68] FISHMAN & MCKENNA, *supra* note 33, § 8:47 at 8-96 to 8-97 & nn. 36-37 (citing United States v. Giordano, 416 U.S. 505, 515 (1974); United States v. Pacheco, 489 F.2d 554, 564-65 (5th Cir. 1974); People v. Milnes, 527 P.2d 1163, 1167 (Colo. 1974); Bell v. State, 429 A.2d 300, 302-04 (Md. Ct. Spec. App. 1981); Commonwealth v. Fenderson, 571 N.E.2d 11 (Mass. 1991); State v. Monsrud, 337 N.W.2d 652, 657 (Minn. 1983); State v. Lozano, 311 N.W.2d 529, 531 (Neb. 1981); People v. Versace, 426 N.Y.S.2d 61 (2d Dep't 1980); State v. Ahmadjian, 438 A.2d 1070, 1083 (R.I. 1981)).

[69] 785 F.2d 214, 223 (8th Cir. 1986).

not require the exhaustion of all normal investigative techniques.[70] Representative of the judicial attitude is the conclusion of one court that the purpose of the statutory exhaustion requirement is "simply to inform the issuing judge of the difficulties involved in the use of conventional techniques."[71]

(5) The minimization requirement also has not been strictly enforced by the judiciary.[72] In *Scott v. United States*,[73] the Supreme Court held that the complete recording of all conversations on a phone line belonging to the woman with whom the subject of the order was living was acceptable. Law enforcement agents in that case had made essentially no efforts to minimize the interception of nonpertinent calls, despite the high proportion of calls on the line that were nonpertinent. The Court justified this pattern of recording on the ground that the subject often used coded language in very brief conversations. In *Scott*, 40% of the conversations intercepted were relevant, but the lower courts have read the case as effectively eliminating the requirement to minimize the recording of innocent conversations. *Scott*'s impact is illustrated by *United States v. Ozar*,[74] where the Eighth Circuit upheld the "two minutes up/one minute down" technique recommended by the Justice Department, in which FBI agents listened to two out of every three minutes of every phone conversation. In *Ozar*, the government intercepted a total of 8,126 minutes of the defendant's telephone conversations, of which 223 minutes, or 2.75% were deemed pertinent to the ensuing charges. The Court of Appeals held that this was not a violation of Title III, not because the conversations were short and coded, as in *Scott*, but because they were lengthy and complicated.[75]

(6) Defendants' after-the-fact challenges to the authorization or conduct of surveillance are rarely sustained.[76] Between 1985 and 1994, judges nationwide granted 138 suppression motions while denying 3,060, for a 4.3% suppression rate.[77]

---

[70] *Id.* at 223.

[71] *See* United States v. Pacheco, 489 F.2d 554, 564-65 (5th Cir. 1974).

[72] FISHMAN & MCKENNA, *supra* note 33, § 14-4 at 14-8 to 14-11; Robert Plotkin, *Breaking the Code: Excluding Illegal Wiretap Evidence*, 10 BNA CRIMINAL PRACTICE MANUAL 432 (1996).

[73] 436 U.S. 128 (1978).

[74] Ozar v. United States, 50 F.3d 1440, 1448 (8th Cir. 1995), *cert. denied*, 116 S.Ct. 193 (1995).

[75] *Id.* at 1447-48.

[76] Plotkin, *supra* note 72, at 432.

[77] Compiled from Wiretap Reports covering the years from 1985 through 1994.

(7) The FISA court in its entire seventeen-year history has never turned down a government electronic surveillance request.[78] Little is known publicly about these taps, but the Justice Department has released figures showing that in 1996, the FISA court issued a record 839 orders, up 20% from the prior year.[79] Meanwhile, FISA has been used increasingly in criminal cases,[80] for which it was not designed. The government does this by claiming that it is conducting parallel intelligence and criminal investigations and proceeds under the more flexible FISA standards. In another very troubling development, Congress recently authorized the use of FISA evidence in secret deportation proceedings, allowing the evidence to be introduced without disclosure to the respondent, thereby dispensing with one of the statute's key procedural protections.[81]

### *C. Enhancements in Government Surveillance*

> *In the long term, digital telephone technology will enhance the FBI's ability to collect, share and analyze information. Many of these enhancements will come without any FBI development effort, driven by consumer demand.* [82]

In many ways, it is clear that this 1991 prediction by the FBI is coming true. While Section IV examines Congress' response to FBI concerns that new technology is making electronic surveillance harder, there are other ways in which new communications and computer technologies provide substantial advantages to law enforcement.

*Wireless Services.* In a host of circumstances where, in the past, persons would have used pay phones or not made a call at all, they now use cellular or other wireless phones, which are readily tapped at central switches. (It is normally far easier to identify a target's wireless service provider than it was to predict which pay phone he or she would use.) Proportionately more wireless phones

---

[78] Jim McGee & Brian Duffy, *Someone to Watch Over Us*, WASH. POST MAG., June 23, 1996, at 9, 12.

[79] 67 FEDERATION OF AM. SCIENTISTS, SECRECY AND GOVERNMENT BULLETIN (May 1997)(citing April 18, 1997 U.S. Dep't of Justice report to Congress).

[80] McGee & Duffy, *supra* note 78, at 9, 13.

[81] Anti-Terrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 401, 110 Stat. 1214, 1262 (codified at 8 U.S.C. § 1534(e)).

[82] FBI Budget Justification for FY 1992, at 67, *reprinted in Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations for 1992: Hearings Before a Subcomm. of the House Committee on Appropriations*, 102nd Cong. 738 (1991).

are tapped by law enforcement than traditional wireline phones.[83] Indeed, law enforcement has been so quick to utilize this capability that in some urban areas cellular companies had been unable to accommodate simultaneously all of the law enforcement agencies seeking to tap cellular phones from mobile telephone switching offices, and therefore had to install additional capacity.

*Location information.* In the course of processing calls, many wireless communications systems collect information about the cell site (or the sector within a cell site) of the person making or receiving a call. Systems may even locate a cellular phone merely while it is turned on, even if it is not handling a call.[84] The technology is proceeding in the direction of providing more precise location information, a trend that has been boosted by the rulings of the Federal Communications Commission in its "E-911" (enhanced 911) proceeding, which requires service providers to develop a locator capability for medical emergency and rescue purposes.[85] Wireless phone location information can be obtained by law enforcement. If it is a record collected and stored as part of the billing process, it can be obtained under current law by a mere subpoena. To obtain it in real-time, law enforcement agencies have been using court orders issued under 18 U.S.C. § 2703 (d). In 1994, three of the four manufacturers of cellular switches had developed the software capability to deliver location information to law enforcement immediately upon call completion.[86]

---

[83] *Digital Telephony Hearings, supra* note 9, at 152 (testimony of Thomas E. Wheeler).

[84] Tim Friend, *Using Cell Phones to Reach Out and Find Someone*, USA TODAY, Dec. 16, 1997, at 6D; Albert Gidari, *Locating Criminals by the Book*, CELLULAR BUS., June 1996, at 70.

[85] In June 1996, the FCC adopted a Report and Order and Notice of Proposed Rulemaking in Docket 94-102, requiring wireless service providers to modify their systems within eighteen months to enable them to relay to public safety authorities the cell site location of 911 callers. Further, the FCC ordered carriers to take steps over the next five years to deploy the capability to provide latitude and longitude information locating wireless telephone callers within 125 meters. Finally, the FCC proposed requiring at the end of the five year period that covered carriers have the capability to locate a caller within a forty foot radius for longitude, latitude and altitude, thereby, for example, locating the caller within a tall building. *In re* Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys., FCC Docket No. 94-102, Report and Order and Further Notice of Proposed Rulemaking (last modified Jan. 2, 1997) [hereinafter FCC E-911 Order] *available at* <http://www.fcc.gov/Bureaus/Wireless/Orders/1996/fcc96264.txt>.

[86] *Digital Telephony Hearings, supra* note 9, at 152-54 (testimony of Thomas E. Wheeler).

*E-mail and other on-line communications.* E-mail is in some respects easier to intercept than regular mail. Indeed, since e-mail messages are often stored with a service provider for a period of time before they are read by the intended recipient (and even sometimes after they are read), e-mail is less transient than telephone calls and thus more vulnerable to interception. Law enforcement can intercept a person's e-mail and other Internet activity in real-time, by monitoring the phone line that serves as most people's connection to the Net.[87] This allows law enforcement, when it chooses to do so, to obtain an extraordinary window into a person's life. More readily, e-mail messages can be obtained from the host computer of the service provider. This is the method most commonly used by law enforcement to access e-mail.[88] In this way, e-mail interception is easier than telephone interception: while a person might have one telephone number at home, a different number at work, and another when traveling on business or vacation, most people have only one e-mail address to which all their e-mail is sent, and where it is all subject to being accessed by the government.[89]

*Remote monitoring.* Technology has freed law enforcement intercepts of the constraints of geography. Agents monitoring wiretaps do not have to sit hunched in vans outside the target's house. Instead, the intercepted communications can be transported hundreds or thousands of miles to a monitoring facility at a law enforcement office. It is now common in investigations spanning multiple jurisdictions to establish a single monitoring plant and transmit there in real-time all intercepted conversations to be monitored, minimized, and recorded. The courts have held that a single federal judge can issue wiretap orders for telephones any-

---

[87] *See* Michael J. Sniffen, *First Computer Wiretap Produces Hacking Charge Against Argentine Student*, ASSOCIATED PRESS, Mar. 29, 1996 (where communications through a major Harvard University computer were sifted in a search for patterns used by a suspected hacker); Gaylord Shaw, *Wiretap Nets a Hacker: In a cyber-monitoring first, U.S. accuses Argentinian*, NEWSDAY, Mar. 30, 1996, at A6.

[88] *See, e.g.*, United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996) (search warrant for e-mail served on America Online); United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996).

[89] By lurking in online "chat rooms," law enforcement officers are able to monitor communications. *See* Graeme Zielinski, *Tracking Pedophiles on Vast Internet No Easy Task,* CHICAGO TRIBUNE, July 6, 1997, at C1 ("In a sense, the Internet has proven a boon to investigators, said an FBI investigator. 'These guys used to be in some back shed somewhere. We couldn't get to them. . . .Now we can get inside their minds.'").

where in the country, so long as the personnel listening to the conversations work in the judge's jurisdiction.[90] The Drug Enforcement Agency forwards intercepts from many different investigations to a central facility in Utah, where they are transcribed and translated by military personnel.[91]

*Computer analysis.* As noted above, law enforcement has recognized the informational richness of signaling and transactional information. Computer analysis is key to law enforcement exploitation of this data. Computers have made it possible for law enforcement agencies to analyze vast amounts of information about personal communications patterns far more easily. Pen registers, which recorded the numbers dialed on a particular phone line, have been superseded by multiline dialed number recorders, and these, in turn, have been computerized, allowing agencies to automatically search for revealing patterns of calls. The DEA has developed an integrated system called TOLLS that will electronically load telephone call data from dialed number recorders into a mainframe system for matching and analysis.[92] Further computer analytic developments may be around the corner. Voice recognition technology, for example, would free law enforcement from the most labor intensive aspects of monitoring conversations, removing one of the biggest practical constraints on the number of interceptions made.

Title III allows law enforcement to take full advantage of these enhancements, requiring telephone companies, service providers and all other communications carriers to provide all technical assistance to law enforcement agencies seeking to carry out authorized interceptions.[93]

## III. Five Broad Technological Trends Affect Privacy and Law Enforcement, Posing Challenges and Offering Opportunities

*Telecommunications, of course, did not stand still after 1986. Indeed, the pace of change in technology and in the structure of the*

---

[90] United States v. Rodriguez, 968 F.2d 130, 135 (2d Cir. 1992).

[91] Jim McGee, *Military Seeks Balance in Delicate Mission: The Drug War; As Involvement Expands, Law and History are Basic Guidelines*, Wash. Post, Nov. 29, 1996, at A1.

[92] David Burnham, Above the Law 159 (1996) (citing U.S. Dep't of Justice, 1994 Congressional Authorization and Budget Submission, vol. 2, DEA section, at 47).

[93] *See* 18 U.S.C. § 2518(4) (1996).

*telecommunications industry accelerated and continues to accelerate.*[94]

Behind the individual enhancements to surveillance capabilities identified above are five broad technological developments[95] that profoundly challenge the assumptions made by Congress in 1968 when it first established the rules for electronic surveillance, and in 1986 when it reaffirmed those assumptions:

(1) The dramatic development of the Internet has transformed all over again methods of gathering, processing and sharing of information, which had already been transformed by the computer itself. In 1981, fewer than 300 computers were linked to the Internet.[96] In 1986, when ECPA was enacted, there were about 50,000.[97] By June 1996, there were over 9.4 million host computers worldwide linked to the Internet. Including users who connect to the Internet via modem, some 40 million people worldwide can access the Internet.[98] In commercial terms, networking has had enormous implications. The average number of electronic point-of-sale transactions in the United States went from 38 per day in 1985 to 1.2 million per day in 1993.[99] Estimates for the potential of "Internet commerce" range up to "tens of billions of dollars by the turn of the century."[100]

The Internet is not like the telephone system, or the mail, or mass media. Rather, the Internet combines a much broader range of functions, serving not only the one-on-one functions of the telephone and the mail, but also the information functions of TV, newspapers and the library; the artistic functions of a movie theater and a museum; the political functions of a town meeting hall;[101] the marketing and shopping functions of a mall; the

---

[94] H.R. REP. NO. 103-827, pt.1, at 12 (1994) (report on CALEA).

[95] A list such as the one that follows cannot be comprehensive of the changes underway in the digital world. Others, for example, would point to the developing "convergence" among voice, data, and images as another major trend in telecommunications. However, the trends discussed here were identified because they seem to have major implications for government surveillance and privacy.

[96] Reno v. ACLU, 929 F. Supp. 824, 831 (E.D. Pa. 1996).

[97] *Id.*

[98] *Id.*

[99] OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS, 1-2 (1994).

[100] The White House, A Framework for Global Electronic Commerce, July 1, 1997, at 2 (the "Magaziner report").

[101] U.S. Senate hearings have been broadcast live over the Internet. *See e.g.*, <http://www.crypto.com/events/072596/>; <http://www.crypto.com/events/062696/>; <http://www.hotwired.com/wiredside/96/25/stuff/senate.28.8.ram>.

organizing functions of door-to-door canvassing;[102] and the social, even romantic functions of a nightclub or coffee house. As an intentionally open system of linked computers, the Internet is inherently insecure.[103] The dramatic development of the Internet as a networked global communications medium and the expansion in the range of transactions that occur on-line have produced a qualitative change in the nature of communications and, accordingly, in the nature and amount of the information that is exposed to both lawful interception and illegal intrusion or misuse.

(2) Signaling information has become an increasingly rich source of information about habits of association and commerce. Congress in 1968[104] and again in 1986[105] assumed that there were two categories of data: content (which would receive the highest protection) and a category of minimally revealing dialing or routing information. However, in recent years, transactional data has evolved into a third, hybrid type, providing detailed information about a person's habits of association and commerce.[106] Yet this "profiling" data was totally unprotected until 1986 and has since been subject only to the most minimal protection. (Congress again tightened the standard for access to certain e-mail addressing information in 1994, as discussed below in Section IV.) On the Internet, this data gives a rich picture of a person's life.[107] In a similar development in the area of voice communications, advanced signaling systems have also blurred the distinction

---

[102] Grassroots groups across the political spectrum use the Internet to inform, organize and galvanize. The "Encryption Policy Resource Page" features an "Adopt Your Legislator" campaign, connecting Internet users with information about their legislators' positions on the encryption issue. The page operates in conjunction with e-mail alerts to interested citizens so that they can contact their representatives when legislative action is imminent. *The Encryption Policy Resource Page: Adopt Your Legislator!* (visited July 26, 1997) <http://www.crypto.com/adopt>.

[103] NRC REPORT, *supra* note 3, at 300.

[104] *See* Omnibus Crime Control and Safe Streets Act of 1968, tit. III, Pub. L. No. 90-351, § 802, 82 Stat. 212 (codified at 18 U.S.C. § 2510-20).

[105] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in sections of 18 U.S.C. including §§ 2510-21, 2701-10, 3121-26).

[106] *Digital Telephony Hearings, supra* note 9, at 158, 160-61, 166-78 (testimony of Jerry Berman, including *Expanded Protection for Online Transactional Information*, memorandum of the Electronic Frontier Foundation).

[107] *See, e.g.*, Alan Boyle, *Eyes Are On You When You're Online* (last modified Sept. 10, 1997) <http://www.msnbc.com/news/34363.asp>; Jeffrey Rothfeder, *No Privacy on the Net*, PC WORLD, Feb. 1997, at 223; John M. Broder, *Making America Safe for Electronic Commerce*, N.Y. TIMES, June 22, 1997.

between call-identifying information and call content. There is some concern that the development of packet switching may obliterate the distinction between signaling data and communications content.[108] In some cellular and other wireless telephone systems, this signaling data includes location information, potentially turning wireless phones into tracking devices.[109] Law enforcement is increasingly turning to transactional or signaling data as a source of investigative importance.[110]

(3) The rapid expansion of wireless services, which are increasingly used not just by the wealthy and in business applications, but by ordinary citizens for personal conversations, has made electronic communication almost totally flexible and constantly available, yet also more insecure. The number of wireless customers has gone from 92,000 in 1984 to 44 million by the end of 1996.[111] Moreover, wireless transmission is no longer important only for voice communication, but is becoming increasingly important for data transfer. Wireless modems and wireless local area networks are linking computers and transferring data that could include proprietary information, medical records, and financial data.[112] Wireless links are increasingly serving as gateways to the global information infrastructure. While offering attractive advantages of flexibility, wireless communications are less secure than traditional landline communications.[113]

(4) Control over technology has shifted away from the hands of government and a few monopolies. Telephony itself is now characterized by competition and rapid innovation, producing an environment with many new products, services and features, and many new service providers. State-of-the-art encryption technology is no longer subject to government monopoly. Users can now affirmatively choose encryption technology that will enhance their

---

[108] *See* U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, ELECTRONIC SURVEILLANCE IN A DIGITAL AGE, at 57-61 (July 1995) [hereinafter OTA ELECTRONIC SURVEILLANCE REPORT].

[109] *Digital Telephony Hearings, supra* note 9, at 33 (testimony of Louis J. Freeh), 154 (testimony of Thomas E. Wheeler), 158 (testimony of Jerry Berman); H.R. REP. NO. 103-827, pt. 1, at 17 (1994).

[110] *See* PEN REGISTER REPORT, *supra* note 63.

[111] *United States Wireless Demographics* (visited July 25, 1997) <http://www.wow-com.com/professional/reference/CusDemog.cfm> (citing Cellular Telecommunications Industry Association, Year-End 1996 Data Survey).

[112] *See* Maryam Alavi, *Dick Tracy's Office : Business Applications of Wireless Technologies, in* THE EMERGING WORLD OF WIRELESS COMMUNICATIONS (INSTITUTE FOR INFO. STUDIES ed., 1996). *See generally,* Boyle, *supra* note 107.

[113] *See Cellular Privacy Hearing, supra* note 2.

privacy and protect the security of their data against criminals. The Internet was designed from the outset as a decentralized medium for rapid transmission of information, and has evolved to a state of unprecedented openness. Barriers to participation are low; anyone with a computer and a modem can be a publisher. Services and even entirely new infrastructures are developing rapidly in response to user demands.[114] Government efforts to control the development and spread of technology become harder to sustain.

(5) The globalization of communications technology and networks is breaking down national borders. One of the great strengths of the Internet is that it can be as easy to send an e-mail message to New York as to Nairobi. The information infrastructure is now global, as are the markets for telecommunications products and services. On the one hand, the irrelevance of borders means that government controls over information and technology become harder to maintain. On the other hand, enforceable privacy protections have not yet emerged for the global information infrastructure.

The remainder of this article examines how these trends have affected the balance between privacy and law enforcement and how that balance can be re-established.

## IV. Protecting "Papers" in Cyberspace — The Internet and the Fourth Amendment

ECPA was intended to establish rules for government surveillance in the digital world. In many respects, it has proven to be a durable statute. However, technology has evolved in ways not contemplated when ECPA was enacted. In drafting ECPA, Congress assumed that it would be adequate to extend to electronic communications the constitutional conclusion that underpinned Title III in 1968: that capture of electronic communications would not be an unreasonable intrusion if there were stringent ex parte judicial review before the fact, minimization during a search, and equally stringent adversarial review after the investigation had been completed.[115] That assumption, however, was made when few if any foresaw the development of the multiple forms of activity that are carried on today in "cyberspace." The interactive

---

[114] For example, certificate authorities are developing to verify identity in the digital world. *See generally* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 Or. L. Rev. 49 (1996).

[115] *See* S. Rep. No. 99-541, at 2-3, 5 (1986).

nature of the Internet, with the rapid emergence of features such as home banking, telecommuting and even telemedicine, has produced an environment in which many people spend hours each day "on-line."[116] In this context, to intercept all of a person's electronic communications means a lot more today than it did in 1968 or 1986. These developments call for an examination of the effectiveness and coverage of ECPA.

A first step toward examining ECPA would be to assess how the rules it set for governmental access to e-mail and other computer communications are working. Unfortunately, however, there is no publicly available data on which to base such an assessment. While the wiretap provisions of Title III require very detailed reports on interception of voice communications and interception of e-mail in transit, there is no similar requirement for collecting and publishing information on the extent of government access to e-mail and other electronic communications while they are in storage with service providers incident to transmission, by far the easier and presumably the more common means of government's accessing electronic communications.[117] This deficiency should be corrected by amending ECPA to require that courts and prosecutors submit reports on orders sought and granted for electronic communication access under 18 U.S.C. § 2703, for inclusion in the Administrative Office reports on wiretapping. Until such a change can be enacted, Congressional committees should exercise their oversight authority to obtain such data from the federal agencies and the major service providers.

Another issue that needs to be re-addressed is whether one of the key protections established in 1968, the minimization rule, can be applied to non-voice communications. Minimization means that law enforcement is not supposed to record non-relevant communications. At the time ECPA was enacted, it was assumed that this was impossible in the e-mail context: law enforcement must get all the communications to and from a target, and read each one to determine if it is relevant.[118] In 1986, in fact, the Senate Judiciary Committee expressly addressed this concern and suggested that minimization should be conducted by the initial law

---

[116] *See generally*, PAUL GILSTER, DIGITAL LITERACY (1997); SHERRY TURKLE, LIFE ON THE SCREEN (1995); HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY (1993).

[117] *Cf.* 18 U.S.C. § 2701 *et seq.*

[118] Larry Downes, *Electronic Communications and the Plain View Exception: More "Bad Physics,"* 7 HARV. J.L. & TECH. 241, 263-67 (1996).

enforcement officers who review the intercepted communications. The committee stated that "[T]hose officials would delete all non-relevant material and disseminate to other officials only the information which is relevant to the investigation."[119] This solution has been criticized as unrealistic.[120] Actually, it is not that different from what happens in the case of ordinary telephone wiretaps, since the initial law enforcement personnel who monitor voice intercepts conduct an initial review of each conversation to decide whether to record it or not.

Technology, however, may offer a solution, producing more effective minimization than is available in the context of voice communications. Whether law enforcement accesses e-mail from the telephone company (or access provider) while in transmission, or from an e-mail service provider while it is in storage incident to transmission, it may be relatively easy for the service provider to perform the minimization. The service provider can use screens or filters to select from the e-mail messages to or from parties identified in the order only those containing certain key words or phrases that would be identical to those used by monitors in the voice context.[121] As the investigation proceeds and law enforcement learns more about the patterns of the target, the interception can become more discriminating.

Another set of assumptions are being challenged by the profound changes occurring as a result of the Internet. These concern the degree of protection from governmental access one can justifiedly expect with respect to transactional records held by third parties. In 1976, the Supreme Court in *United States v. Miller* ruled that individuals had no constitutionally protected privacy interest in business records that were held by a third party.[122] *Miller* involved checks held by a bank, and the rationale of the case assumed a world of paper records, yet the holding in its broadest implications has been applied unquestioningly to the electronic world. Thus, in 1979, the Court in *Smith v. Maryland* ruled that the use of a pen register to collect the phone numbers dialed on a surveillanced line did not implicate Fourth Amendment interests.[123]

---

[119] S. REP. No. 99-541, at 31 (1986).

[120] Downes, *supra* note 118, at 267.

[121] Law enforcement already took this approach in one case involving interception of computer communications. *See* Sniffen, *supra* note 87.

[122] *See* 425 U.S. 435 (1976).

[123] *See* 442 U.S. 735 (1979).

ECPA responded to *Smith* by requiring a judicial order for pen registers and trap and trace devices.[124] For transactional information relating to e-mail and other electronic communications, ECPA required a subpoena, a warrant or a court order.[125] In 1994, Congress recognized that transactional data associated with e-mail and other computer communications was emerging as a hybrid form of data, somewhere between addressing information and content, and was becoming increasingly revealing of personal patterns of association. Therefore, Congress set a higher standard for access to transactional data regarding electronic communications and eliminated subpoena access.[126] Congress should examine the Justice Department's interpretation and application of the new standard to see if it is adequate or should be strengthened. Such an examination must give adequate attention to the communicative, associational nature of the transactional data itself in an online environment. (Congress should also strengthen the procedure for access to transactional records in the ordinary telephone context, a point discussed below in Section VIII.)

Finally, reexamination of ECPA must question the assumption that there is a distinction between the communication of content and its storage. In an era when people work for "virtual companies" and conduct personal, political and business lives in "cyberspace," that distinction is increasingly blurred. The growth of online commerce, politics and relationships, the shift to distributed, networked computing, the growth of the World Wide Web as an information source, and the ready ability to encrypt records stored with third parties, call into question the application to the Internet of concepts developed for governmental access to business records in a relatively static, paper-based environment and may radically change the legal notion of what is a reasonable expectation of privacy.

It is time to reconsider how the lines have been drawn between records entitled to full Fourth Amendment protection and records under *Miller* that fall outside the protection of the Fourth Amendment. There are now essentially three legal regimes for access to electronic data: (i) the traditional Fourth Amendment standard, for records stored on an individual's hard drive or floppy disks; (ii) the Title III-ECPA standard, for records in transmission; and (iii) a third standard, the scope of which is probably unclear, for

---

[124] 18 U.S.C. § 3121 (1996).
[125] Pub. L. No. 99-508, § 201, 100 Stat. 1862 (adding 18 U.S.C. § 2703(c)).
[126] *See* 18 U.S.C. § 2703(c) (1996).

records stored on a remote server, such as the research paper (or the diary) of a student stored on a university server or the records (including the personal correspondence) of an employee stored on the server of the employer.[127] As the third category of records expands because people find it more convenient to store records remotely, the legal ambiguity grows more significant. Are the records stored on such a server accessible by mere subpoena? Are they covered by the "remote computing" provisions of ECPA?[128] If the records were seized from the individual's hard drive or floppies using a warrant or subpoena, contemporaneous notice would be required.[129] If the records were seized in transmission, a court order would be required, but the interception could proceed secretly.[130] If the records were seized from a third party, notice might be delayed.[131] Do these distinctions make sense? Is the delay or denial of notice for stored records acceptable any longer? Conceptions of the Fourth Amendment developed in a 20th century world of paper records may not be applicable to 21st century technologies where many of our most important records are not "papers" in our "houses," but are "bytes" stored electronically and accessed remotely at "virtual" locations.

## V. Preserving Government Surveillance Capabilities While Protecting Privacy and Encouraging Technological Innovation

While some technological developments have made electronic surveillance easier, more intrusive or more revealing, the FBI in the early 1990's began to complain about the ways in which technological developments were making law enforcement interception more difficult.[132] These difficulties were often encompassed by the term "digital telephony," although digital transmission itself was not really the problem. In fact, there were a number of problems. Some of the difficulties related to the rapid growth of wireless systems, which are easily tapped at the central switches but did not always have the capacity to accommodate multiple

---

[127] *See* 18 U.S.C. §§ 2701-2703 (1996).

[128] *See* 18 U.S.C. § 2703.

[129] Standard Fourth Amendment practice requires notice, achieved by service of the warrant or subpoena on the person possessing the items to be seized or produced. Wayne R. La Fave, Search And Seizure, § 4.1-4.13 (3d ed. 1996).

[130] *See* 18 U.S.C. § 2511(2)(a)(ii) (1996).

[131] *See* 18 U.S.C. § 2703(b).

[132] *See Digital Telephony Hearings*, *supra* note 9, at 5-6 (testimony of Louis J. Freeh).

surveillances. Others were related to the increased competition in the telecommunications industry, which meant that a target could use two or more service providers, making one-stop surveillance impossible. Some problems arose due to services and features that put more control in the hands of users. During the 1994 hearings, the FBI voiced concerns about a number of these problems, some of which existed in analog systems, but which had become more common in digital switches. Among them were problems intercepting calls rerouted through call forwarding services and the inability to identify the destination of calls made using a speed dialing feature.[133] Some problems had to do with physical changes in the networks. For example, the FBI anticipated increasing trouble in covertly isolating the communication stream associated with a particular target as multiplexed transmission technologies and fiber cables replaced the paired copper wires that traditionally had been associated uniquely with each customer.[134]

Congress responded to these technological developments by enacting the Communications Assistance for Law Enforcement Act of 1994 (CALEA, sometimes referred to as the "digital telephony" legislation).[135] CALEA requires telephone companies to ensure that new technologies (and some old technologies) do not impede law enforcement interception of communications.[136] The legislation mandates, in effect, that carriers must take steps to ensure that the broad technological trends in the industry do not eliminate law enforcement access to communications of targeted individuals.

In adopting CALEA, Congress explicitly stated its intention to preserve the balance among the three interests that had guided the drafters of ECPA in 1986: law enforcement needs, privacy, and technological innovation.[137] Congress accepted the FBI's assurances that the legislation would preserve the status quo in terms of law enforcement surveillance, without expanding govern-

---

[133] *See id.* at 121 (information submitted by Louis J. Freeh, "Technology-Based Problems Encountered by Federal, State, and Local Law Enforcement Agencies").

[134] *See id.* at 24 (testimony of Louis J. Freeh).

[135] Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001-1010 and scattered sections of 18 U.S.C. and 47 U.S.C. (1994)).

[136] *See id.* at §§ 103, 104.

[137] H.R. REP. No. 103-827, pt. 1, at 22 (1994).

ment capabilities.[138] Congress stressed specifically that the surveillance requirements of CALEA should be narrowly interpreted.[139] Congress also required carriers to change their systems to protect the privacy and security of communications not authorized to be intercepted.[140] To ensure that implementation did not block technological innovation, Congress prohibited the FBI from dictating network or equipment design standards.[141] Finally, Congress also amended some provisions of ECPA to heighten privacy protections.[142]

However, since CALEA was enacted, a struggle has been underway in which the FBI, on behalf of law enforcement generally, has attempted to broadly interpret the requirements of CALEA, by dictating system design and mandating, nationwide, certain capabilities in excess of traditional interception practices.[143] The most

---

[138] When FBI Director Louis Freeh appeared before a joint hearing of the House and Senate Judiciary subcommittees in August 1994 to support the final version of CALEA, he stressed that the legislation would preserve wiretapping as it had existed since 1968:

> Without question. . . court-authorized electronic surveillance is a critical law enforcement and public safety tool. I think we have reached a remarkable compromise and achievement in preserving that tool as it has existed since 1968 . . . .We believe that the legislation, as introduced this past Tuesday, offers the strongest investigative assurances that the authority which Congress gave us in 1968 will continue unimpeded by technology. . .

*Digital Telephony Hearings, supra* note 9, at 112-13. These assurances followed a series of statements of Director Freeh to the same effect at the March 18, 1994 hearing of the same subcommittees. *Id.* at 7, 9, 10, 16, 29-30, 14, 49.

[139] Congress stated as follows:

> The Committee intends the assistance requirements in section 2602 to be both a floor and a ceiling. The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past. The Committee urges against overbroad interpretation of the requirements. The legislation gives industry, in consultation with law enforcement and subject to review by the FCC, a key role in developing the technical requirements and standards that will allow implementation of the requirements. The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements.

H.R. REP. No. 103-827 at 22-23.

[140] *See* H.R. REP. No. 103-827, pt. 1, at 17; CALEA, § 103(a)(4)(a) (codified at 47 U.S.C. § 1002(a)(4)(a)).

[141] *See* CALEA, § 103(b)(1) (codified at 47 U.S.C. § 1002(b)(1)).

[142] *See* Pub. L. No. 103-414, §§ 202-207.

[143] John Markoff, *Telephone Industry Seeks Aid in Wiretap Battle with F.B.I.*, N.Y. TIMES, July 16, 1997, at A13; Jim McGee, *FBI Calls for Greater Wiretap Capability, Phone Industry Pressed to Install New Surveillance Equipment*, WASH. POST, Apr. 30, 1997, at C13; John Markoff, *Dispute Arises Over Proposal For Wiretaps*, N.Y. TIMES, February 15, 1997, at 35; Seth Schiesel, *F.B.I. Reduces Scope of Proposal on Wiretapping Phone Networks*, N.Y. TIMES, Jan. 15, 1997, at

notable and troubling aspect of this campaign is the FBI's effort to use CALEA, in contravention of explicit assurances during the drafting process, to require cellular phone companies and other wireless service providers to have location tracking capability built into their systems for law enforcement purposes.[144] The FBI is also claiming, for example, that CALEA mandates interception of certain conference calls after the targeted facility has been dropped from the conversation, thus continuing the surveillance against parties and facilities for which no judicial approval was granted.[145] Seeking to exploit the increasing value of signaling information, the FBI has argued that CALEA requires the configuration and delivery of a signaling channel that includes detailed message notifications about the targeted facility. The FBI maintains that this configuration and delivery should be performed whether or not there is a call in progress and for facilities not identified in the surveillance order.[146] In a provision with far reaching implications, anticipating the adoption of packet switching protocols that could obliterate the distinction between signaling and content,[147] the FBI and industry have proposed allowing carriers to deliver communication content to law enforcement under a mere pen register order, depending once again on law enforcement to sort out the signaling information from the content.[148]

### *A. Congress' Legislative Mandate for Surveillance Features Was Premised on the Effective Enforcement of Strict Privacy Protections*

CALEA was based on the dual premise that (i) Title III and other laws authorizing electronic surveillance have strict legal

---

A11; Jim McGee, *Heightened Tensions Over Digital Taps*, WASH. POST, Oct. 27, 1996, at H1; John Markoff, *Cellular Industry Rejects U.S. Plan for Surveillance*, N.Y. TIMES, Sept. 20, 1996, at A1; John Markoff, *F.B.I. Wants Advanced System To Vastly Increase Wiretapping*, N.Y. TIMES, Nov. 2, 1995, at A1.

[144] Telecommunications Industry Liaison Unit, FBI, Electronic Surveillance Interface Document, at 39, 50 (June 24, 1996)[hereinafter ESI Document].

[145] *Id.* at 17.

[146] *Id.* at 32 (feature status message providing updates whenever the subject alters a network-provided feature); 41 (surveillance status message indicating the status of the tap if the subject is not making or receiving a call); 36-37 (party hold and party join message); 32-33 (incoming call identifying message).

[147] *See* OTA ELECTRONIC SURVEILLANCE REPORT, *supra* note 108, at 57-61.

[148] TELECOMMUNICATIONS INDUSTRY ASSOC., STANDARDS PROPOSAL NO. 3580-A, PROPOSED NEW STANDARD, "LAWFULLY AUTHORIZED ELECTRONIC SURVEILLANCE," 22-25 (July 31, 1997) [hereinafter SP 3580-A].

requirements and (ii) those requirements are being stringently enforced by the courts to protect privacy. As suggested above, this premise is becoming increasingly tenuous. If privacy protections afforded by the wiretap laws are not being strictly enforced, then the foundation of CALEA falters and the legislation becomes far more threatening, requiring as it does the ubiquitous adoption of features in the nation's telephone systems to ensure ready government access.

The premise of CALEA would also be negated by legislative weakening of the wiretap standards. Already the Justice Department has successfully won Congressional repeal of the provision extending ECPA to wireless data transfers.[149] The extension of ECPA to wireless data transfers was one of the privacy enhancements adopted in CALEA with the intent of balancing privacy concerns with law enforcement needs.[150] In addition, in its proposed anti-terrorism law forwarded to Congress in 1995, the Clinton Administration sought numerous weakening changes in Title III, including: (i) weakening the sanctions against illegal wiretapping, (ii) facilitating the procurement of roving taps and warrantless taps,[151] and (iii) creating exemptions from the carefully crafted privacy protection standards of the Foreign Intelligence Surveillance Act.[152] Although many of the Clinton changes were not enacted, the Justice Department has continued to pursue them and has proposed others that would loosen the privacy standards of the wiretap laws.[153]

As discussed in Section VIII, many of the proposed changes in the wiretap laws should be rejected on the merits. However, the fact that CALEA now requires telephone companies to design their systems to facilitate law enforcement surveillance is an additional reason to oppose any weakening of the wiretap standards. If the Executive Branch and Congress wish to fulfill the intent of CALEA, they should strengthen, not weaken, the privacy protections of Title III, ECPA and FISA. Unless these laws, in light of judicial interpretation and continuing technological developments, offer meaningful protection to privacy, the foundations of CALEA will be eroded.

---

[149] *See* Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 731, 110 Stat. 1214, 1303 (amending 18 U.S.C. § 2510(12)).

[150] *See* Pub. L. No. 104-414, § 203.

[151] H. REP. No. 105-896 (1997).

[152] *See* Pub. L. No. 104-132, § 401, 110 Stat, 1214, 1258.

[153] *See* JULY 1996 ELECTRONIC SURVEILLANCE REPORT TO CONGRESS, *supra* note 6.

### *B. In CALEA, Congress Denied the Government Design Control and Mandated Privacy Protection*

During the Bush Administration, the Justice Department urged Congress to adopt legislation that would have created de facto licensing authority over the development and deployment of new communications technology.[154] Telecommunications companies and civil liberties groups opposed the legislation, arguing that any legislation should be narrowly crafted to address identified problems while providing for public accountability and protecting privacy and not interfering with the innovation and competitiveness that have fueled the digital revolution. After hearings and consultations with industry, privacy groups, and law enforcement, Congress rejected the broad approach originally proposed by the FBI. Instead, with the strong support of the FBI, Congress enacted CALEA, which established minimum functional requirements intended to preserve rather than expand law enforcement access to communications, and deferred to industry to develop solutions.[155]

CALEA requires telephone companies to design (and in some cases retrofit) their networks to ensure that law enforcement agencies can carry out electronic surveillance on advanced digital equipment and services.[156] Three of its four requirements are intended to preserve law enforcement access. These pertain to (1) the interception of call content;[157] (2) the interception of call-identifying information;[158] and (3) the delivery to law enforcement of intercepted call content and call-identifying information.[159] In contrast, the fourth requirement of CALEA, section 103(a)(4), requires carriers to protect the privacy and security of communications not authorized to be intercepted.[160]

Congress intended that, in the first instance, common carriers and equipment manufacturers, not government agencies, would develop publicly the details for implementation of these assistance

---

[154] *Digital Telephony Hearings, supra* note 9, at 67 (prepared statement of Jerry Berman and Ronald L. Plesser); 71 (Interim Report of the Digital Privacy and Security Working Group on the FBI's Digital Telephony Proposals).

[155] Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. § 1001 *et seq.* (1994)).

[156] 47 U.S.C. § 1002(a).

[157] *Id.* at § 1002(a)(1).

[158] *Id.* at § 1002(a)(2).

[159] *Id.* at § 1002(a)(3).

[160] *Id.* at § 1002(a)(4).

requirements.[161] Congress expected that this approach would temper law enforcement demands with considerations of privacy and innovation, as well as cost and competitiveness. If industry failed to produce a standard or if any agency or person had concerns about the standard, the legislation gave the Federal Communications Commission the authority to develop an appropriate standard, taking into account the need to protect privacy and to promote innovation.[162]

A distinction should be drawn between what CALEA mandated as a minimum national standard for law enforcement access versus what expansions in surveillance capability will be available to law enforcement as a result of market-driven technological developments. Before CALEA, some changes in telecommunications technology were making law enforcement surveillance harder, while other changes were making surveillance easier or more productive. CALEA was intended to "preserve the status quo" by ensuring that technological developments did not erode law enforcement access to call content and identifying information. Congress did not intend to impede the development of technology that makes surveillance easier or more fruitful, nor did it intend to deny law enforcement the authority to take advantage of those developments.[163] Congress left intact the existing authority under 18 U.S.C. § 2518(4), which authorizes law enforcement to take advantage of all technological developments enhancing surveillance capability and requires companies to make available whatever advanced capability they have. But Congress did not mandate the nationwide ubiquitous installation of every technologically possible surveillance enhancement. Instead, Congress mandated the nationwide availability only of certain minimum features, based upon its understanding of past surveillance practices as described in the CALEA hearings and based upon the FBI's description in the CALEA hearings of what its needs were.[164]

---

[161] *See* H.R. REP. No. 103-827, pt. 1, at 26 (1994).

[162] *See* CALEA, §107(b) (codified at 47 U.S.C. § 1006(b)). *See* H.R. REP. No. 103-827, pt. 1, at 27.

[163] Congress did intend in CALEA to raise the legal standard for access to certain categories of information, including location information that was already available in some systems and transactional data associated with e-mail. *See* H.R. REP. No. 103-827, pt. 1, at 17-18, 31-32.

[164] *See* H.R. REP. No. 103-827, at 17-18, 31-32.

### C. *CALEA Implementation: Law Enforcement Efforts to Require Carriers to Provide Expanded Surveillance Capabilities*

In some respects, the checks and balances Congress wrote into CALEA have worked as intended. The FBI published in the Federal Register, under a notice and comment procedure, a capacity notice that was widely criticized and withdrawn.[165] The FBI published a second capacity notice revealing much more data about historical surveillance patterns,[166] but that second notice also raised serious questions which the Bureau must address in finalizing the capacity requirements. In terms of capability, industry bodies drafted "safe harbor" technical standards to provide the detail necessary to translate CALEA's broad functional requirements into network and equipment specifications.[167] The FBI had extensive input in the standards process, articulating law enforcement's desires and pushing hard for an expansive reading of the requirements.

Unfortunately, the FBI's participation went beyond the consultation intended by Congress and instead amounted to an effort to dominate the standards process and dictate specific surveillance features. Nonetheless, as of October 1997, industry had largely rejected FBI demands for surveillance features that, in contravention of the clear intent of CALEA, would expand the government's electronic surveillance capability beyond its current reach.[168] In two respects, however, industry acceded to FBI demands for features that would go beyond the status quo.

(1) *Location information.* Industry yielded to FBI insistence that cellular and other wireless systems be designed to provide information on the location of their customers as they make and receive calls. This involves capturing and delivering to law

---

[165] Implementation of the Communications Assistance for Law Enforcement Act, 60 Fed. Reg. 53643 (1995) (Initial Notice and Request for Comments).

[166] Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, 62 Fed. Reg. 1902 (1997) (Second Notice and Request for Comments).

[167] CALEA, § 107(a) (codified at 47 U.S.C. § 1006(a) (1994)).

[168] The House Judiciary Committee set forth its intent as follows:

> The Committee intends the assistance requirements in section 2602 to be both a floor and a ceiling. The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past. The Committee urges against overbroad interpretation of the requirements. . . .The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements.

H.R. REP. No. 103-827, at 22-23.

enforcement the signals that identify a wireless telephone user's location for call processing purposes.[169] It is clear from the legislative history that Congress did not intend to impose geographic location information as a CALEA requirement with respect to cellular or other wireless systems.[170] Concerns with "location tracking" were initially a major source of opposition to the legislation, so the FBI was eager to disavow any interest in location information at an early stage. Thus, early in 1994, the FBI expressly assured Congress that CALEA did not mandate provision of location information,[171] and nothing in the legislative history suggests that any of the changes made as the legislation proceeded through the drafting process were intended to bring location information within the scope of CALEA requirements.

(2) *Packet switching.* In a decision that has potentially far-reaching implications for the future of telephony, the Internet and government surveillance, the proposed CALEA implementation standard issued in July 1997 would allow telecommunications companies using "packet switching"[172] to provide the full content of customer communications to the government even when the

---

[169] *See* Gidari, *supra* note 84, at 70.

[170] "[T]he bill requires telecommunications carriers to ensure their systems have the capability to. . . (2) Isolate expeditiously information identifying the originating and destination numbers of targeted communications, but not the physical location of targets . . . . " H.R. REP. NO. 103-827, pt. 1, at 16.

[171] In the hearings leading to enactment of CALEA, FBI Director Freeh testified that CALEA would not require carriers to make location information uniformly available. Freeh testified that "call setup information" (later "call-identifying information") listed as a CALEA requirement was not intended to include location information. Freeh was very clear in disavowing any interest in covering such information:

> [Call setup information] does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent whatsoever, with reference to this term, to acquire anything that could properly be called 'tracking' information.

*Digital Telephony Hearings, supra* note 9, at 29.

[172] In the future, telecommunications systems will rely increasingly on "packet switching" protocols similar to those used on the Internet. This development has potentially profound implications for government surveillance. In a packet switching system, communications are broken up into individual packets, each of which contains a segment of the communication plus addressing information that gets the packets to their intended destination, where they are reassembled. Previously utilized primarily on the Internet for electronic communications, this technology offers substantial advantages in the voice environment as well, and telecommunications companies are beginning to incorporate it in their systems. *See* OTA ELECTRONIC SURVEILLANCE REPORT, *supra* note 108, at 57-61.

government is only authorized to intercept addressing or signaling data.[173] Despite indications that it is feasible to provide signaling information separate from the content in a packet switching environment, the proposed standard would allow companies to deliver the entire packet data stream, including call content, when law enforcement is entitled to receive only dialing or signaling information under a pen register order. Such orders are issued without probable cause and without the discretionary review accorded to full call content interceptions. The proposed CALEA standard relies on law enforcement to sort out the addressing information from the content, keeping the former but ignoring the latter. This approach, were it followed, could totally obliterate the distinction between call content and signaling information that was a core assumption of ECPA and of CALEA itself. It also would violate section 103(a)(4) of CALEA, which requires the telecommunications industry to protect communications not authorized to be intercepted.

In the old analog systems, law enforcement agencies authorized to receive signaling information were provided with access to the target's entire line, including content.[174] With subsequent developments in technology, the signaling data was carried on a channel separate from the call content. In this respect, technology itself enhanced privacy, creating an environment in which a law enforcement agency conducting a pen register could receive only information it was entitled to receive. Absent CALEA, packet switching might have reversed that privacy enhancement. However, CALEA imposed on the industry an affirmative obligation to protect privacy. Yet, the proposed industry standard initially failed to ensure that law enforcement agencies receive only the information appropriate to the level of authorization in hand.

Another capability sought by the FBI, but rejected by industry as of November 1997, was the ability to monitor all conversations during a conference call initiated by a targeted facility, even if the targeted facility is on hold or has hung up from the call.[175] It is

---

[173] SP 3580-A, *supra* note 148, at 22-25.

[174] *See* Ellis v. State, 256 Ga. 751, 753, 353 S.E.2d 19, 21 (1987).

[175] The matter arises as follows: A is the intercept subject. A sets up a conference call with B and C using the conference call capability provided by A's service provider. Then A puts B and C on hold (or hangs up entirely) and calls D. The FBI is seeking the delivery of both A's conversation with D and the conversation between B and C. It is not clear that there is legal authority to intercept the ongoing conversation between B and C after A has hung up. Title III, embodying the Fourth Amendment standard of particularity, requires the

questionable whether law enforcement has authority under the particularity requirement of the Fourth Amendment and Title III to intercept communications involving only non-targeted facilities just because a targeted facility initiated a conference call.

A number of the enhancements sought by the FBI were related to the Bureau's attempts to exploit transactional data. In legislative terms, the FBI tried to force more information into the definition of the CALEA term "call-identifying information." The plain language of CALEA and the legislative history indicate that "call-identifying information" means the numbers dialed by a subscriber to direct a communication, or other signaling information that serves the same call routing purpose as the dialed digits. This includes the switch-based information equivalent to a seven or ten digit phone number that directs a call when a voice dialing or speed dialing feature is used.[176] The term likely includes information indicating that the party under surveillance has terminated a call by hanging up. However, the FBI argued that this term includes much more. For instance, at various points in the CALEA implementation process, the FBI argued that carriers must build in the capability to provide not only location-related information on wireless phone users, but "location-related updates during calls." The Bureau also asked for detailed "call progress" tones relating to both the target of the investigation and persons with whom the target is communicating, and messages during three-way calls that would indicate when a party, who is not the target of the surveillance, drops off a three-way call. Further, the FBI sought "voice message waiting" tones to notify the government when a surveillance target has a voice mail waiting and feature status messages that would notify the government in real

---

specification in the order of the telephone facility to be tapped and the particular conversations to be seized. The Supreme Court has held that conversations between unknown individuals using a specified telephone line could be lawfully intercepted under Title III. *See* United States v. Kahn, 415 U.S. 143 (1973). Lower courts have upheld the roving tap authority so long as it is limited to the interception only of conversations of named subjects. *See* United States v. Ferrara, 771 F. Supp. 1266, 1318 (D. Mass. 1991); United States v. Silberman, 732 F. Supp. 1057, 1062 (S.D. Cal. 1990). No court has held that there is authority to intercept the communications of unknown persons using unspecified facilities while the named target is on another monitored call.

[176] H.R. REP. NO. 103-827, at 21 (1994).

time when a surveillance target changes his or her mix of service features.[177]

### *D. The Role of Congress and the FCC in Ensuring Balanced Implementation of CALEA*

Both Congress and the Federal Communications Commission (FCC) have oversight roles to ensure that CALEA is properly implemented in a way that preserves the crucial balance between privacy and law enforcement powers.

CALEA requires the FBI to obtain annual appropriations for implementing the law.[178] This has allowed the House and Senate Appropriations Committees to examine the issues posed by implementation and to withhold funds until they are satisfied that implementation is proceeding appropriately. In 1995, the first year after CALEA was enacted, Congress declined to appropriate any funds for implementation.[179] In 1996, Congress established a CALEA Compliance Fund but blocked the FBI from expending any funds until it had submitted a detailed implementation plan.[180] In 1997, after reviewing the implementation plan, both Houses expressed concern about the lack of priority in the FBI's plan. The Senate Appropriations Committee declined the Administration's request for $100,000,000.[181] Instead, the Committee directed the FBI to create a working group with the purpose of creating "a more rational, reasonable, and cost-effective CALEA implementation plan."[182] The Committee recommended that no funds be expended for CALEA implementation until the working group provided a plan satisfactory to the Committee.[183] The House-Senate conference committee on the fiscal 1998 appropriation for the Department of Justice came to a somewhat different resolution. The conference agreement, which passed the Congress and was signed into law, included no additional funding for CALEA implementation, but the report noted that there had been recent discussions between the Committees on Appropriations,

---

[177] ESI Document, *supra* note 144, at 36 (party disconnect, party hold, and party join messages), 34 (message waiting indicator), 32 (feature status message).

[178] *See* Pub. L. No. 103-414, § 110; H.R. REP. No. 103-827, at 19 (1994).

[179] *See* Pub. L. No. 104-99.

[180] H.R. REP. 104-863 (1996), *printed in* CONG. REC. H1164, H11646 and H11649-50 (1996).

[181] S. REP. No. 105-48, at 23 (1994).

[182] *Id.*

[183] *Id.*

the Justice Department and representatives of the telecommunications industry.[184] As a result of these discussions, the conference report stated, an agreement had been reached, which included a commitment by industry and law enforcement to provide to the Committees on January 4, 1997 cost estimates for the deployment of "the solution," along with a timetable for deployment and signed agreements from two carriers or equipment manufacturers (presumably to begin development of the solution).[185]

The FCC has ample jurisdiction to ensure that CALEA implementation protects privacy. The most important source of the FCC's jurisdiction is section 107 of CALEA, which authorizes the Commission to intervene to establish an implementation standard if the industry standard-setting process fails to produce an acceptable standard.[186] In that event, the FCC is required to ensure that the standard protects the privacy and security of communications not authorized to be intercepted and achieves other specified public policy goals, including promotion of technology innovation.[187] Any party, including public interest groups, may seek a proceeding under section 107 to challenge CALEA implementation. Also, section 105 of CALEA requires that carriers ensure that any interception within their switching premises be activated only in compliance with a court order and with the affirmative intervention of an individual officer or employee of the carrier. These provisions give the FCC ample authority to reject elements of the FBI-industry implementation standard that go beyond preserving the status quo and that do not adequately protect privacy. Attention also needs to be given to law enforcement compliance with the new language in the pen register and trap and trace section, requiring the use of reasonably available technology that limits pen registers and trap and trace devices to the collection of "dialing and signaling information used in call processing."[188]

---

[184] 143 CONG. REC. H10836 (1997).

[185] *Id.*

[186] Section 107 of CALEA states:

> If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards that. . .(2) protect the privacy and security of communications not authorized to be intercepted.

47 U.S.C. § 1006.

[187] CALEA, § 107(b)(1)-(5) (codified at 47 U.S.C. § 1006 (b)(1)-(5)).

[188] 18 U.S.C. § 3121(c) (1996).

### *E. CALEA as an Exercise in Control and Accountability*

CALEA imposed on the nation's telecommunications systems an unprecedented new obligation: to design their systems and services with the objective (along with all their other objectives related to provision of quality service) of ensuring the government's ability to carry out electronic surveillance. It was the judgment of Congress that wiretapping was a law enforcement capability worth preserving. And Congress had before it the acknowledgment of industry representatives that, unless action was legislatively forced, the electronic surveillance capability might be lost or substantially diminished as a result of technological development.[189] However, Congress fully recognized the dangers to privacy and technological innovation inherent in what it was mandating. Therefore, Congress wove throughout CALEA a series of limitations, and it established a series of checks and balances, lodging in a number of entities authority to influence or control the implementation of the law.

Thus, CALEA spelled out four capability requirements.[190] These four requirements, while phrased in general terms, are nonetheless exclusive; anything that law enforcement would want to require under CALEA has to fit under one of these four requirements or it cannot be mandated. Further, Congress specifically excluded certain capabilities. It specified that carriers have no obligation to ensure the ability to unscramble encrypted communications when the user controls the encryption keys.[191] It specified that a given carrier has no responsibility to continue monitoring when a target using cellular roaming moves out of the carrier's service area and into the service area of another carrier.[192] The legislation denied to law enforcement any authority to dictate system design.[193] Instead, the legislation defers to industry to establish standards.[194] Any publicly available standard adopted in good faith to implement the requirements of the law constitutes a safe harbor. Companies are deemed in compliance with the act if they comply with the industry standard.[195] Law enforcement cannot unilaterally declare a standard deficient. If law enforcement

---

189 H.R. REP. No. 103-827, pt. 1, 15-16 (1994).
190 CALEA, § 103(a)(1)-(4) (codified at 47 U.S.C. § 1002(a)(1)-(4)).
191 *Id.* at § 103(b)(3) (codified at 47 U.S.C. § 1002(b)(3)).
192 *Id.* at § 103(d) (codified at 47 U.S.C. § 1002 (d)).
193 *Id.* at § 103(b)(1) (codified at 47 U.S.C. § 1002(b)(1)).
194 *Id.* at § 107(a) (codified at 47 U.S.C. § 1006(a)).
195 CALEA, § 107(a) (codified at 47 U.S.C. § 1006(a)).

is not satisfied with the industry standard, it must petition the FCC to adopt a different standard, and the FCC's latitude is limited by a specified set of criteria that must guide the development of a standard.[196]

The concept of "reasonableness" appears throughout the legislation. Carriers are obligated to make available only such call-identifying data as is "reasonably available."[197] The FCC may grant an extension of time for compliance if compliance within the specified period is not "reasonably achievable."[198] A court can order compliance only if alternative technologies or facilities of another carrier are not "reasonably available" to law enforcement for implementing the interception and only if compliance is "reasonably achievable."[199] Carriers are not required to bear the costs of retrofitting equipment installed before January 1, 1995 if compliance is "not reasonably achievable."[200]

Congress also included in CALEA mechanisms of public accountability. Capacity requirements must be adopted only after a public notice and comment proceeding in the Federal Register.[201] Technical standards for implementing the capability requirements have to be "publicly available."[202] Funding is subject to the annual appropriations process, with hearings, reports, and enacted laws. The Attorney General is required to issue periodic reports on implementation.[203]

As a series of checks and balances, CALEA placed authority over implementation in a number of hands. Thus, industry bodies develop the standards. Upon the petition of industry, law enforcement or any other person, the FCC can develop a superseding standard. The FCC was also granted the authority to issue extensions of the compliance deadline, and to determine that compliance is not reasonably achievable with respect to a certain service or carrier. The courts have jurisdiction over compliance proceedings.[204] Congress has control through its appropriations committees, which must annually appropriate funds for compliance and therefore can use the power of the purse to control how

---

196 CALEA, § 107(b) (codified at 47 U.S.C. § 1006(b)).
197 *Id.* at § 103(a)(2) (codified at 47 U.S.C. § 1002 (a)(2)).
198 *Id.* at § 107(c) (codified at 47 U.S.C. § 1006(c)).
199 *Id.* at § 108(a) (codified at 47 U.S.C. § 1007(a)).
200 *Id.* at § 109(b)(2) (codified at 47 U.S.C. § 1008(b)(2)).
201 CALEA, § 104 (codified at 47 U.S.C. § 1003).
202 *Id.* at § 107(a)(2) (codified at 47 U.S.C. § 1006(a)(2)).
203 *Id.* at § 112 (codified at 47 U.S.C. § 1010).
204 *Id.* at § 108(a) (codified at 47 U.S.C. § 1007(a)).

the legislation is being implemented.[205] The Judiciary Committees and the Commerce Committees, as the authorizing committees, can always revisit the legislation and amend it as circumstances change and in light of experience.

For the CALEA legislation to work in a balanced fashion, the limitations and reasonableness provisions written into law by Congress must be invoked and the entities with responsibility for overseeing the implementation of the statute must choose to exercise their authority to preserve the intended balance. The FBI has substantial resources and the politically powerful anti-crime rhetoric at its disposal, and it has the ability to mobilize state and local law enforcement to promote its position. Thus, the FBI will dominate the implementation process unless the other government institutions exercise the authority granted them under the statute to promote the counterbalancing values of privacy and innovation. In this sense, CALEA is merely one more manifestation of the on-going efforts in our democratic society to regulate the police and national security powers of the government. Congress, deeming it necessary to preserve an electronic surveillance authority, can legislate limits and controls, but those limits must be enforced and the controls must be exercised by the executive and regulatory agencies, future Congresses, and the courts.

## VI. Realizing the Privacy-Enhancing Potential of Encryption Technology

*Illegal electronic intrusion into computer networks is a rapidly escalating crime problem. White collar criminals, economic espionage agents, organized crime groups, foreign intelligence agents, and terrorist groups have been identified as "electronic intruders" responsible for penetrations of American computer networks. It is estimated that the Pentagon's computers are subject to hackers' attempts 250,000 times a year. The United States Government relies upon the National Information Infrastructure (NII) for the efficient, uninterrupted flow of electronic information for air traffic control, military communications, energy distribution, public safety, and other essential government programs and services. Intelligence and industry forecasts indicate the United States is just beginning to realize the potentially damaging effects and extent of the computer crime problem.*[206]

---

[205] CALEA, § 110 (codified at 47 U.S.C. § 1009).

[206] FBI, U.S. Dept. of Justice, FY 1998 Authorization and Budget Request for the Congress, at A-3 (1997).

*[O]n balance, the advantages of more widespread use of cryptography outweigh the disadvantages.*[207]

Newer communications media are inherently insecure.[208] Wireless telephones have great advantages in convenience compared with wireline counterparts, yet, since wireless phones transmit over the airwaves, eavesdropping is easier not only for curious neighbors but also for burglars identifying potential targets and industrial spies stealing trade secrets.[209] Similarly, decentralized computer networks such as the Internet have low barriers to entry, are much less expensive, are more robust and can be used to accomplish a far greater variety of tasks than the proprietary networks of the past, but, again, at the expense of intrinsic security. The vulnerabilities of the national and global information infrastructures have been recognized not only by the FBI, but also by the Defense Science Board Task Force on Information Warfare-Defense[210] and by the President's Commission on Critical Infrastructure Protection.[211] The losses to date from inadequate system security are enormous. In one series of transactions in 1994, an international group of criminals penetrated Citicorp's computerized electronic transfer system and moved about $12 million from legitimate customer accounts into their own accounts in banks around the world.[212] In 1996, after a comprehensive study, the National Research Council concluded, "Of all the information vulnerabilities facing U.S. companies internationally, electronic vulnerabilities appear to be the most significant."[213]

Given these inherent vulnerabilities, widespread use of encryption to protect communications and stored data is essential to prevent fraud and other forms of crime in the digital age. At the same time, encryption poses challenges to law enforcement and

---

[207] NRC REPORT, *supra* note 3, at 300.

[208] HAL ABELSON ET AL., THE RISKS OF KEY RECOVERY, KEY ESCROW AND TRUSTED THIRD-PARTY ENCRYPTION, at 5 (1997).

[209] *See Cellular Privacy Hearing*, *supra* note 2.

[210] Report of the Defense Science Board Task Force on Information Warfare-Defense (Nov. 1996) (last modified June 29, 1997) <http://www.jya.com/iwd.htm>. The Task Force recommended spending $3 billion over the next five years hardening the nation's telecommunications infrastructure against attack, noting that the Defense Information Infrastructure is largely dependent upon the commercial telecommunications system.

[211] President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructure (Nov. 1997) available at <http://www.pccip.gov/report_index.html>.

[212] *See* NRC REPORT, *supra* note 3, at 23.

[213] *Id.* at 31.

national security agencies, which have raised the specter of criminal suspects' undecipherable stored information or voice communications. This has led to a vigorous legislative debate over control of encryption technology.[214]

In some ways, the encryption debate has been a conflict between two competing models of security, one in which private individuals, businesses and governments choose from a variety of encryption options to protect their security, and another wherein the federal government assumes the primary responsibility for protecting personal and business as well as governmental security through government-promoted weaknesses in encryption technology.[215] While there are law enforcement equities on both sides of the encryption issue, the centralized model of security based on government-controlled encryption weaknesses is incompatible with certain defining characteristics of the digital communications revolution: decentralization, competition, globalization, and the dynamics of decreasing cost and increasing computing power that have put more control and more choices in the hands of end users.

The Executive Branch's various efforts to impose a centralized model of security on a decentralized medium have delayed full realization of the Internet's economic, personal and democratizing potential. They have also hurt the competitiveness of American computer companies by prohibiting export abroad, thereby inhibiting in the U.S. the use of strong encryption that is already available overseas.[216] At the same time, given the already widespread proliferation of user-controlled encryption technology, the centralized model cannot offer assurances of achieving the desired law enforcement access. Strong non-escrowed encryption is and will continue to be available to those who want it. There are currently hundreds of encryption products available worldwide. This led the National Research Council to conclude that, on balance, the security-enhancing, crime-preventing benefits of encryption outweigh the impediments to law enforcement.[217]

Globalization is a key factor, and the global market has rejected all government proposals to control encryption technology. U.S. proposals in 1993 for government agencies to serve as key escrow

---

[214] *Id.* at 31.

[215] *See* ABELSON ET AL., *supra* note 208, at 6-7.

[216] It has also been argued that there is a First Amendment right to use and export encryption. *See* Bernstein v. Department of State, 945 F. Supp. 1279 (N.D. Cal. 1996).

[217] NRC REPORT, *supra* note 3, at 300.

agents were immediately rejected by business and individual users as involving an unacceptable level of vulnerability.[218] More recent approaches that depend upon government licensing or "registration" of escrow agents or other forms of government control of decryption mechanisms (including proposals to require key recovery features as a condition of receiving public key certificates) are also not achieving market acceptance.[219] The type of ubiquitous, near-instantaneous key escrow, key recovery, or key management "infrastructure" sought by the U.S. government is so complex, so vulnerable, so expensive and/or so cumbersome — so fundamentally at odds with user needs — that it will not by accepted by users.[220]

Yet the market alone will not address all of the privacy issues posed by encryption. While it seems clear that most businesses and individuals will not trust the government or government-dictated private structures to hold their keys, it also seems clear that under some encryption applications, particularly those involving stored data, some users are interested in securing a means to recover their encrypted data if they lose their own key. (There is less incentive for development of key escrow for transmissions.) Market-based efforts to address this problem — responses to user needs — are resulting in a range of key escrow, key recovery, or "trusted third party" systems for decryption assistance.[221] These are quite different from the systems proposed by the Administration under its legislative proposal, which is voluntary in name only.[222] These user-driven, user-controlled data-recovery or key escrow arrangements will offer law enforcement an opportunity to satisfy many of its basic access needs for stored data.[223]

As the market develops key recovery arrangements, government agencies will be seeking access to those keys for law enforcement and national security purposes, to decrypt seized files and

---

[218] John Markoff, *Computer Code Plan Challenged*, N.Y. TIMES, May 29, 1993; John Markoff, *Panel Sees Flaws in Plan for Encoding*, N.Y. TIMES, June 5, 1993; John Schwartz, *U.S. Data Decoding Plan Delayed*, WASH. POST, June 8, 1993, at A12.

[219] Edmund L. Andrews, *U.S. Restrictions on Exports Aid German Software Maker*, N.Y. TIMES, Apr. 7, 1997, at D1.

[220] *See* ABELSON ET AL., *supra* note 208.

[221] *See id.*

[222] *Id.*

[223] In many cases (e.g., suspects communicating with their banks or engaging in credit card transactions or other on-line commercial transactions), there will be plaintext of messages and data readily available to the government by subpoena or other legal process.

communications intercepted under the wiretap laws. Government efforts to access stored keys will pose obvious privacy concerns. Given the centrality of encryption to privacy and security in the digital age, there is a strong argument that escrowed encryption keys and key recovery assistance should be entitled to greater protection than that traditionally accorded to so-called "third party records." In the past, as noted above in Section IV, the courts have accorded little Fourth Amendment protection to business records like checks or credit card records created in the course of commercial transactions and knowingly revealed to banks and other third parties.[224] The Fourth Amendment, however, may have stronger application to especially sensitive information such as a decryption key entrusted to a third party under an escrow arrangement.[225] Disclosure of keys, even escrowed keys, also raises serious questions under the Fifth Amendment's protection against compelled self incrimination.[226]

Encryption will play a central enabling role in the protection of privacy in the digital age. Government attempts to access keys or decryption assistance will raise important privacy interests. Reliance on the courts to sort out the issues will produce a possibly long period of uncertainty and conflicting decisions. Legislative action setting clear privacy standards for government access to keys and decryption assistance held by second or third parties would be far preferable. Such legislation should include standards that prohibit escrow agents from providing keys or decryp-

---

[224] United States v. Miller, 425 U.S. 435 (1976); Fisher v. United States, 425 U.S. 391 (1976).

[225] The compelled disclosure of decryption information poses concerns quite different from those normally applied to business records under *Miller* and *Fisher*. Current Fourth Amendment jurisprudence suggests that the government cannot always use a mere subpoena to compel even from a third party production of a person's private, personal documents. *Fisher*, 425 U.S. at 401 n. 7; 1 SARA S. BEALE ET AL., GRAND JURY LAW AND PRACTICE, § 6.27 (1986 & 1996 Cum. Supp.).

[226] Generally, the courts have held that a voluntarily created document does not contain compelled testimonial evidence. Almost all these cases, however, have arisen in the context of business records. The leading case, *Fisher v. United States*, *supra*, involved a subpoena of accountants' workpapers relating to two taxpayers, which were in the possession of the taxpayers' attorney. The *Fisher* Court itself recognized that there may be some category of private papers that are protected under the privilege against self-incrimination. *Fisher*, 425 U.S. at 414. The federal Circuit Courts of Appeals are split. Two federal Appeals Courts have held that the Fifth Amendment bars compelled disclosure of private, non-business papers. United States v. Davis, 636 F.2d 1028 (5th Cir. 1981), *cert. denied*, 454 U.S. 862 (1981); *In re* Grand Jury Proceedings, 632 F.2d 1033 (3d Cir. 1980).

tion assistance except in conformity with a court order issued upon a finding of probable cause and a showing that there is no feasible alternative of obtaining the plaintext, and should require minimization in the use of the key or assistance.[227]

## VII. Protecting Wireless Communications

In the network of networks that comprises the telecommunications "system" of today and the future, it is no longer appropriate to look at wireless telephone systems as distinct from wireline systems or to look at the telephone system as separate from the Internet. The increasing use of wireless communications services, the seamless integration of wireless and wireline networks, and the importance of wireless data links heighten the urgency of ensuring the privacy and security of wireless communications. In this context of a global communications network increasingly dependent on wireless links, it is a serious invasion of privacy to eavesdrop on wireless telephone conversations.[228] Wireless eavesdroppers are invading the privacy not only of the person who is using a wireless phone, but also of anybody else who is in the conversation using an ordinary landline telephone. As wireless telephones become more ubiquitous, scanning threatens the privacy of all telephone users.[229]

Encryption will play an essential role here too, for securing over-the-air links. But it is clear that there is a need for legislative improvements clarifying both the prohibitions against unauthorized private interception and the legal standards for governmental access to wireless transmissions.

*Location information*. As noted already, wireless telephone systems are developing the capability to provide more refined location information on wireless phone users. Nonconsensual government monitoring of location through a wireless phone implicates privacy interests.[230] Since wireless telephones are regularly carried

---

[227] Sen. Patrick J. Leahy (D-VT) introduced legislation in the 105th Congress, S. 376, with elements of such a privacy protection scheme.

[228] *Cellular Privacy Hearing*, *supra* note 2, at 10-11 (testimony of Jerry Berman).

[229] *Id.*

[230] In *United States v. Karo*, the Supreme Court held that the monitoring of a beeper in a private location is a search subject to the Fourth Amendment warrant requirement. 468 U.S. 705, 706 (1984). The Court distinguished this from the use of a beeper to follow an object being transported on the public roads, or to monitor the general vicinity of an object, both of which had been held not to implicate the Fourth Amendment in *United States v. Knotts*, 460 U.S. 276

into places where a person has a reasonable expectation of privacy, Congress should clarify the law by requiring a warrant based on a showing of probable cause for nonconsensual governmental access to real-time wireless telephone location information.

*Wireless data transfers*. At a time when wireless local area networks are proliferating and when wireless data transmissions could be used for everything from proprietary data to medical records, it is not clear that wireless data transfers are protected to the same extent as wireless voice communications. The status of legal protection for wireless data transfers has a confused history, leaving it unclear whether they are currently protected by ECPA. An industry and privacy task force concluded in 1991 that wireless transfers of data might not be covered by ECPA, and recommended that coverage be extended.[231] In 1994, in CALEA and with the support of the Administration, Congress passed a provision making it clear that the privacy of wireless data transfers was protected by ECPA.[232] But less than two years later, in the anti-terrorism act of 1996, Congress repealed the provision on the basis of the Justice Department's claim that the 1994 amendment was inappropriately overbroad.[233]

---

(1983). *Karo*, 468 U.S. 705, 714-716. Obviously, wireless phones are carried by their users into places where there is a legitimate expectation of privacy. Wireless phone location tracking through the facilities of service providers is becoming more precise, as a result of the E-911 requirements imposed by the FCC E-911 Order, and as a result of technical developments that are producing smaller and smaller cell sites and cell sectors. FCC E-911 Order, *supra* note 85. If anything, monitoring the location of wireless phones is more intrusive than the use of a beeper. The beeper cases usually involve the attachment of the beeper to an object (often contraband or precursor chemicals for illegal drug manufacture). Unlike drums of precursor chemicals, cellular phones are often directly associated with an individual user. They implicate movements of the person going about his or her daily life and entering a variety of locations (homes, offices) where there is a legitimate expectation of privacy. The ongoing nature of such monitoring (as opposed to the tracking of a barrel of precursor chemicals from the manufacturer to the clandestine laboratory in the typical beeper case) raises much more serious privacy interests. These interests merit full Fourth Amendment protection.

[231] *See Digital Telephony Hearings, supra* note 9, at 179, 183 (Final Report of the Privacy and Technology Task Force Submitted to Senator Patrick J. Leahy).

[232] *See* Pub. L. No. 103-414, § 203, 108 Stat. at 4291 (1994) (amending 18 U.S.C. § 2510(16)).

[233] Pub. L. No. 104-132, § 731 (1996). The repeal came at the behest of the Justice Department, which argued that the privacy provision was inappropriately overbroad, and included ham radio and CB radio broadcasts, which should not be privacy-protected. The Justice Department, reversing the Administration's earlier provision, argued that wireless data transfers were

This confusion should be resolved by appropriate legislative language extending the privacy protections of ECPA unambiguously to wireless data transfers.

*Interception devices.* ECPA made it a crime to manufacture, sell, assemble, possess or advertise any device that is "primarily useful" for the interception of wireless telephone conversations.[234] Unfortunately, the effectiveness of this provision is quite limited, since it is difficult to prove that a device capable of intercepting cellular and a range of other frequencies is "*primarily* useful" for prohibited interceptions. Congress should delete the word "primarily," at least as it affects manufacture, sale, assembly, and advertisement.

The manufacture and import of scanners equipped or readily alterable to receive transmissions in frequencies assigned to the "domestic cellular radio telecommunications service" are prohibited under section 302(d) of the Communications Act.[235] However, since the enactment of this provision, a new category of services called "commercial mobile radio services" has been created, into which cellular, as well as additional mobile services at different frequency ranges, such as personal communications systems (PCS), have been added. The law does not appear to prohibit manufacture and import of devices equipped to scan these frequencies. Congress should extend the section 302 prohibition to the parts of the spectrum used for PCS and other wireless telephone communications.

## VIII. Strengthening the Wiretap Laws to Reestablish the Principles of *Katz* and *Berger*

The balance among the interests of law enforcement, privacy and technological innovation has come under challenge in recent years. Steadily growing numbers of wiretaps, longer and longer surveillances intercepting more and more communications suggest that the wiretapping laws are not working as originally intended to constrain the use of this highly intrusive technique. These developments point to the need for amendments to the law to reestablish the balance Congress originally sought. Until such corrective amendments are enacted, it would be premature to con-

---

already protected. Rather than propose narrower language to make that clear, the Administration successfully argued for repeal of the entire provision. In the context of the many issues in the terrorism bill, this one received little attention.

[234] *See* 18 U.S.C. § 2512 (1996).

[235] 47 U.S.C. § 302(a)(d) (1996).

sider proposals to further expand the scope of, or weaken the privacy protection standards in, the wiretap laws.

Unfortunately, the focus of the legislative debate recently has been in the opposite direction, on proposals to give the government greater latitude in wiretapping. As noted above in Section VII, the Justice Department sought and obtained repeal of one of the privacy protections that were adopted in CALEA. Further, the President sought in his terrorism legislation a series of other changes in the wiretap laws that would have weakened the sanctions against illegal government wiretapping; weakened the standards for so-called "roving taps;" and expanded the availability of warrantless taps in "emergency" situations.[236] While these other changes were ultimately rejected, they were considered and debated without attention to counterbalancing proposals to enhance privacy.

The Clinton Administration has continued to support these and other changes in the wiretap laws. In July 1996, the Department of Justice submitted to Congress a report recommending eight amendments to the federal electronic surveillance laws, including the change in the statute's exclusionary rule, the loosening of the standard for "roving taps," and additional authority for emergency wiretaps without judicial approval.[237] The report stated that "several other proposed amendments are under consideration by the Department, . . . [which] are expected to be submitted to Congress at a later time."[238]

By far, the most dangerous change the Administration proposed was an amendment to Title III to allow courts to receive evidence obtained in violation of the wiretap law. When Title III was adopted, Congress included a statutory exclusion rule, calling it "an integral part of the system of limitations designed to protect privacy."[239] The Administration proposal, although sometimes described as a good faith exception, would require a person to

---

[236] Omnibus Counterterrorism Act of 1995, H.R. 896 (1995); S. 390 (1995). *See also* Comprehensive Antiterrorism Act of 1995, H.R. 1710 (1995) (Republican terrorism bill).

[237] *See* JULY 1996 ELECTRONIC SURVEILLANCE REPORT TO CONGRESS, *supra* note 6.

[238] *Id.* Significantly, the Justice Department report was able to identify only one revision to the wiretap laws that would have enabled law enforcement authorities to better fulfill their responsibilities. This was the addition of an additional predicate offense for the use of wiretapping, namely, 18 U.S.C. § 842, involving manufacturing, dealing in, and importing explosive materials without a license and the unlawful distribution of explosive materials.

[239] S. REP. No. 90-1097, at 96 (1968).

prove "bad faith" on the part of the government, before evidence will be excluded for violation of the law - an almost impossible undertaking. The Administration's 1995 proposal was not limited to situations where law enforcement officers relied on a technically defective warrant.[240] The Supreme Court has already held that the statutory suppression or exclusion rule in Title III is not to be applied to technical violations.[241] The Administration proposal would apply to all provisions of the wiretap law, including those governing the conduct of the government after the warrant is issued. Thus, it would remove the only real incentive against violating such central protections as the minimization and evidence preservation rules. The Administration argued that the proposed change would merely apply to wiretaps the same standard applicable to other searches. However, the constitutional presupposition of Title III is that special, heightened standards are necessary for electronic surveillance because of its unique nature.[242]

If amendments to the wiretap laws are to be considered, then it must be in the context that gives equal weight to an examination of issues from a privacy perspective. It should be clear from the discussion in Section II (B) that amendments are necessary to repair the damage done by judicial interpretation. Specifically, it is time to strengthen the minimization rule and to clarify the requirement that law enforcement exhaust other techniques before seeking an interception order. Other changes are necessary as well:

*Transactional data.* Advanced signaling systems for voice communications have blurred the distinction between call identifying information and call content. Currently, the standards for governmental access to signaling data under what are known as "pen registers" and "trap and trace devices" require a court order, but the statute puts the judge in a purely ministerial role: the sole function of the judge is to determine whether the signature of an Assistant United States Attorney is on the application.[243] One improvement would be an amendment requiring that the judge exercise discretion and only approve the request upon finding,

---

[240] S. 390, at § 105 (1995) (Omnibus Counterterrorism Act of 1995).

[241] United States v. Giordano, 416 U.S. 505, 527-28 (1974) ("[W]e think Congress intended to require suppression where there is failure to satisfy any of those statutory requirements *that directly and substantially implement* [the intended limitations on the use of wiretapping]" (emphasis added)).

[242] S. REP. No. 90-1097, at 96 (1968).

[243] *See* 18 U.S.C. § 3123(a) (1996).

based on a showing by the government, that the information sought is relevant and material to an ongoing criminal investigation. As argued in Section VII, above, one type of transactional data, namely real-time location information generated in wireless telephone systems, implicates such serious privacy interests that Congress should clarify the law by requiring a warrant based on a showing of probable cause for nonconsensual governmental access to such information when obtained on a real-time, tracking basis. In light of the growing significance of transactional and signaling data, it is time for Congress to examine more generally the implications of government access to and analysis of all forms of such information for subscriber profiling purposes.

*Roving wiretaps.* The Justice Department has proposed loosening the standard for so-called roving or multi-point wiretaps.[244] Roving taps (taps placed on a phone line other than the line subscribed to by the target of a surveillance order) are considered especially sensitive because they often entail tapping the phone of someone who is not the subject of an investigation and not suspected of any involvement in criminal conduct.[245] The Justice Department argues that the current statute requires the government to show the subjective intent of the subject to evade interception.[246] The Department argues that it should be enough that the subject's actions have the objective result of thwarting interception.[247] If Congress changes the standard for roving taps, it should add to the law an explicit prohibition against interception of the conversations of innocent third parties, so that such conversations would be outside the scope of the warrant. While this conforms to stated Justice Department policy and the few lower court decisions,[248] it would be desirable to write the principle into the Title III statute.

---

[244] *See* 18 U.S.C. § 2518(11) (1996); S. 390, at § 108 (1995).

[245] *See e.g.* United States v. Bianco, 998 F.2d 1112, 1122-24 (1st Cir. 1993), *cert. denied*, 114 S. Ct. 1644 (1994). *See generally*, Michael Goldsmith, *Eavesdropping Reform: The Legality of Roving Surveillance*, 1987 U. ILL. L. REV. 401 (1987).

[246] *See* JULY 1996 ELECTRONIC SURVEILLANCE REPORT TO CONGRESS, *supra* note 6, at 33-34.

[247] *See id. See also* H.R. Rep. 104-383 (1995) (Comprehensive Antiterrorism Act) (citing "[t]oday's rapidly changing telecommunications technology" and the widespread use of "cellular telephones, pagers, portable fax machines and portable computers" as justification for the roving tap changes).

[248] *See* United States v. Ferrara, 771 F. Supp. 1266, 1318 (D. Mass. 1991); United States v. Silberman, 732 F. Supp. 1057, 1062 (S. D. Cal. 1990).

*Emergency wiretaps.* Title III allows the use of wiretapping without court approval in emergency situations involving immediate danger of death or serious physical injury, threats to the national security, or organized crime. In such cases, an application for a court order must be filed within forty-eight hours.[249] The Administration has recommended expanding this emergency authority to include terrorism cases that do not involve an immediate danger of injury or threat to the national security.[250]

More appropriate than the Administration's proposed change would be a careful reexamination of the Title III emergency exception itself. The emergency exception was enacted in 1968. Now, given the pervasiveness of faxes, wireless telephones, and e-mail, it is hard to understand why it would ever be impossible or even difficult to reach a federal judge to obtain prior approval for electronic surveillance. It should be noted that in 1977 the Federal Rules of Criminal Procedure were amended to allow for telephonic submission of search warrant applications and affidavits in emergency situations, with procedures for contemporaneous recording of the oral testimony supporting probable cause.[251] This seems to be a far more appropriate model for updating the emergency tap authority of Title III.[252]

*Limiting use of FISA in criminal cases.* In most FISA cases, since the target is never notified of the existence of the surveillance, there is never an opportunity for after-the-fact adversarial review of the legality of the taps.[253] Even if there is a criminal investigation and notice is provided, the adversarial hearing is inadequate because the target is not allowed to see the affidavit that provided the basis for the order. The increasing use of FISA intercepts in criminal cases suggests that FISA is turning out to be a bigger than expected exception to ordinary wiretap procedures.[254] In espionage cases involving U.S. persons, long after it is clear that the subject is suspected of engaging in espionage, and

---

[249] 18 U.S.C. § 2518(7) (1996).

[250] *See* S. 390, at § 107 (1995).

[251] FED. R. CRIM. P. 41(c)(2) (1997).

[252] In addition, it would be appropriate to update the emergency procedures under FISA, 50 U.S.C. § 1805(e), written in 1979, which allow emergency taps for twenty-four hours.

[253] *See Foreign Intelligence Surveillance Act: Hearings before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary*, 98th Cong., at 27-35 (1983) (testimony of Mark H. Lynch, American Civil Liberties Union).

[254] *See* McGee & Duffy, *supra* note 78, at 13.

long after there is adequate basis to open a criminal case and obtain a wiretap order under Title III, the FBI continues to proceed under a FISA order, maintaining that the investigation serves a dual purpose of counterintelligence and criminal investigation.[255] This is directly contrary to the intent of FISA.[256] FISA should be amended to exclude from any criminal trial evidence obtained from a FISA surveillance after there was probable cause to believe that a crime was being committed. This will require the FBI to obtain a Title III order at the appropriate time, making the wiretap subject to the higher standards applicable to Title III intercepts.

## IX. International Issues

The Internet is a global medium. One of its great strengths is the ease with which it spans the globe: information flows as effortlessly from New York to Nairobi as from one building to another in Washington, D.C. Moreover, a communication from New York to Nairobi might travel through the United Kingdom and five other countries one day, but through France and five different countries the next. In this global context, it has been said, the U.S. Bill of Rights is a local ordinance, meaning that the U.S. constitutional guarantees (and the procedures of the U.S. wiretap laws) offer no privacy protection against foreign government interception of the communications of U.S. citizens that cross national borders.

As U.S. law enforcement agencies become more active abroad, and as they engage in more joint operations with foreign police organizations, the line blurs between intelligence agencies and law enforcement agencies. Greater attention will have to be paid to the rules governing electronic surveillance abroad. For both the Internet and traditional telephony, new rules need to be developed to govern U.S. surveillance abroad and the increasing extent of joint international operations, which currently take place in a legal no-man's-land. It has been held that the U.S. wiretap statutes have no extraterritorial application.[257] Congress should address this gap by extending the court order requirements of Title III and FISA to interceptions of communications by the U.S. government abroad for use in U.S. criminal cases.

---

[255] *Id.*

[256] S. Rep. No. 95-604 (1978).

[257] *See* United States v. Barona, 56 F.3d 1087 (9th Cir. 1995); United States v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987).

U.S. government agencies, particularly the FBI, have been promoting the adoption of CALEA-type standards on an international scale. In 1994, the "Barrett Commission" in Australia, crediting the FBI's leadership, supported the development of "international user requirements" as the most effective means of "international cooperation to ensure that law enforcement's needs are taken into account in the development of new technology."[258] In 1995, the Council of the European Union adopted a set of interception requirements for telecommunications systems, similar to the requirements developed by the FBI, and urged member states to implement the requirements with respect to systems and service providers in their own countries.[259] Efforts were also undertaken to urge non-EU countries to adopt the requirements. In 1997, the Telecommunications Standardization Sector of the International Telecommunication Union, upon a motion by Australia, adopted a resolution directing all its standards groups to consider the EU surveillance requirements in their standards development.[260]

If the U.S. government is promoting surveillance standards for systems abroad, it should be U.S. policy to also promote worldwide adoption of privacy protections at least as strong as those in the United States.

The U.S. government has been less successful in promoting international adoption of key recovery for encryption. Despite the Administration's best efforts, international bodies have not endorsed key escrow solutions.[261] The OECD Cryptography Policy Guidelines specifically do not endorse key escrow; rather, they cautiously propose that "national cryptography policies *may* allow lawful access to plaintext or cryptographic keys"[262] (emphasis added).

Nonetheless, as market-driven key escrow arrangements emerge, Fourth and Fifth Amendment concerns about what standards will govern access to keys take on international implica-

---

[258] P.J. BARRETT, REVIEW OF THE LONG TERM COST EFFECTIVENESS OF TELECOMMUNICATIONS INTERCEPTION (Mar. 1994).

[259] Council of European Union Resolution of 17 January 1995 on the Lawful Interception of Telecommunications, (96/C329/01).

[260] ITU, Document C97/58-E (May 9, 1997).

[261] John Markoff, *U.S. Fails to Win Global Accord on Police Internet Eavesdropping*, N.Y. TIMES, Mar. 27, 1997, at D1. *See* Jennifer L. Schenker, *EU Is Expected to Reject U.S. Proposal for Monitoring Internet Communications*, WALL ST. J., Oct. 8, 1997, at B9.

[262] Organization for Economic Cooperation and Development, *Recommendation of the Council Concerning Guidelines for Cryptography Policy* (Mar. 27, 1997).

tions, because governments will be seeking access to keys escrowed outside their territory. If commercial key escrow systems achieve acceptance in the United States, foreign governments are likely to seek access to escrowed keys and decryption assistance, raising the question of standards to be applied when a foreign government seeks cooperation of U.S. authorities. To regulate any assistance provided to foreign governments seeking access to escrowed keys or decryption assistance in the United States, and to prevent the disclosure of decryption keys or decryption assistance to foreign governments that do not respect privacy and other human rights or provide due process, Congress should adopt statutory rules that include strict court order standards. The rules for a foreign request should have to satisfy three basic criteria: 1) the foreign government should comply with the treaty and other standards normally governing the provision of U.S. legal assistance to that government; 2) the foreign request should have to meet a standard at least as high as U.S. law enforcement agencies; and 3) standards should be in place that prohibit the disclosure of keys or decryption assistance for political offenses or other activity that would be protected under the U.S. First Amendment, or to foreign governments that do not adhere to minimum standards of due process and privacy protection.

## X. Conclusion

Communications privacy is a bedrock constitutional principle, and electronic communications must be protected through strong privacy legislation implementing the Fourth Amendment's requirements. For the past quarter century, the law of this nation regarding electronic surveillance has sought to balance the interests of privacy and law enforcement. The uses of new technologies, however, are always outpacing the law, often in ways that threaten privacy, and also in ways that limit law enforcement's effectiveness. Other changes in technology offer the possibility of enhancing privacy. Still other changes increase surveillance capabilities. Consequently, Congress has been required periodically to examine the legal framework for protecting privacy while ensuring that law enforcement has the necessary and appropriate capabilities. It did so in 1968 when it responded to widespread eavesdropping by prohibiting wiretapping without a court

order.[263] It did so in 1986 with the adoption of ECPA, which extended the protections and authorities of Title III to e-mail and cellular telephone communications.[264] It did so again in 1994 when it responded to law enforcement concerns about the impact of new technologies by enacting CALEA, which required telecommunications carriers to ensure that their systems could accommodate government surveillance. I have argued here that it must do so again, to protect privacy.

As exemplified by the Internet, the digital communications technologies are flexible, decentralized, networked, open and interactive. They merge voice, data, and images. They eliminate distinctions between what is kept in the home and what is stored with third parties. They generate large quantities of easily captured transactional data, combine wireless and wireline systems seamlessly, and place choices and control in the hands of users. Their economics are characterized by competition and innovation. They are global in reach. The explosion in the amount of information transmitted and stored electronically and the emergence of a form of online existence for both businesses and individuals have produced a qualitative change in the nature of communications and, accordingly, in the amount and nature of the information that is exposed to intrusion, interception and misuse. A re-examination of the wiretap laws must take into account these defining features of the digital revolution.

Such a review should also consider the overall balance between the technical and legal capabilities of government and the technical and legal status of privacy protections. Piecemeal amendments to the surveillance laws in response only to government concerns will inappropriately upset the balance. Any amendments to the wiretap laws must be narrowly crafted to ensure that they do not erode privacy protections, and must be balanced by other, privacy-enhancing amendments. New technologies enhance the ability of law enforcement to intercept and analyze communications and track individuals. Many of these enhancements are coming about without government intervention, as the unintended consequences of market-driven changes in technology. Existing law allows law enforcement to take advantage of these developments. As technology enhances surveillance capabilities,

---

[263] Omnibus Crime Control and Safe Streets Act of 1968, tit. III, Pub. L. No. 90-351, 82 Stat. 212 (codified at 18 U.S.C. § 2510 *et. seq.*).

[264] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in sections of 18 U.S.C. §§ 2510-21, 2701-10, 3121-26).

the legal standards for government use of these new technologies must be increased to adequately protect privacy. I have recommended here a number of amendments that respond to technological changes to protect against abuse without curtailing legitimate law enforcement access.

Government efforts to control the development of technology to preserve its communications surveillance capability must be carefully circumscribed. Merely as a practical matter, the rapid and decentralized changes occurring in technology are likely to outstrip government efforts at control. The most notable case in point is encryption: there seems to be no way to limit the spread of virtually unbreakable encryption. Changes in technology since 1994 when Congress adopted the CALEA legislation pose equally difficult problems, while also creating opportunities for enhancing privacy. Congress and the FCC should restrain FBI efforts to use this legislation to obtain surveillance capacities that go beyond the status quo.

The legislature must continually strive to develop rules that keep pace with technological developments. The process never reaches a point of final repose, but there are clear steps that should be taken now to reestablish the balance between privacy and government surveillance powers.