ECPA and Online Computer Privacy

Ruel Torres Hernandez*

CONTENTS

INTRODUCTION

During the ninety-ninth term of Congress, legislation was introduced which sought to provide federal statutory guidelines to protect the privacy of electronic communications, including electronic mail (e-mail), found on commercial computer-based services and on other remote computer systems. Ultimately, this legislation was enacted as the Electronic Communications Privacy Act of 1986 (ECPA). Before enactment of ECPA, federal law did not provide any guidelines for protecting technologically advanced forms of communication. Case law also failed to pro-

* B.A. University of California at San Diego, 1984; M.A. San Diego State University, 1987; J.D. California Western School of Law, 1988.

vide adequate guidance in this area. The peculiarities of computers and computer storage were not addressed by previous wiretap laws. Moreover, electronic communications were not protected by the constitutional right to privacy as defined by the United States Supreme Court. In sum, existing law was "hopelessly out of date."[1]

When the old wiretap laws were first enacted, the possibility that computer-based electronic communications systems would be used to transmit messages across telephone lines had not been contemplated. Fortunately, with ECPA, e-mail and other private electronic communications are given federal statutory privacy protection. In particular, ECPA provides both criminal procedure guidelines and rules for obtaining civil remedies.

This discussion of ECPA and related areas is prompted by one of the first civil lawsuits which relies upon ECPA as a basis for some of its claims.[2] The lawsuit, *Thompson v. Predaina*, was filed in March of 1988 in the district court for the Southern District of Indiana.[3] While *Thompson* later was voluntarily dismissed by the plaintiff, it is an example of a fact situation which raises privacy concerns covered by ECPA. The facts of the case were as follows: Linda Thompson, a third-year law student, filed a *pro se* complaint against Bob Predaina, the systems operator (sysop) of the Professional's Choice Bulletin Board, a fee-based "hobbyist" electronic bulletin board system. The suit alleged that Predaina intruded, without any right or privilege, into Thompson's private e-mail. Thompson based her action on federal theories, including two under ECPA, as well as on common-law state claims. In this author's opinion, the *Thompson* case would have been an excellent ECPA test case. An opportunity to see how ECPA will operate to protect, or not protect, one's privacy in the electronic communications context has not yet arisen.

This Article will discuss the following issues: (1) the com-

1. S. REP. NO. 541, 99th Cong., 2d Sess. 2, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3556 (quoting 132 CONG. REC. S7992 (daily ed. June 19, 1986) (statement of Sen. Leahy)).

2. The one published decision in which the privacy protections of ECPA are involved is Michigan Bell v. Drug Enforcement Admin., 693 F. Supp. 542 (E.D. Mich. 1988). This case involves telephone toll records, however, not user-generated communications as in *Thompson*.

3. Thompson v. Predaina, No. 88-93C (S.D. Ind. *dismissed* Aug. 10, 1988).

puter communications environment; (2) an example of the pre-ECPA criminal situation; (3) the law prior to the passage of ECPA; (4) a preliminary discussion of ECPA with emphasis on its criminal procedure aspects; (5) ECPA as applied in the civil context to the *Thompson* situation; and (6) ECPA as applied in the civil context to the corporate situation.

I. THE COMPUTER COMMUNICATIONS ENVIRONMENT

The computer communications environment can be divided into three parts: (1) commercial systems and networks; (2) hobbyist systems and networks; and (3) corporate systems and networks.

The commercial systems and networks electronically provide private e-mail, public discussion conferences, real-time "chat" facilities, public domain software exchange, and access to news and various databases. Included within this category are the popular consumer computer online services of CompuServe, GEnie, the Source, BIX, the WELL, Portal, QuantumLink, AppleLink, and Prodigy. Also included in the commercial catagory are the more specialized computer databases such as LEXIS, WESTLAW, DIALOG, and the Dow Jones News Retrieval, in which some limited private e-mail and private user area facilities may be provided. Commercial data communications networks, such as Telenet and Tymnet, comprise a third component of this commercial category. In his report on the telephone industry, Peter Huber writes that there are "[h]undreds, perhaps thousands of [commercial] information service providers . . . offering immediate access to vast amounts of electronically stored information in an extremely broad range of fields."[4] Indeed, he notes, "[t]he industry has grown explosively since 1979."[5]

Hobbyist systems and networks include electronic bulletin boards (BBS's) and the various cooperative networks. The ECPA Senate Report contains one definition of electronic bulletin boards:

> Electronic "bulletin boards" are communications networks created by computer users for the transfer of information among computers.

---

4. P. HUBER, THE GEODESIC NETWORK: 1987 REPORT ON COMPETITION IN THE TELEPHONE INDUSTRY 7.1 (1987).

5. *Id.*

> These may take the form of proprietary systems or they may be noncommercial systems operating among computer users who share special interests. These noncommercial systems may [or may not] involve fees covering operating costs and may require special "passwords" which restrict entry to the system. These bulletin boards may be public or semi-public in nature, depending on the degree of privacy sought by users, operators or organizers of such systems.[6]

Users of hobbyist systems are generally "recreational" computer users who use computers and modem communications as a hobby.[7] Such users are akin to amateur ham radio and citizen band radio operators. In these hobbyist networks, BBS's are provided and maintained by computer hobbyists out of their own personal resources. These individuals, who typically provide the BBS on their own stand-alone personal computer, are specifically known as sysops (systems operators). While access to some BBS's may be free, some sysops require the payment of use fees. For instance, some sysops ask that users pay a charge for the system's phone line. In addition to providing public domain software and "shareware" exchange, these systems generally provide free public and private e-mail exchanges to computer/modem-equipped members of local communities.[8] Some sophisticated systems, such as the ProLine system written for Apple II computers, also provide users with personal user directory areas. Such systems allow users to maintain personal

---

6. S. REP. NO. 541, 99th Cong., 2d Sess. 8-9, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3562-63. Congress may have made a poor choice of words by broadly describing BBS's as "communications networks." Individual BBS's may not be affiliated with an outside network system. They may merely take the form of individual stand-alone computers set up to take incoming modem telephone calls from users. However, by using the term "network," Congress may merely have been trying to indicate its knowledge that users can "network" together when calling a single BBS.

7. *See* S. Dick, Towards a Rational Private Policy For Recreational Telecomputing (Sept. 1, 1988) (unpublished Michigan State University Mass Media Ph.D. Program paper).

8. In the legal sense, public domain software is computer software in which its author does not claim a copyright. However, in the common jargon of computer users, "public domain" also means a free form of distribution of software which may or may not be copyrighted. For instance, some software copyright owners may retain a copyright to the software, but give free licenses to interested users to copy and distribute copies of the software. "Shareware" is the term used to denote the distribution of computer software according to a unique marketing concept: a user may freely download the software from the host BBS computer to his personal computer, try out the software, and if he likes the software or continues to use it, must pay a registration fee to the software author or publisher.

files in their own directory, a feature similar to the CompuServe personal file areas.[9]

Augmenting the single stand-alone BBS's are the various cooperative and research networks that link network-affiliated BBS's or other online systems or services. This networking is often conducted with the assistance of business, government, and university mainframe computers through the use of sophisticated routing networks. Examples of such networks include ARPA, Internet, UUCP, USENET, BITNET, FIDO, OPUS, and ProLine. These networks utilize computer automation and sophisticated message-addressing instructions to link computers via common carrier telephone lines. Through such systems, users of different systems may exchange private e-mail. Moreover, these systems allow publicly "posted" messages to be exchanged in national, and often worldwide, conference discussions. Given the proper address-routing instructions, a user may communicate with another user on a crosstown BBS or on a BBS in another part of the country. For instance, in networks like FIDO and OPUS, messages may be echoed in echo conferences along the network.[10] Although the use of routing networks involved in echoing creates some delay, such networks help reduce or eliminate a computer hobbyist's need to make direct toll or long distance telephone calls to faraway systems and his having to pay subscription fees for the use of a commercial online communications service.

---

9. A CompuServe user has his own personal file area where he may privately keep his own personal electronic files. *See* COMPUSERVE INFORMATION SERVICE USERS GUIDE 4-25 to 4-27 (1985). This feature is very useful for people who travel or who are constantly away from their regular computer systems. For instance, a reporter, writer, or businessperson away from home can simply connect with CompuServe through his laptop computer and upload an electronic document or file to his personal file area on CompuServe. Upon return home, he may simply download the document or file for more permanent storage on his regular computer system. Users of the ProLine system now have an identical capability through use of that system's personal directory areas.

10. "Echoing" is a process by which message traffic contained in an echo conference is automatically uploaded to other BBS's which are linked via an "echo mail" program. This feature allows users to call different systems, while still participating in the same echo conference. Depending on the toggles or flags set on particular messages, the echoed messages may be seen publicly along the network or only by a particular user. This is just one of the many different message distribution processes available. For a discussion of other distribution processes, see Quarterman & Hoskins, *Notable Computer Networks*, 29 COMM. OF THE ACM 932 (1986).

Corporate systems and networks, unlike hobbyist systems, may provide complete private networks, private-line service between two points with no connection to the public telephone network, and private branch exchanges handling computer calls within an organization. These systems may be privately-owned or leased facilities dedicated to the exclusive use of a company. "They may range from point-to-point telephone lines to nationwide switched voice and data systems. . . . Stations connected to the network may call one another without using public toll facilities."[11]

According to Huber,

> Private networks are used primarily by business and governmental customers whose telecommunications expenditures are $10 million or more annually. A private network consists of transmission facilities, nodal switches, and other customer premises equipment configured for the exclusive use of a single, geographically dispersed organization. The transmission facilities used in the network may, however, be provided largely or entirely by public (i.e. common) carriers, both local and interexchange. Many private networks rival public networks in their geographic scope and in the number of telephones they serve.[12]

Large corporations like AT&T, DEC, IBM, and Xerox have implemented internal computer communications networks in support of their business operations.[13] "Many of these are just LAN [Local Area Networks] within particular buildings, although some are international or even intercontinental in scope. The administration and funding of such networks usually come from a single company and their users are mostly employees of that company."[14]

On a smaller scale, many businesses have also been turning to the use of computer BBS-type systems and BBS-type networking in order to increase productivity, reduce paperwork, improve client contact, and eliminate "telephone tag."[15] In

---

11. W. BLYTH & M. BLYTH, TELECOMMUNICATIONS: CONCEPTS, DEVELOPMENT, AND MANAGEMENT 89 (1985).

12. P. HUBER, *supra* note 3, at 3.45.

13. Quarterman & Hoskins, *supra* note 9, at 933.

14. *Id.*

15. Keaveney, *Custom-Built Bulletin Boards*, PERS. COMPUTING, Aug. 1987, at 91. "Telephone tag" is a common office occurrence where a busy person in one office cannot reach another person in a different office by telephone. The original caller leaves a message asking that the other person call him back. When the other person returns the call, she may not be able to reach the original caller and she too leaves a

some cases, such computer communications systems may also be networked with corporate or cooperative networks.

In addition to the three system categories of commercial, hobbyist, and corporate networks, another facet of the computer communications environment is the use of gateways. Gateways consist of either network routing addresses or specific services that connect separate hobbyist networks with commercial and corporate systems and networks. In many cases, this computer interconnectivity allows the sending of e-mail across "network boundaries."[16] On commercial systems, gateways typically allow a subscriber to cross over from the host system to another commercial system's database without breaking the login connection to call the other system directly. "Together, these networks form a *metanetwork* (sometimes called Worldnet) that is used daily by many communities of interest throughout the world."[17]

The pervasive use of computers for information transmission underscores the need for privacy. However, the complexity of the software, the networking schemes, and the actual use of computer communications means that any privacy protection must be both comprehensive and flexible. Privacy protection for computer communications must be comprehensive enough to cover the different types of computer communications, whether while in transmission, or while stored and waiting for retrieval by an intended recipient. The protection must also be flexible

---

call-back message. An electronic mail system can eliminate this round robin. A voice mail system, as is being used in some companies, can also eliminate the problem. *See TE&M Special Report Electronic/Voice Mail*, TELEPHONE ENGINEER & MGMT, Sept. 1, 1987, at 57-81.

16. Quarterman & Hoskins, *supra* note 9, at 941. Each network is self-contained. Fortunately, there are ways to interconnect different networks, *i.e.*, to cross a "network boundary" from one network to another. For example, in the case of electronic mail, one can send e-mail from from an ARPA Internet affiliated node to a mailbox on the MCI Mail service and *vice versa* using specific address routing instructions. *See* A. DeSchon & J. Postel, Mail Forwarding Between MCI-Mail and ARPA-Mail Using Intermail (Oct. 1985) (electronic document). Likewise, a CompuServe user can send e-mail to and receive e-mail from an MCI Mail user. *See* CompuServe Online Instructions (GO QAMCI) (electronic online instructions). However, some boundaries may not be crossed. For instance, one will find that although e-mail may be sent from a CompuServe mailbox to MCI Mail and then on to a mailbox on an ARPA Internet node, e-mail from an ARPA Internet node cannot be sent through MCI Mail to CompuServe unless there is special government or industry clearance.

17. Quarterman & Hoskins, *supra* note 9, at 932 (emphasis in original).

enough to account for the practical aspects of maintaining and operating a computer communications system or network.

II. INITIAL CRIMINAL PROCEDURE CONFLICT

As the use of computer communications increases, law enforcement officials will more frequently seek criminal evidence stored as private e-mail or other data on commercial computer services and hobbyist BBS's. For example, suppose that a computer user calls up a computer communication system. Then, by using the e-mail function, he leaves a private message that can only be read by a particular intended recipient. The message is to inform the recipient of a conspiracy plan that would violate a federal or state criminal statute. Law enforcement obtains a tip about the criminal activity and learns that incriminating evidence may be found on the computer system. What privacy protection should be afforded the incriminating e-mail?

In 1982, such a situation actually occurred. A Detroit federal grand jury, investigating a million-dollar cocaine ring, issued a subpoena ordering a commercial service, the Source, to hand over a private user's data files.[18] The files were easily obtainable as they were routinely backed up by the sysop to guard against system crashes. The grand jury sought evidence to show that the cocaine ring had been using the Source as a communications base with which to send messages to members of the ring. Presumably, with such evidence the grand jury could have indicted those suspected of participating in the cocaine ring. The Source refused to obey the subpoena, citing the right to privacy of the users. The prosecution, though, argued that since the files containing messages had already been duplicated by the service, the user's expectation of privacy had been extinguished.[19] A court battle ensued. However, before a ruling could be made, the kingpin of the cocaine ring entered a surprise preemptive guilty plea to federal drug trafficking charges and the case

18. Meeks, *Life at 300 Baud: Crime on the BBS Network*, PROFILES, Aug. 1986, at 12, 12-13.

19. Another prosecution argument, although not reported by Meeks, would be that the Source could not vicariously assert a user's privacy rights. According to the Supreme Court, fourth amendment rights are personal and can only be asserted by the person whose rights are invaded. Rakas v. Illinois, 439 U.S. 128, 133 (1978) (petitioners lacked standing to object to prosecution evidence of a rifle and shells seized by police during a search of an automobile in which petitioners were merely passengers).

against the Source was discontinued.[20]

Publicly posted messages and other public material found on an online system or service may be retrieved easily by law enforcement. For example, a police officer could use a modem-equipped computer to call into a local BBS or an online service and read publicly posted messages on the system. There is, after all, no privacy interest in admittedly public material. It is the private material, such as e-mail, which requires protection if it is to remain private. In the above police enforcement example, the police would want the private e-mail, or other private files, transmitted between suspected criminals on a particular online system. Both the system provider and the user, however, have an interest in privacy which conflicts with this objective. The service provider of the computer communications system has assumed a role as keeper of transmitted private electronic messages, and generally does not want to turn over private data. Such actions might very well cause users to lose confidence in his system. Needless to say, the user also wishes to avoid invasions of his private electronic communications. Unfortunately, pre-ECPA privacy law did not provide much protection for either party.

III. Inadequacy of Old Law

Before ECPA, no adequate privacy protection for electronic communications existed. Previously, it was widely believed that "[a]ny law enforcement authority . . . [could] . . . for example, confiscate a local BBS and examine all the message traffic," including private e-mail and other private files, contained thereon.[21]

A. Pre-ECPA Case Law

Very few pre-ECPA cases concern computer communications and fourth amendment constitutional problems. Most of the available cases arose with regard to disputes over the financial information found in bank and consumer credit database computers. In *United States v. Davey*,[22] the court ruled that the

20. Meeks, *supra* note 17, at 13.
21. *Id.*
22. United States v. Davey, 426 F.2d 842 (2d Cir. 1970) (IRS-issued summons

federal government could require the production of relevant evidence regardless of where it was stored.[23] The form in which the information was kept and the manner in which it could be retrieved were held to be irrelevant, as long as the government paid the reasonable costs of retrieval.[24]

In a California case, *Burrows v. Superior Court*,[25] a depositor was found to have a reasonable expectation that a bank would maintain the confidentiality of both papers in check form originating from the depositor and the depositor's bank statements and records of those checks.[26] Notably, however, in *United States v. Miller*,[27] the Supreme Court held that customer account records maintained on a bank's computer were not the private papers of the bank customer.[28] Thus, there was no fourth amendment privacy protection for the records and they could be subpoenaed directly from the bank.[29]

While these three cases concern business and financial information, in contrast to the personal nature of e-mail found on computer systems such as CompuServe and hobbyist BBS's, it is reasonable to assume that there would be little to legally prohibit police from gaining access to a user's private records as well as his business records. For example, although under *Burrows* a user may have a reasonable belief that an online system would maintain the confidentiality of his private e-mail stored on the system, such material may be held not to be the private papers of the user under *Miller*. A fourth amendment privacy problem thus would not exist under the law.

Additionally, a prosecutor would be able to take advantage of the fact that the provider or systems operator routinely duplicates files for purposes of providing a back-up system. The user has no reasonable control of the duplicates under existing law.

---

requiring a consumer credit corporation to produce certain credit reports of named individuals held valid).

23. *Id.* at 844-45.

24. *Id.*

25. Burrows v. Superior Court, 13 Cal. 3d 238, 529 P.2d 590, 118 Cal. Rptr. 166 (1974) (police detective illegally obtained photostatic copies of an attorney's bank statements from attorney's bank).

26. *Id.* at 243, 529 P.2d at 593, 118 Cal. Rptr. at 169.

27. United States v. Miller, 425 U.S. 435 (1976).

28. *Id.* at 441-43.

29. *Id.*

Unfortunately, the duplication and backup of computer data is a necessary safety precaution in case of power failure or magnetic destruction. All computer users know of this common practice.[30] Yet many users believe that the duplicated data is simply stored and remains inaccessible for examination by others. The user's subjective belief that his duplicated e-mail is private may arguably be seen as an objectively reasonable belief, thereby creating a constitutionally protected expectation of privacy under the fourth amendment.[31]

However, despite these expectations of privacy, under pre-ECPA law the user himself was responsible for protecting his personal e-mail from privacy intrusions. User attempts at protection are almost always defeated, however, as the provider or operator of the service has ultimate control over the stored material. The provider may easily examine all material on the system. Thus, a legal knothole exists, through which an observer may lawfully observe all the user's stored material, effectively excluding any reasonable expectation of privacy.[32] The Justice Department itself noted this in a response to Senator Leahy's questions over whether the pre-ECPA wiretap law was adequate to cover computer communications. As one Justice Department official noted, it was "not always clear or obvious" whether a reasonable expectation of privacy existed.[33] Importantly, if there is no expectation of privacy there is no search, so the fourth amendment is not violated.

B. Old Federal Wiretap Statutes

Although e-mail might appear to come under the old Title 18, section 2510(1) definition of the term "wire communica-

30. The common refrain among computer users, computer manufacturers, and software publishers is "back up your data." Otherwise, a user may suffer an irretrievable loss of information or software. The magnetic media, *e.g.*, diskette, hard drive, or ramdisk, may encounter many problems, such as power surges, which cause data to be lost.

31. For there to be a constitutionally protected expectation of privacy under the fourth amendment, a person's subjective privacy expectation must be seen as objectively reasonable. Katz v. United States, 389 U.S. 347, 360-62 (1967) (Harlan, J., concurring).

32. California v. Ciraolo, 476 U.S. 207, 219 (1986) ("[I]f there is an opening, the police may look.").

33. S. REP. NO. 541, 99th Cong., 2d Sess. 4, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3558.

tion," the term in that statute was limited to audio transmissions by wire or cable.[34] The prior section 2510(4), which applied to unlawful interception of "any wire or oral" communications, required that there be a human voice involved in the transmission which could be heard as in normal non-telephonic voice conversations.[35] A question thus arose as to whether an electronic communication could be intelligibly heard by the human ear. Data transmissions over telephone lines generally sound like unintelligible noisy static or high pitched tones.[36] This fact contributed to uncertainty over whether e-mail and other forms of electronic communications were protected by the old statutes.

Importantly, the old statutes also failed to provide for protection of a communication after completion of its transmission and subsequent storage on a computer. Only communications in transmission were protected.[37] This is understandable in that "[e]ighteen years ago . . . Congress could not appreciate—or in some cases even contemplate—[today's] telecommunications and computer technology."[38] Moreover, courts uniformly rejected attempts to read computer communications protection into the old federal wiretap statute or into existing state laws. This reluctance can be attributed to the judiciary's belief that the legislatures should define the boundaries in such a novel area. Congress itself recognized that the courts were "in no hurry to [update the law] and [that] some judges [were] openly asking Congress for help. . . . [F]ederal Appeals Court Judge Richard Posner in Chicago said Congress needed to revise current law, adding that 'judges are not authorized to amend statutes even to bring them up-to-date.' "[39] Thus, the stage was set for legisla-

34. 18 U.S.C. § 2510(1) (1982).

35. 18 U.S.C. § 2510(4) (1982).

36. Modem communications involves a process whereby the digital signals of a computer are converted into analog signals which can be transmitted over telephone lines. Once the signals are received at another computer, the signals are converted back into digital signals easily understood by the other computer. This modulation and demodulation process requires the use of a modem device as the interface between the computer and the telephone network. While the signals are on the telephone line, they sound like unintelligible static or high-pitched tones to the human ear. Only a computer equipped with a modem can understand the signals. *See* W. BLYTH & M. BLYTH, *supra* note 10, at 70, 306.

37. 18 U.S.C. §§ 2510, 2511 (1982).

38. 132 CONG. REC. S7992 (daily ed. June 19, 1986) (statement of Sen. Leahy).

39. Cohodas, *Congress Races to Stay Ahead of Technology*, 44 CONG. Q. WEEKLY REP. 1233, 1233 (1986).

tive action in the area.

IV. ECPA — THE NEW LAW

On October 21, 1986, President Reagan signed the Electronic Communications Privacy Act of 1986 into law, thereby amending the federal wiretap law. ECPA created privacy protection against both interception of electronic communications while in transmission and unauthorized intrusion into electronic communications stored on a system.

ECPA provides privacy protection for electronic communications made by "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[40] Thus protection for electronic communications is defined in terms of what is transmitted and how it is transmitted.[41] The primary requirement is that the means of transmission must affect interstate or foreign commerce.[42] Under ECPA, all telephonic means of communication that "cannot fairly be characterized as containing the human voice" should be protected.[43] The Senate report noted examples of protected electronic communications as including non-voice communications such as "electronic mail, digitized transmissions, and video teleconferences."[44] Both interception and disclosure of such electronic communications are prohibited.[45]

ECPA also protects electronic communications stored after transmission, such as e-mail left on an electronic computer communication system for later retrieval by its intended recipient. It is now a federal offense to break into any electronic system holding electronic communications. It is also illegal for anyone to exceed authorized access to a system and alter or obtain

40. 18 U.S.C. § 2510(12) (Supp. IV 1986); *see also* 18 U.S.C. § 2511 (Supp. IV 1986).

41. *See* 18 U.S.C. § 2510(12)(B) (Supp. IV 1986).

42. 18 U.S.C. § 2510(12) (Supp. IV 1986).

43. S. REP. No. 541, 99th Cong., 2d Sess. 14, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3568.

44. *Id.*

45. 18 U.S.C. § 2511(1) (1982 & Supp. IV 1986). ECPA coverage in the corporate context, however, may be limited to "cracker" and unauthorized employee situations. *See infra* Section VI.

stored communications, or to subsequently disclose the contents of the electronic communications of others.[46]

In addition, ECPA specifically prevents law enforcement invasion of user e-mail without a court order.[47] The burden of preventing disclosure of e-mail is placed upon the subscriber or user of the system. However, the government must give the subscriber or user fourteen days notice before conducting a search. This time period should be sufficient to allow a user to file a motion to quash a subpoena or a motion to vacate a court order seeking disclosure of his computer material.[48] This requirement is not comprehensive, however, as the government may give delayed notice when exigent circumstances exist, or no notice at all when the exigent circumstances are extreme.[49]

ECPA also allows the government to include in its subpoena or court order a requirement that the provider or operator of the system retain a backup copy of electronic communications when there is a risk of destruction.[50] However, in instances where the material sought is unusually voluminous or burdensome to supply, the system provider may be reimbursed for the extra effort required to obtain the communications or for any disruptions in its business.[51]

A. Systems Covered

ECPA covers both electronic communication services and remote computing services. Under ECPA, " 'electronic communication service' means *any* service which provides to users thereof the ability to send or receive wire or electronic communications."[52] A "remote computing service" is defined in the Act as an electronic communications system that provides computer storage or processing services to the public.[53] With regard to

46. 18 U.S.C. §§ 2701(a), 2702(a) (Supp. IV 1986).
47. 18 U.S.C. §§ 2516, 2517, 2518, 2703 (1982 & Supp. IV 1986).
48. 18 U.S.C. § 2704(b) (Supp. IV 1986).
49. The Act lists the following exigent circumstances: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction or tampering with evidence; (4) intimidation of a potential witness; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial. 18 U.S.C. § 2705(a)(2) (Supp. IV 1986).
50. 18 U.S.C. § 2704(a) (Supp. IV 1986).
51. 18 U.S.C. § 2706 (Supp. IV 1986).
52. 18 U.S.C. § 2510(15) (Supp. IV 1986) (emphasis added).
53. 18 U.S.C. § 2710(2) (Supp. IV 1986).

stored communications, the "remote computing service" definition also sets public online systems and services apart from wholly private corporate systems, which may have more limited protection.[54] Importantly, ECPA also covers any "person or entity providing the wire or electronic communication service."[55] Such broad language indicates the inclusion of individuals and businesses who provide commercial, hobbyist, and corporate systems and networks.

ECPA takes note of the different levels of security found on commercial and hobbyist systems. The Act discriminates between systems upon the basis of whether the system is configured to contain private e-mail or public material.[56] Electronic communications which a user seeks to keep private through configurations provided by the system are protected by ECPA.[57] However, there is no liability for unauthorized access to files configured by the system to be readily accessible by the general public.[58] An indication of privacy on the system, such as a password or prompt asking if a message is to be kept private, triggers ECPA coverage unless the user has been notified to the contrary.[59]

B. Escaping Coverage

There are at least two possible ways to escape coverage

---

54. Again, in the context of corporate online communications systems, ECPA coverage may be limited to situations involving "cracker" intrusions and unauthorized employee access. *See infra* Section VI.

55. 18 U.S.C. § 2702(a)(1) (Supp. IV 1986).

56. 18 U.S.C. § 2511(2)(g)(i) (Supp. IV 1986); S. REP. NO. 541, 99th Cong., 2d Sess. 18, 36, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3572, 3790.

57. 18 U.S.C. §§ 2511(1), 2701(a), 2702(a) (Supp. IV 1986).

58. 18 U.S.C. § 2511(2)(g)(i) (Supp. IV 1986).

59. *See* Wiley & Leibowitz, *Electronic Privacy Act Is Progress—But It Still Is Not a Panacea*, NAT'L L.J., Jan. 12, 1987, at 20.

> Restrictions on access to stored communications, however, are not intended to apply to electronic bulletin boards and similar services readily available to the general public. One seeking access may imply authorization where the means of access are widely known and there are no "warnings, encryptions, password requests, or other indicia of intended privacy" encountered.

Id. (quoting H.R.REP. 647, 99th Cong. 2d Sess. 62 (1986)). *See also* S. REP. NO. 541, 99th Cong., 2d Sess. 36, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3590. However, if a BBS has an indicia of privacy, such as passwords or segregation of private and public messages, then ECPA may apply. Most online systems, whether commercial or hobbyist, have password login procedures, user registration or validation processes, or private e-mail facilities.

under ECPA. First, the sysop may simply fail to provide any means of private communications, *e.g.*, no private e-mail. Second, the sysop may provide adequate notice that *all* material on a system is to be publicly accessible by all users even though methods of providing privacy appear to remain on the system. The bulletin board system maintained by DePaul University College of Law provides an example of an electronic notice which is displayed upon user access:

> PURSUANT TO THE ELECTRONIC AND [sic] COMMUNICATIONS PRIVACY ACT OF 1986, 18 USC 2510 et. seq., NOTICE IS HEREBY GIVEN THAT THERE ARE NO FACILITIES PROVIDED BY THIS SYSTEM FOR SENDING OR RECEIVING PRIVATE OR CONFIDENTIAL ELECTRONIC COMMUNICATIONS. ALL MESSAGES SHALL BE DEEMED TO BE READILY ACCESSIBLE TO THE GENERAL PUBLIC.
>
> Do NOT use this system for any communication for which the sender intends only the sender and the intended recipient or recipients to read.

Although the DePaul notice states otherwise, user-operated message privacy toggles remained on the board when this disclaimer first appeared. Before ECPA, similar disclaimers were used on hobbyist BBS's. Sysops often warned users that their systems were not secure from "crackers,"[60] advising users to go elsewhere if they wished to maintain privacy. Even today, a warning such as that on the DePaul system may be adequate to exempt the system from ECPA coverage.[61] However, the existence of privacy toggles does lead to a sense of security on the part of the user.

One traditional way of prohibiting access to duplicate copies of private electronic communications is by encrypting private e-mail with a password. However, the system's encryption technique must be one that no one, not even the provider, knows how to decipher.[62] Thus, while law enforcement would be able

60. Unfortunately, journalists have confused the terms "hacker" and "cracker." Hackers are computer users who happen to be very good at computer programming. Crackers, on the other hand, are individuals who criminally attempt to "crack" into computer networks for illegal access. *See* S. LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION (1984).

61. *See supra* note 53. If there are no privacy toggles, the warning certainly would be adequate.

62. There is a commercial consumer service that finds itself in this situation.

to acquire backup copies of private messages, the encryption scheme would foil efforts to read such protected messages.

V. ECPA AND *THOMPSON V. PREDAINA*

In her civil complaint against Predaina, Thompson alleged 10 separate counts and asked for $112,250 in damages.[63] According to the complaint, Thompson was exchanging private e-mail via an "echo" intermail networked conference on Predaina's BBS system. After reading the messages she received, she routinely deleted them.[64] Predaina, however, allegedly restored the private e-mail and caused the e-mail to become public.[65] The e-mail was also allegedly echoed publicly on other BBS's along the network. Thompson's complaint also contains a state claim of libel, alleging that Predaina then made false remarks concerning her reputation, which caused Thompson emotional distress.[66] Such remarks presumably were circulated on the Predaina BBS and elsewhere along the network. In BBS slang, such conduct would be the most extreme form of "flame" (as in inflaming one's emotions).[67]

"Not even [their] 'god' number could ever read the [passworded] mail." Hernandez, *Computer Electronic Mail and Privacy*, 3 COMPUTER L. & SEC. REP. 4, 8 (1987).

63. Complaint, Thompson v. Predaina, No. 88-93C (S.D. Ind. *dismissed* Aug. 10, 1988) [hereinafter Complaint].

64. *Id.*

65. Some BBS software programs do not completely remove a message from the system when the user "deletes" or "erases" it. Although the message may no longer be in a user's queue to read, the message may still be in the message base until completely purged from the system by the sysop. Until then, depending on the software, the sysop may be able to "undelete," "unerase" or "restore" the message for anyone to read. Depending on what toggles the sysop activates, the restored message may become public or private. Unlike a mere user who has only a limited number of privileges on the BBS, a sysop has the greater ability to manipulate his system in almost any way he chooses. Of course, the ability of the sysop to engage in such manipulation depends upon the software that he is using.

66. Complaint, *supra* note 63.

67. News of the *Thompson* case has heightened the liability awareness of sysops around the nation. Articles for online electronic publications have been distributed about the case, and discussions about the case have been held on various commercial and hobbyist online services and systems. In May of 1988, a live conference was held at the John Marshall Law School Center for Information Technology and Privacy Law to discuss the problem. Shortly after news of the *Thompson* case became known, but perhaps more in response to the general problem situation, a book discussing privacy, copyright, state criminal laws, and other BBS legal issues was published by two New York attorneys who also happen to be veteran sysops. *See* J. WALLACE & R. MORRISON, SYSLAW: THE SYSOP'S LEGAL MANUAL (1988).

Thompson essentially brought three separate federal claims. Two are under ECPA and a third is under the Cable Communications Policy Act of 1984, which covers encrypted satellite cable broadcasts.[68]

A. Federal Civil Claims

Thompson's first claim arose under Title I of ECPA ("Wire and Electronic Communications Interception and Interception of Oral Communications"). Under Title I, "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate."[69] The classic example of a violation under this section occurs when someone intercepts a private communication while in transmission and divulges its contents to someone other than the intended recipient (or his agent).[70]

The civil relief provided under the statute may include

(1) equitable or declaratory relief;
(2) actual damages;
(3) punitive damages; and
(4) reasonable attorney's fees and litigation costs.[71]

There are, however, a number of defenses that can be asserted in a Title I action. Statutory defenses to such a violation include good faith reliance on any of the following:

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (even if it turns out to be invalid);
(2) a request by an investigative or law enforcement officer in emergency situations such as:
    (i) immediate danger of death or serious bodily injury to any person,
    (ii) conspiratorial activities threatening national security, or
    (iii) conspiratorial activities characteristic of organized crime;

68. Cable Communications Policy Act of 1984 § 5(b), 47 U.S.C. § 605 (Supp. III 1985). The original section 605 of the Communications Act of 1934 was previously replaced with a substitute section 605 under the Omnibus Crime Control and Safe Streets Act of 1968. S. REP. NO. 1097, 90th Cong., 2d Sess. 84-85, *reprinted in* 1968 U.S. CODE CONG. & ADMIN. NEWS 2112, 2196-97.

69. 18 U.S.C. § 2520(a) (Supp. IV 1986).

70. 18 U.S.C. §§ 2520(a), 2511 (Supp. IV 1986).

71. 18 U.S.C. § 2520(b) (Supp. IV 1986).

(3) a good faith determination that ECPA allowed the intrusion.[72]

Clearly, a great deal of latitude is allowed in these defenses once a court has found the existence of good faith on the part of the alleged violator.

Thompson's second federal cause of action arose under Title II of ECPA ("Stored Wire and Electronic Communications and Transactional Records Access"). Title II of the Act states that

> [a]ny provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.[73]

A violation of this section occurs whenever someone intentionally accesses private communications that are stored on a system or forwarded along a network. It is also a violation of this section to knowingly divulge the contents of such communications to someone other than the intended recipient or another statutorily authorized person.[74] A plaintiff may seek the same types of relief as those provided under Title I.[75] In addition, a plaintiff under this section may also seek any profits made by the wrongdoer as the result of his unlawful access to the private communications. Profits made are to include any financial advantage the wrongdoer obtained as a result of access to the private communications, provided that he would not have received the profits otherwise and that the damages are at least one thousand dollars.[76]

Thompson's final federal claim arose under Title VII of the Cable Communications Policy Act of 1984, which concerns the unauthorized publication or use of communications. This statute provides that

> no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception,

---

72. 18 U.S.C. § 2520(d) (Supp. IV 1986).
73. 18 U.S.C. § 2707(a) (Supp. IV 1986).
74. 18 U.S.C. §§ 2707(a), 2701(a), 2702(a) (Supp. IV 1986).
75. 18 U.S.C. § 2707(b) (Supp. IV 1986).
76. 18 U.S.C. § 2707(c) (Supp. IV 1986).

> (1) to any person other than the addressee, his agent or attorney,
> (2) to a person employed or authorized to forward such communication to its destination,
> (3) to proper accounting or distributing officers of the various communication centers over which the communication may be passed,
> (4) the master of a ship under whom he is serving,
> (5) in response to a subpoena issued by a court of competent jurisdiction,
> (6) on demand of other lawful authority.[77]

This section focuses on the individuals charged with handling messages such as e-mail, *i.e.*, those engaged in the "receiving, assisting in receiving, transmitting, or assisting in transmitting" of communications. It "is designed to regulate the conduct of communications personnel" who are charged with handling private transmissions.[78] As one who facilitates the transmission of electronic communications, a BBS sysop evidently is included among this group of individuals.

The civil remedies allowed under this section are as follows:

> (1) an injunction against the wrongdoer to stop what he is doing;
> (2) actual damages suffered by the plaintiff, plus any profits made by the wrongdoer which he would not have made but for the unlawful use of the communications; or
> (3) $250 damages for each violation, but not more than ten thousand dollars.[79]

Additionally, if a violation is willfully committed for commercial advantage or private financial gain, a court may increase the plaintiff's award by up to fifty thousand dollars.[80] However, if it is found that the wrongdoer did not know and had no reason to know that his actions constituted a violation, a judge has the discretion to reduce an award to plaintiff under this section downward to one hundred dollars.[81]

B. Judicial Application of ECPA

If decided, *Thompson* would have been significant as the

---

77. 47 U.S.C. § 605(a) (Supp. III 1985).
78. S. REP. NO. 1097, 90th Cong., 2d Sess. 85, *reprinted in* 1968 U.S. CODE CONG. & ADMIN. NEWS 2112, 2197; *see* 47 U.S.C. § 605(a) (Supp. III 1985).
79. 47 U.S.C. § 605(d)(3)(B), (C) (Supp. III 1985).
80. 47 U.S.C. § 605(d)(3)(C)(ii) (Supp. III 1985).
81. 47 U.S.C. § 605(d)(3)(C)(iii) (Supp. III 1985).

first BBS case under ECPA and the Cable Communications Policy Act. In a situation involving stored communications, like that alleged in *Thompson*, a sysop should now face civil liability under both Title II of ECPA and the Cable Communications Policy Act. Any sysop who undeletes e-mail on the host system and then causes a private message to become public will almost certainly be found to have violated the two provisions. There may well be no liability under Title I of ECPA, however, since the private communications had already been received by the intended recipient and were not necessarily intercepted while in transmission.

VI. ECPA AND CORPORATE SYSTEMS

In this author's opinion, ECPA should be applied fully to corporate computer communications systems. However, in the corporate context, both coverage and liability under ECPA may be limited to certain situations. The wording of the Act creates questions as to who could be held liable under ECPA for invading a company's wholly private online system. The cracker and corporate "big brother" situations present the greatest potential problems.

A. The Cracker Situation

Title I of ECPA provides some clues as to the potential liability of crackers. Under Title I, private systems are differentiated from public systems in the protection they receive. ECPA provides that "[i]t shall not be unlawful . . . for any person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is *readily accessible to the general public*."[82] Thus, under this section, there is no legal liability for reading a public message in a conference configured to be public on a BBS. However, with regard to systems configured for privacy, the ECPA prohibition against unauthorized interception, access, and disclosure of transmitted and stored electronic communications stands.[83] Thus, it would be unlawful for a cracker or an unauthorized employee to intercept, access, or

82. 18 U.S.C. § 2511(2)(g)(i) (Supp. IV 1986) (emphasis added).
83. 18 U.S.C. §§ 2511(1), 2701(a), 2702(a) (Supp. IV 1986).

disclose private electronic communications transmitted or stored on wholly configured private online systems. Such private systems primarily consist of corporate online systems which are not accessible to the general public.

The legislative history of ECPA provides some evidence of its intended application to corporate systems. The "Purpose" section of the Senate report contains the following paragraph:

> Today we have large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices and video teleconferencing. A phone call can be carried by wire, by microwave or fiber optics. It can be transmitted in the form of digitized voice, data or video. Since the divestiture of AT&T and deregulation, many different companies, not just common carriers, offer a wide variety of telephone and other communication services. It does not make sense that a phone call transmitted via common carrier is protected by the current [pre-ECPA] federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major U.S. corporations today, would not be covered by the statute.[84]

Thus, in the Senate report itself, Congress stated its intention that both publicly accessible systems and wholly private corporate systems should be treated identically.[85] Congress also addressed the privacy problems of corporate computer communications by adopting Title II of ECPA.[86] In those sections, ECPA addresses "the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications *that are not intended to be available to the public.*"[87] Wholly private corporate systems, in this author's opinion, undoubtedly are included within this stated concern.

Finally, Congress further evidenced its intent to protect corporate computer systems by amending the definition of "wire communications" to include "communication affecting interstate or foreign commerce."[88] According to the Senate report,

---

84. S. REP. NO. 541, 99th Cong., 2d Sess. 2-3, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. News 3555, 3556-57.

85. While this statement seems to ring true with regard to the cracker situation, it may not apply in the big brother situation. *See infra* Section VI(B).

86. 18 U.S.C. §§ 2701-10 (Supp. IV 1986).

87. S. REP. NO. 541, 99th Cong., 2d Sess. 35, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3589 (emphasis added).

88. 18 U.S.C. § 2510(1) (Supp. III 1986).

this new "language recognizes that private networks and intra company communications systems are common today and brings them within the protection of the statute."[89] Congress thus intended to apply ECPA to both public and private systems.

Wholly private corporate systems are statutorily protected by ECPA from unauthorized intrusions by those not privileged to access and use the system. Specifically, protection is provided from intrusions by crackers and unauthorized employees.

B. The Corporate Big Brother Situation

However, another question remains. If an employee is authorized to use a company's in-house computer system for communications purposes, does he have the same privacy rights against his employer under ECPA as a user on a hobbyist BBS or consumer commercial online service has against unintended recipients? The answer to this question is found under Title II of ECPA.

Under section 2701, although it may be illegal for others to gain access without authorization or to exceed authorized access to a system, "the person or entity providing a wire or electronic communications service" is not liable for any offenses regarding stored communications, *i.e.*, voice mail, e-mail, or other recorded communications.[90] In other words, there simply is no ECPA violation if "the person or entity providing a wire or electronic communications service" intentionally examines everything on the system, whether or not it is for the purpose of a system quality control check. Section 2701 thus appears to be a statutory license for the corporate "big brother" who wishes to access and sift through private e-mail on the company's online computer system.

Moreover, section 2702(b)(5) may allow a company to divulge the contents of an employee's electronic communications on its private system under certain circumstances. Under that section an employer may divulge an employee's communications "as may be necessarily incident to the rendition of the service or

89. S. REP. NO. 541, 99th Cong., 2d Sess. 12, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3566 (emphasis added).

90. 18 U.S.C. § 2701 (Supp. IV 1986).

to *the protection of the rights or property of the provider or the service.*"[91] An employer could conceivably extend his right to protect "the rights or property of the provider or the service" to include actions taken to protect the private internal business interests of any company which happens to have a private in-house online system. All company secrets, including private corporate communications, and other material within the system would be corporate property. Electronic communications found on a corporate online system could thus be accessed, examined, and disclosed by the corporate sysop or owner. As telelaw expert Brock Meeks notes,

> [i]f the "entity" is a corporate sponsored system, then the sysop of that corporate system could indeed make any private files public without fear of coming under the jurisdiction of the ECPA. Because all [those] using the corporate system are "employees" of the entity, there is no expectation of privacy.[92]

ECPA protection in the employer-employee situation may indeed be non-existent.[93] While the corporate exception acknowledges an employer's property rights in all parts of his business, it leaves the employee's privacy interests completely unprotected.

In the corporate context, ECPA thus protects from without, but not from the within. A corporate online system may be statutorily protected from outside crackers and unauthorized employees, but an employee authorized to use an in-house company system for business purposes is not protected from intrusions by his employer. His employer may electronically look over his shoulder to search through any "private" material transmitted or stored on the system.

The two major threats to corporate communications privacy are thus treated differently by the ECPA. One may only be liable under the ECPA if (a) he is not part of the company, *i.e.*, he is a cracker invading the system from the outside with a remote modem-equipped computer, or (b) he is an employee, or

---

91. 18 U.S.C. § 2702(b)(5) (Supp. III 1986) (emphasis added).

92. Electronic message from Brock Meeks (Mar. 30, 1988).

93. This legislative intent to exclude corporate monitoring of employees from ECPA was confirmed by those who followed the drafting of the legislation. According to Jerry Berman, counsel for the American Civil Liberties Union, a participant in the drafting of the legislation, "ECPA 'goes right up to the water's edge [of employee privacy protection] but stops short' and to have included some employee privacy protection against employers in the corporate context 'would have killed the bill.' " Electronic message from Brock Meeks (Mar. 31, 1988).

other person, who is not authorized, or exceeds his authorization, to use the system. However, an employer, or one authorized by the company, is committing no offense if he electronically eavesdrops on e-mail correspondence found on the system. The corporate "big brother" situation is unfortunately maintained under ECPA as an exception to the user's privacy protection.[94]

CONCLUSION

As we move into the twenty-first century, it is likely that more cases like *Thompson* will develop. The future is also likely to bring the passage of more electronic privacy legislation in the manner of ECPA. Most recently, California was in the process of developing an "Information Bill of Rights."[95] While this bill died in committee, it did point out a growing awareness at the state level of the need to develop computer privacy law. Clearly, formulation of similar legislation must continue in both Congress and the state legislatures if the law is to keep a steady pace with constantly advancing technology. Fortunately, ECPA set the stage for much-needed changes in the present law by closing some of the loopholes which existed in electronic communications privacy law.

94. Needless to say, the same ECPA criminal procedures may apply in the corporate context as in the commercial and "hobbyist" contexts if law enforcement officials seek to obtain evidence from a corporate system. However, a corporate entity may have more discretion whether to seek protection from governmental intrusion under ECPA or to voluntarily turn over the evidence to law enforcement on a mere request under the corporate "big brother" exception.

95. Cal. Assembly Const. Amend. 36 (1987). The proposal "died" in the California Senate Judiciary Committee on June 21, 1988. Electronic message from Bob Jacobson, Principal Consultant to Assemblywoman Moore (June 21, 1988).