Copyright © 1993 IEEE. Reprinted from *Collection of Award Winning Papers 1993 Honorarium Competition*, Computer Sciences Corporation Systems Group, Catherine A. (Wood) Ferguson, "Electronic Mail and Privacy in the Corporate Environment."

This material is posted here with permission of the IEEE. Such permission of the IEEE does not in any way imply IEEE endorsement of any of Banner & Witcoff's products or services. Internal or personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution must be obtained from the IEEE by sending a blank e-mail message to pubs-permissions@ieee.org.

By choosing to view this document, you agree to all provisions of the copyright laws protecting it.

ELECTRONIC MAIL AND PRIVACY IN THE CORPORATE ENVIRONMENT

Catherine A. Wood
Computer Sciences Corporation
Integrated Systems Division
Moorestown, NJ 08057

ABSTRACT This paper addresses the issues related to electronic mail (E-mail) with respect to privacy in the workplace. It is not intended for a technical audience, but rather for managers and attorneys who may have to deal with the hazy areas of corporate concerns in the technical and legal arena.

In addition to some technical background, there are three main topics covered in the paper. The first topic reviews the sections of the Electronic Communications Privacy Act (ECPA) of 1986 that may be applicable to E-mail privacy in the corporate environment. The ECPA was enacted to protect against unwarranted search and seizure on the part of the government, or Big Brother. However, there is some question as to how the ECPA applies to corporations, or Little Brother. The second topic reviews recent litigation that has risen out of corporate inspections of employee E-mail. These employee suits involve the use of corporate assets that supported "private" E-mail for employees. The third topic presents some proactive corporate strategies to prevent or at least reduce the risk of corporate liability. The best policy is to have a policy; doing nothing can be very costly. It is important to establish a corporate privacy policy with respect to E-mail and publish it. A policy tucked away in a manual will be of little help in the event of a lawsuit.

I. INTRODUCTION

While there is no federal law that guarantees a general right to workplace privacy, state laws, local statutes, and/or private contracts (e.g., collective bargaining agreements) may confer such rights. The Electronic Communications Privacy Act (ECPA) guards only against unauthorized users of electronic mail (E-mail). The ECPA never addresses E-mail privacy in the workplace.

The 99th Congress passed the ECPA of 1986, which substantially updated the law protecting advanced forms of communications and networking [1]. This was the first time Congress had addressed the issue of communications privacy since Title III of the Omnibus Crime Control and Safe Streets Act of 1968 [2]. Technology had advanced considerably during the intervening 18 years, but the law had not kept pace [2].

Under Title III, interception of wire communications over a "common carrier" [3] was prohibited unless authorized by a court order [4]. Interception was restricted by definition to aural acquisition [3].

The ECPA was enacted to update the law in order to protect all forms of electronic communications from unauthorized interception [5]. The ECPA was an attempt to balance the legitimate needs of government law enforcement agencies with the privacy rights of the citizenry [2].

This paper discusses (a) the technical background of E-mail, (b) the sections and definitions of the ECPA applicable to E-mail, (c) the ECPA as it relates to recent lawsuits involving the monitoring of E-mail in a corporate setting, and (d) related corporate policy procedures and options.

II. TECHNICAL BACKGROUND

E-mail can transfer messages around the office and around the world [4]. E-mail basically consists of electronically transmitted messages like regular mail or telephone conversations. These private messages are usually sent over public or private telephone systems [3]. Public telephone systems and public service carriers/providers include AT&T, MCI, and Western Union [4]. Private systems include corporate networks.

In general, electronic mail is entered into a computer or terminal by a sender [3]. An E-mail message is somewhat similar to a corporate memorandum in that there is usually a "TO," "FROM," and "RE" as part of what is commonly known as the header. The address typically increases in size and complexity as the distance increases between sender (source) and receiver (destination). Distance is not necessarily geographic, and may include factors such as whether the destination is another company using another service provider, even though the company may only be across town. E-mail is commonly transmitted via telephone lines [3]. However, an E-mail system may transmit via a local area network (LAN), which may subsequently be "gatewayed" to a public service provider [6]. In either case, the message is stored at the destination in the receiver's "mailbox" until it is retrieved [3].

Communications system performance, determined by how much data can be forced through the communications pipeline, is affected by many factors. One significant factor is the use of electronic security measures. In general, the greater the security, the less the effective throughput, or rate at which data flows through the pipeline. This is particularly true with message/data encryption devices, such as the commonly used Data Encryption Standard (DES). The rates at which these devices operate are limited, as are the number of virtual circuits that they can support. This is because message streams are combined, or multiplexed, to reduce the number of encryption devices required. The

maximum operating rate of the DES is 56,000 bits per second (56 Kbps), and it can support a maximum of 64 virtual circuits. This means that only 64 users can operate the system simultaneously and, while a typical terminal processes about 1,200 bits per second (bps), each DES-equipped terminal would process less than 900 bps.[1] For a large company, the costs for data encryption and multiplexing alone could be astronomical if the company had to provide such electronic security for each user. As a result, companies often must weigh that cost against the potential costs of not providing security.

III. ECPA - THEN, NOW, AND LOOKING AHEAD

The ECPA addresses "problems relating to the transmission (and related storage) of electronic communications [8, Summary of Changes between H.R. 3378 and H.R. 4952]." In particular, the purpose of the ECPA is to "protect against the unauthorized interception of electronic communications [3]." The principal changes from the 1968 version of Title III are (a) an expansion of coverage from strictly voice communications to voice, data, and video communications, and (b) expansion of the recognized service providers to include private as well as common carriers [8, Summary of the Electronic Communications Privacy Act].

In passing the ECPA, Congress heeded the call to protect citizens' privacy and thus maintained the Fourth Amendment rights guaranteeing freedom from unreasonable search and seizure by the government. The ECPA protects electronic communications not by controlling the contents of the communications, but by attempting to control the communications systems themselves [8, Dr. Lynn Ellis]. In fact, the main thrust of the Act is to specify the circumstances under which the government "may conduct electronic surveillance [8, Dr. Lynn Ellis]."

The ECPA defines electronic communications, by means of a laundry list of both the types of communications and the media [1], as "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 [9]." Carefully excluded are (a) the radio portion (between the handset and base unit) of a cordless telephone, (b) oral or wire communications that are covered under the Wiretap Act (Omnibus Crime Control and Safe Streets Act of 1968), (c) communications from tracking devices, and (d) communications of a tone-only paging unit [9].

The ECPA would provide a nationwide floor of protection [8, Rep. Carlos J. Moorehead] for electronic communications that affect "foreign or interstate commerce [9]" only. Individual states can act to protect the privacy of electronic communications whether carried by a private or public service provider if such communications are wholly intrastate. This means that a corporation that has its own private system would have its wire transmissions protected under the Wiretap Act. The company itself would not be subject to any federal privacy controls under the ECPA, because, as the service provider, it would be protecting its own rights or property [1]. Individual states could therefore expand privacy protections in the area of intrastate wire electronic communications.

Any discussion of jurisdiction with respect to intrastate non-wire electronic communications requires some technical definitions. *Microwaves* are "any electromagnetic waves in the radio-frequency spectrum above 890 megacycles." Satellite communications are a form of microwave. This means that both microwave and satellite communications are radio broadcast media and, as such, are subject to Federal Communications Commission (FCC) regulation, even if wholly intrastate. This effectively preempts any further action on the part of individual states in terms of regulation or privacy protections for radio broadcast media.

Under the ECPA, an *electronic communications system* comprises the transmission facilities "and any computer facilities or related equipment for the electronic storage of such communications [9]." *Electronic storage* is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communications by an electronic communication service for purposes of backup protection of such communication [9]." The expansion of the scope of an electronic communications system is necessary to accommodate situations involving multiple service providers or multiple stations of a single service provider in the communications path across the country. The communication is essentially forwarded from one service provider or station to the next. Upon reaching any subsequent service provider or station, the communication is temporarily stored until the header is read in order to route the message to the next service provider or station. At each "intermediate system"[2] in the network, the message may be temporarily stored in a computer or other electronic media such as tapes or disks, which must be protected just as computer memories are protected [3]. Without protection of this "temporary, intermediate storage [9]," any electronic communications would be vulnerable.

An *electronic communications service* includes any carrier, public or private, which provides its users with the "ability to send or receive wire or electronic communications [11]." This

[1] IRE XHS operates at 56 Kbps (or 56,000 bps) and offers 64 virtual circuits. 56,000 bps/64 virtual circuits = 875 bps per circuit or user.

[2] "Intermediate system" is the Consultative Committee for International Telegraphy and Telephony (CCITT) International Standards Organization (ISO) Open System Interconnection (OSI) standard terminology for any system or node in the communications path (network layer and below) that is capable of routing. An "intermediate system" is used when an end system is not connected to a Wide Area Network (WAN) but rather to a Local Area Network (LAN) or is a point-to-point connection. International Standard #ISO 9543 (1988-08-15), pgs. 4-6.

includes telephone and telegraph companies, as well as E-mail companies, both public and private [3]. However, as noted earlier, protection is granted only to those communications affecting interstate or foreign commerce.

In a corporate setting, there is usually a difference between the E-mail *user* and the *subscriber*. The user is often an employee with a personal computer or terminal connected to a mainframe. The user may also be operating a personal computer from his or her home. A subscriber purchases the service from the service provider. While a user and subscriber may be synonymous, it is unlikely in the corporate environment. In this case, the corporate entity is almost always the subscriber and the employees the users [4].

The ECPA makes it illegal to "intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient [9]." This raises the question of whether the user can be the agent of the subscriber and vice versa. Specifically, if the employer is the subscriber, is the employer or its designated agent also the agent of a user of the electronic communications system where the user may be an employee?

Interception is any acquisition of the contents of any electronic communications by any means [9]. It is illegal only when there is an unauthorized user or an unauthorized use involved.

The ECPA further prohibits providers of wire or electronic communications from interception, disclosure, and use of customer communications except as necessary, incident to the service or in order to protect the provider's property or rights [3]. Examples of such permitted uses may be the interception of the header information for proper routing of the message, for quality assurance checks [3], for backup of messages needed to restore the system in case of failure, and for accounting and billing purposes akin to call detail records used by telephone companies. Accounting operations are generally performed by computers without human intervention.

The backing up of messages is one of several examples of communications-related storage of data in computers. The protections afforded to communications while electronically stored incident to transmission are separate from protection during electronic transmission. Recent E-mail cases have focused on the electronic storage portion of the electronic communications system.

An *unauthorized user* is one who has no right to access the E-mail system under any circumstances or conditions, whereas an *unauthorized use* is a prohibited use which may be perpetrated by an otherwise authorized user [3].

The ECPA addresses unauthorized users and unauthorized use and specifies the punishment for a user who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system [10]." This subsection thus deals with third parties that are neither the service provider nor the government. The limitation on this unauthorized access is for communications "not intended to be available to the public [3]" and effectively expands the definition of electronic communications to include electronic storage [3]. The ECPA stipulates further protection from knowing disclosure of the contents of any communication electronically stored by the service provider's equipment [11] except to the intended recipient (or addressee) or to the recipient's authorized agent [3]. The exceptions to this protection are when communications are disclosed (a) with the sender's or receiver's lawful consent, (b) by a service provider's employee during the normal course of business, (c) as part of the service provided or to effect protection of the service provider's property or rights, or (d) to a law enforcement agency if the service provider obtained the contents inadvertently and the contents "appear to pertain to the commission of a crime [3], [11]."

Senator Patrick J. Leahy of Vermont, one of the principal sponsors of the ECPA, formed a task force in 1991 to research new technologies in order to assess the continued viability and vitality of the ECPA, which is only seven years old [13]. This was deemed necessary in light of the current spate of lawsuits over E-mail privacy and radio-based communications technologies [13]. While the task force concluded that no changes to the ECPA were necessary at that time, it also reported that "the distinction between private and public E-mail systems will become blurred by interconnections between the two, so it may become more and more difficult to determine which systems are covered by ECPA [13]."

In early 1991, the First Conference on Computers, Freedom, and Privacy was held in Burlingame, California. Issues such as the rights of computer users, individual privacy, and constitutional protections for electronic communications were discussed [14]. The results culminated in a proposed 27th Amendment to the U.S. Constitution in order to "explicitly extend constitutional protection to all communications 'without regard to . . . technological method or medium [14].' "

IV. E-MAIL AND LITTLE BROTHER

Security and privacy are closely related, but they are not always in concert. In fact, in many cases they are in direct conflict. As more information about individuals is stored in computers across the nation, there is an increasing need to guard that information against misuse, such as unauthorized alteration or dissemination. This means that heightened security is needed in our

computer and electronic communication systems. Increased security may require increased auditing and surveillance in the workplace in order to ensure that databases are kept safe. However, the same tools that can be used to ensure systems security can also be used to measure productivity, for example, by counting keystrokes [15] or monitoring access in order to determine which data files are being used (e.g., computer games, personal letters, or even E-mail). This type of monitoring can lead to both perceived and actual reductions in workplace privacy. Employees (and others who may not be in an employee relationship with the monitor) are, in many cases, paying for increased computer and electronic communications system security with their personal privacy. There are many factors in the complex equation that attempts to balance security, privacy, and property [32]. The monitor in these situations is not the government, or Big Brother, which the ECPA guards against, but rather Little Brother, or corporate management, against which workers have no federally based legal protection [15].

There have been two suits in California courts against Epson America, Inc.: the widely publicized Shoars suit and a subsequent class action suit on similar grounds filed by representatives of the approximately 700 employees of Epson America [16].

In her suit, Alana Shoars alleged wrongful termination, defamation, and invasion of privacy on the part of Epson [17]. Epson was both an E-mail subscriber and a provider. That is, Epson subscribed to the MCI-mail, and the mail was stored on Epson's HP mainframe computer system in mailboxes until it was retrieved [19]. The latter function made Epson a service provider with the right to access messages incident to the service [1], [11] and with an interest in protecting its property or rights under the ECPA, at least [11]. Moreover, E-mail falls squarely into the category of an investment, and companies typically look at the bottom line, monitoring usage and controlling costs in order to maximize their return on investment [7]. Therefore, under the ECPA, Epson America was within its rights to access all E-mail on the system. The employer's rights to protect its property and rights thus leaves the employees wholly unprotected [1]. The employer has property rights in all aspects of its business [1], especially in the protection of proprietary information. Therefore, if Shoars has a cause of action, it is not under the ECPA but must be based on state law.

California has enacted more restrictive standards in order to raise the level of protection afforded to users of electronic communication systems. Shoars alleged violations of California Sec. 631 or California Sec. 632 in the alternative, and claimed a right to bring the action under California Sec. 637.2(a) [18]. California Sec. 631 prohibits wiretapping, nonconsensual reading, use, conspiracy, and causing to be read [18], [33, §631], while California Sec. 632 prohibits eavesdropping [18], [33, §632]. The Shoars complaint was amended several times and was appealed from a lower court dismissal. Epson America had demurred, asserting that California Sec. 632 only protects "confidential communications," which are defined as those communications in which there can be a reasonable expectation of privacy [17]. Epson America further asserted that California Sec. 632 is only applicable to interception using equipment not connected to the transmission medium [17]. Shoars had counterclaimed that, until she discovered that the E-mail was being recorded and printed, she believed that the E-mail system was private because she had been issued a password. She had never been advised that the E-mail was not private, nor had she ever consented to the monitoring or interception [18] of her E-mail. Upon discovering the monitoring process, she "asserted her expectation of privacy [18]." The arguments boil down to the plaintiff arguing for privacy because there was an expectation of privacy and there was no advance warning of the monitoring, and the defendant countering that there should not have been an expectation of privacy for messages generated and transmitted on company time using corporate assets [20].

An additional problem arises when messages contain both personal and business information [20]. An example of such a hybrid message might be a valid business message that ends with "Let's have lunch together tomorrow" or "We have a 7:30 a.m. tee time on Saturday." The class action suit has suffered a fate similar to that of the Shoars case [16]. This action was based solely "upon an alleged violation of Penal Code Sec. 631 [16]." The court found "no legal support for plaintiffs' contention that the E-mail communications system described and alleged in the complaint herein comes within the protection of said statutory scheme, even if it be assumed, for purposes of demurrer, that plaintiffs 'had an expectation of privacy in their communications and none had given EPSON prior authorization to monitor or print up their electronic communications [16].'" The court based its decision heavily on an article in the *Federal Communications Law Journal* entitled "ECPA and Online Computer Privacy," by Ruel Torres Hernandez, in which the author concluded that there was no ECPA violation, even for intentional monitoring, if it was perpetrated by the entity providing the service [16].

A policy is only effective if it is enforced. No matter what the protection scheme — password, encrypted password, or encrypted message — the system administrators, or superusers, can still access anything they want to or are directed to access. If the superusers do not know a password, they simply change it. Superusers can see it all, read it all, or print it all [21].

While E-mail has been compared to a letter or telephone call, it differs from both with respect to the source of payment for the service and, consequently, the privacy rights of its users. Charges for public E-mail services are based on the number and size of the messages in addition to a flat monthly fee. In the corporate environment, the employer is paying for the E-mail service, and is therefore the subscriber, the user, and possibly, as in the case of Epson America, in part the service provider. In using the U.S.

Postal Service, the user is purchasing the service from the government, as opposed to the employer funding the service. In the case of telephones, the company is also paying for the service. Telephones, on the other hand, are relatively inexpensive, as are unlimited local calls. Although they are either legally prohibited from monitoring conversations or simply choose not to, most companies do maintain some form of billing and accounting records based on call detail records supplied by the phone company. Presumably, if any abuse or abnormalities are apparent, companies can take corrective action. Ostensibly, the same type of monitoring could take place on an E-mail system. However, there is still a major cost differential. Making some reasonable assumptions, MCI-mail could cost a company like Epson in excess of $600,000 per year.[3]

Because of the classified nature of the work, all direct employees of the Department of Defense, as well as all contractors and their employees, waive their privacy rights upon employment. Some of the individual rights waived are far more significant than the degree of privacy diminished by the monitoring of E-mail. However, this interdiction of individual rights is not unique to the Department of Defense. Any government agency that uses FTS2000 (the new federal telecommunications system) is responsible for internal audits and abuse control [22]. If it is not the nation's biggest employer, then the federal government is certainly one of the nation's largest users of E-mail. As such, a significant portion of the population is already subject to some form of monitoring or interception based on security (protection of proprietary or classified information) or the employer's property rights.

In addition to subscription charges, there are hidden costs related to E-mail. Encryption of E-mail communications has costs beyond the initial investment in equipment. As mentioned earlier, encryption reduces the speed and volume of communications traffic, so that additional costs must be incurred to bring system performance back up to the levels achieved before encryption. As an overall cost of doing business, this cost is passed on to the consuming public, not unlike other costs of doing business, such as ensuring safety and protecting the environment.

However, the decision to monitor employees' private communications should not be based on these costs alone. The decision-maker should weigh factors such as loss of productive time for the individual performing the monitoring, loss of respect for and trust of management, and inhibited creativity due to fear of the consequences of sending a message.

Companies form a wide spectrum in how they perceive and measure their return on investment. Some weigh such factors as creativity and personal freedom more highly than others. Companies at this end of the spectrum would include Shoars' current employer [23]. The Department of Defense and its corporate contractors are most certainly at the other end of the spectrum. Interestingly, both of these positions are probably well publicized, that is, employees are well informed of their employer's position. The privacy issue is more likely to arise in companies in the middle of the spectrum, or even at the security-conscious end if the employees are uninformed.

Since Shoars filed her suit, at least two similar lawsuits have been filed. One is against Nissan Motor Corp. for similar conduct [20], [24], [25]. The second is by Ron Collins, an employee of the Department of Labor and Industries of the State of Washington. Collins, represented by the Washington Federation of State Employees counsel, maintains that during training, state employees were "regularly advised that the electronic mail system . . . is available for personal communications with other employees, and that department publications tell employees that using a password will prevent unauthorized access to their 'personal files [26].' " Yet another upcoming event may be the admission as evidence of E-mail messages exchanged between Los Angeles police officers after the well-publicized and televised beating of Rodney King earlier this year [20]. If Los Angeles provided or subscribed to an E-mail system, then under the ECPA, the city has a right to access everything on the system, including E-mail sent between the officers. This could substantially affect the officers' positions, as well as any subsequent liability on the part of Los Angeles.

Prodigy, a joint venture of IBM and Sears, is also encountering legal problems. In order to enforce guidelines for using the system and for accounting and billing purposes, the service providers are inspecting user communications apparently by trapping communications based on certain patterns. According to Marc Rotenberg, Director of the Washington Office of Computer Professionals for Social Responsibility, "If Prodigy was in fact reading the contents, then they may, in fact, be violating the communications privacy act [27]." Not so; as a service provider, Prodigy is probably not doing anything illegal, since the interception is incident to the service and protects the provider's property or rights [27]. Thus, it appears that, while this may be a poor business decision, it may not be illegal, at least under the ECPA [27]. The E-mail bulletin boards are rife with rumors of investigations and sensitive data such as lawyer-client notes being intercepted on the Prodigy system.

[3] Using three-quarters of the employees transacting ten messages per day (based on Texas Instruments statistics cited in *USA Today* on 26 June 1991, pg. 1B) for 260 days per year at $0.45 per message for a small message (based on tariffs cited in *PC Magazine*, August 1989).

V. CORPORATE POLICY OPTIONS

John Podesta, a former aide to Senator Leahy, a lobbyist for special interest groups such as MCI and AT&T, and chairman of Senator Leahy's new task force [28], and David Johnson prepared a report for the Electronic Mail Association in December of 1990 [29]. Podesta and Johnson addressed a number of issues in an attempt to raise employer consciousness. The authors urged a balanced policy based on full consideration of the issues and, above all, complete disclosure of that policy to all employees in advance. The report offered sample policies ranging from the most restrictive (which gives highest priority to protection of employer's property) to the most liberal (which emphasizes employees' rights) [29]. Regardless of the policy type selected, it will not be effective unless it is understood by employees. Companies have used a variety of methods to inform employees, such as equipment warning stickers, on-screen warning messages, and signed affidavits acknowledging that employees have read and understood the policy [30]. All of this is reminiscent of the intent embodied in the Miranda warnings.

It is not only important for employers to advise employees of their policies, it is equally important that employers keep abreast of their "legal protection and liability for electronic communications [14]." This includes state and local legislation because a policy is no good if it is illegal [31]. Jerry Berman, a representative of the American Civil Liberties Union and a witness at the ECPA hearings in 1985, postulates that the privacy versus property issues will "be decided partly by the courts, partly by Congress, and partly by the institutions developing a culture around these technologies [30]."

Topics such as the roles of the parties to the E-mail process are addressed not only in terms of their rights but also in terms of their duties. For example, while an employer has the right to set and enforce E-mail policy, supervise employees, and prevent illegal use of its systems, the employer may also have a duty to respect employees' reasonable privacy expectations. Conversely, while employees have a right to be informed of the corporate E-mail policy and a right to some security with respect to unauthorized interception, employees also may have a duty to disclose communications made as an agent of the company. Similarly, third parties may have some privacy rights as well as some duties to disclose [29]. Service providers have a right to protect their own rights and property [11], and in doing so, have an interest in ensuring that companies and their employees comply with the service provider's rules and policies. Service providers have an equally strong interest in knowing a subscriber's policy, especially in knowing who may request or give consent to access employees' E-mail [29]. Employers may also be subject to significant tax ramifications when the E-mail system is provided for personal use [29].

There are some technological considerations in formulating corporate E-mail policy. While wiretapping a telephone line without a warrant based on probable cause is strictly forbidden, and voice communications are very transient, E-mail, which is often used as a substitute for a telephone call, is not necessarily protected from corporate interception and is more easily accessed because it is stored, often before and after receipt. E-mail files are easily altered, forwarded, or broadcast. Erasure is not fully effective either, as archival or backup and transactional records may be maintained [29]. As with the corporate memorandum, E-mail supports "attachments [29]" which, if unchecked, could result in the wholesale transfer of proprietary company data to anyone, including a competitor, either unwittingly or by a disgruntled employee. Since E-mail usually travels over a telephone system using some form of modem, which is a full-duplex device (two-way communications), outsiders can send communications into the corporate facility. These communications can consist of almost anything, including messages, data, or a "worm" or "virus," such as the one that was sent through academic, government, and military facilities several years ago by Robert Morris. That particular worm did not destroy data, although some viruses are designed to do so. The Morris worm entered computers, duplicated itself, and acquired available memory. This continued until the computer could perform no useful work because it had no memory to allocate to valid programs. As a result, many computers came to an abrupt halt. One estimate placed damages in the $5 million to $15 million range. This could be considered the ultimate argument for employers' property protection and security and against individual privacy in E-mail.

VI. CONCLUSION

Computers are simultaneously shrinking in size and becoming more powerful. The power of a Cray computer will soon be contained in a device no larger than a coffee mug. In today's research laboratories, technology is pushing the limits of physics in the area of communications. Laser and other technologies will soon support raw data rates in excess of 500 megabytes per second (Mbps) [12]. Technical literacy for all citizens will soon be a necessity, not a convenience. Because of such technological advances, the ECPA may become obsolete more quickly than Title III.

There is no federally based legal protection for individual privacy in the workplace, nor have the states provided such protection to any significant extent. Even in California, a qualitatively persuasive state where more protective provisions have been enacted than in other states, privacy protections have not been read expansively when the workplace is involved. However, this narrow view may be reconsidered as technology advances and invasions of personal privacy become so flagrant that they shock the conscience of the court. As the lines between the workplace and home continue to blur and equipment ownership (indi-

vidual assets versus corporate assets) shifts, privacy protection may be expanded, by necessity or by demand.

REFERENCES

[1] R. Hernandez, "ECPA and Online Computer Privacy," 4 *Federal Communications Law Journal*, 1989.

[2] R. Kastenmeier, D. Leavy, D. Beier, "Communications Privacy: A Legislative Perspective," *Wisconsin Law Review* 717, 1989.

[3] S. Rep. No. 541, 99th Congress, 2nd Session, 1986.

[4] L. Simone, "E-Mail, The Global Handshake," *PC Magazine*, p. 175, August 1989.

[5] N. Welch, "E-Mail Privacy Not Guaranteed: Some Systems Still Unprotected Legally," *MacWeek*, no. 12, p. 12, 12 March 1991.

[6] S. Caswell, "Corporate Mail Networks," *Datapro Research*, p. 101, October 1989.

[7] S. Caswell, "Planning and Implementing E-Mail," *Datapro Research*, p. 105, November 1989.

[8] Electronic Communication Privacy, 1985: Hearing on §1667 before the Subcommittee on Patents, Copyrights and Trademarks, 99th Congress, 1st Session, p. 156, 1985.

[9] 18 U.S.C. §2510, 1986.

[10] 18 U.S.C. §2701(a), 1986.

[11] 18 U.S.C. §2702(a), 1986.

[12] Statement of Work for Architecture for Survivable System Processing (ASSP), PR no. A-1-1351, Rome Laboratory, Griffiss Air Force Base, p. 27, 10 June 1991.

[13] M. Betts, "Do Laws Protect Wireless Nets?", *ComputerWorld*, p. 47, 17 June 1991.

[14] "Extending the Reach of Free Speech," *MacWeek*, p. 22, 9 April 1991.

[15] J. Schwartz, "How Did They Get My Name?", *Newsweek*, p. 40, 3 June 1991.

[16] Flanagan v. Epson America, Ruling on Submitted Matter, 4 January 1991 (BC 007 036).

[17] Shoars v. Epson America, Defendant Epson America Inc.'s Memorandum of Points and Authorities in Support of Its Demurrer to Plaintiff's Verified Second Amended Complaint, 30 November 1990 (SWC 112749).

[18] Shoars v. Epson America, Plaintiff's Combined Opposition to Defendant's Demurrer to Second Amended Complaint, 14 December 1990 (SWC 112749).

[19] J. Nash, "E-Mail Lawsuit Cranks Open Privacy Rights Can of Worms," *ComputerWorld*, p. 7, 13 August 1990.

[20] S. Silverthorne, "E-Mail Growth Draws Industry Heavyweights," *Investor's Daily*, p. 1, 4 April 1991.

[21] S. Manes, "No, Virginia, There's No Such Thing as Total Electronic Privacy," *PC Computing*, p. 72, April 1991.

[22] American Telephone and Telegraph, *FTS2000*, Chpt. 1, General Agency Responsibilities, p. 1, 1989.

[23] J. Nash, "E-Mail Spurs New Privacy Debate," *ComputerWorld*, p. 78, 15 October 1990.

[24] G. White, "Suit Says Nissan Fired Pair Over Privacy Issue," *Los Angeles Times*, p. 3, 8 January 1991.

[25] "Nissan Motor Corp. in U.S.A. Named in Lawsuit for Electronic (E-Mail) Eavesdropping," *Business Wire*, 7 January 1991.

[26] Knox, *The American Lawyer*, December 1990, p. 24.

[27] Y. Lee, "New Prodigy Guidelines Raise Question of Privacy, Four E-Mail Protesters Receive Warnings," InfoWorld, p. 5, 26 November 1990.

[28] A. Kornhauseer, J. Sarasohn, "Forging a High-Tech Consensus," *Legal Times*, p. 5, 25 February 1991.

[29] D. Johnson, J. Podesta, "Formulating Your Company's Policy on Access to and Use and Disclosure of Electronic Mail Sent on Company Computer Systems," a white paper for the Electronic Mail Association, 10 December 1990.

[30] C. Casatelli, "Setting Ground Rules for Privacy," *ComputerWorld*, p. 47, 18 March 1991.

[31] S. Salamone, "Attorney Discusses How to Avoid E-Mail Privacy Woes; Employers Should be Up-Front about Office Policy," Network World, p. 21, 25 March 1991.

[32] D. Clark, *Computers at Risk*, Appendix 2.1, National Academy Press, p. 68, 1991.

[33] California Penal Code.