1-1-1992

Private, Legislative and Judicial Options for Clarification of Employee Rights to the Contents of Their Electronic Mail Systems

Michael W. Droke

Follow this and additional works at: http://digitalcommons.law.scu.edu/lawreview

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/lawreview/vol32/iss1/6

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara Law Review by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
PRIVATE, LEGISLATIVE AND JUDICIAL OPTIONS FOR CLARIFICATION OF EMPLOYEE RIGHTS TO THE CONTENTS OF THEIR ELECTRONIC MAIL SYSTEMS

I. INTRODUCTION

Few employees consider privacy concerns when interacting with other employees in the workplace. They talk on the telephone or gossip by the water cooler, often with disregard that their fleeting words might be overheard. This attitude prevails while more sophisticated methods of communication have entered the workplace, even when the new technology has created privacy concerns unknown less than fifty years ago.

The privacy rights of Americans are being invaded by new technology at a pace never before imagined. With the rapid development of technology, questions arise as to the increased availability of surveillance and storage of confidential information. The concerns include the actions of those who are

© 1992 Michael W. Droke
The author gratefully acknowledges Professor Eric Wright, Santa Clara School of Law, and Mrs. Mendy Moss Droke for their patient assistance throughout the writing of this comment.

1. Six million employees are spied upon by their employers every year, with cameras, searches and computer systems which can track output and tap into information. This surveillance poses a significant problem for telephone and data entry employees. CBS Evening News (CBS television broadcast, Jan. 2, 1991) (transcript on file at Santa Clara University School of Law Heafey Library). See also Richard Lacayo, Nowhere to Hide, TIME, Nov. 11, 1991, at 34 (discussing emergence of electronic surveillance and its perceived effect on the public).


authorized to access computer systems, as well as those who are not.4

These changes in technology greatly impact the employment environment, as they are frequently designed or quickly adapted to the needs of the workplace. One such new technology which has recently gained great popularity is electronic mail.5 The convenience and ease of use of electronic mail systems have turned them into "a strategic communications backbone in many corporations."6

This comment provides a statutory and constitutional analysis of employees' privacy rights in the contents of their electronic mail systems.7 It also discusses the possible application of wiretapping and computer crime statutes8 and tort causes of action.9 To protect business and employee interests, this comment proposes that businesses unilaterally adopt corporate policies,10 and both physical11 and administrative controls12 regarding their electronic mail systems. Therefore, throughout this comment both the legal and practical ramifications are discussed.

This comment proposes a variety of ways that business and employee interests could be protected through legislative and judicial action. It first proposes that the Electronic Communications Privacy Act of 198613 be interpreted to include electronic mail.14 Alternatively, it proposes a new statute

5. See Walter Ulrich, Electronic Mail is at Critical Turning Point, THE OFFICE, Aug. 1986, at 129, which cites expert predictions that over ten billion messages per year will be sent through electronic mail systems by the early 1990s.
6. Joanie M. Wexler, Users Find Frustration in Bulky E-Mail Links, COMPUTERWORLD, April 30, 1990, at 55. See also Lee Comes, Memo to E-mail Lovers: High-tech Notes are a Staple in the Office, SAN JOSE MERCURY NEWS, May 6, 1991, at D1 (Approximately 3.5 million desk-tops have electronic mail, and software sales should quadruple to $850 million by 1994.).
7. See infra notes 141-42 and accompanying text.
8. See infra notes 130-40 and accompanying text.
9. See infra section III.B-C.
10. See infra section III.D.1.
11. See infra notes 144-51 and accompanying text.
12. See infra section III.B.3.
14. See infra section IV.B.
which would directly apply to electronic mail. Finally, it concludes that the most long-lasting change may occur by reallocating the burden of proving that the system was not private to the employer, which has the most control in the employment environment. By proving this element, the employer overcomes any objective expectation of privacy and insulates it from liability.

II. BACKGROUND

A. How Electric Mail Systems Operate

Imperative to the comprehension of the issues which surround electronic mail is obtaining a grasp of its method of operation. Electronic mail is a communication system which allows a computer user to send messages to another person's terminal in a different location. All systems require that the user access the system using some type of name or identification code. This procedure authorizes the user to access the system, provides system security, and identifies the proper location for receiving messages. Once inside the system, the user may manipulate the contents of the mailbox in a variety of ways.

The levels of access and number of users vary among electronic mail systems. Standard electronic mail systems allow one user to communicate with another individual or a group. Ordinarily, messages on such systems remain confidential.

15. See infra section IV.B.3.
16. See infra section IV.B.3.

The workstations may be connected in a variety of ways. The simplest systems allow users to interact directly through use of a cable or wire. Id. at 93. Others use a modem and standard telephone lines, often transmitting and storing messages through a host computer system. Id.

The more complicated systems connect users through the use of a local area network (LAN) system, which interfaces many users with a mainframe or central processing unit. This main processing feature may run a variety of file servers, computers, printers, or other special-purpose devices. Id. at 93-96.

18. Id. at 46.
19. Id.
20. Id. at 47.
among the users.22 Other systems operate more as a bulletin board for general announcements, allowing all with access to read the messages.23 Bulletin boards may be privately or commercially organized, and do not afford the confidentiality available to standard electronic mail systems.24

The information sent may include text, graphics or audio signals.25 When transmitted, the data is transferred almost instantaneously to the receiving location,26 allowing the sender and receiver to interact quickly. It also allows corporate managers to better supervise the use of the system.27 Most modern systems do not require both parties to be on line simultaneously, and some permit the sender to choose a specific time for the central processing system to send the message.28 Some electronic mail systems copy each message as it goes through the system, while others destroy them automatically.29 Thus, unlike telephone systems, electronic mail systems may create a document which survives the destruction of the message by the receiver.30

B. The Recent Cases

Use of information obtained through electronic mail systems arises in many employment-related contexts. One of the

22. Id. at 3.
23. Id. at 3, 74. See also NETWORKING, supra note 17, at 16-17.
24. NETWORKING, supra note 17, at 17.
25. NETWORKING, supra note 17, at 3.
26. NETWORKING, supra note 17, at 3.
27. This efficient communication method creates a variety of benefits for companies in that it allows managers and supervisors to “track information that has been entered concerning a project[,] [s]upports activities such as conferencing[,] . . . [i]nforms and reminds users of scheduled events[,] [r]educes message reading time . . . [and] [i]ncreases the scope of information and communications flow, allowing more people, expertise, and data to be included.” NETWORKING, supra note 17, at 7-8.
28. NETWORKING, supra note 17, at 6.
30. Indeed, listed among the benefits of electronic mail are that it “establishes message or information files[,] [r]ecords message[s] automatically and accurately [and] [t]racks messages systematically [thereby] establish[ing] a message ‘audit trail.’” NETWORKING, supra note 17, at 7.
most widely publicized uses was during the Iran-Contra affair, which was uncovered in part by discovery of electronic mail messages sent by Lieutenant Colonel Oliver North.31 These transmissions had been stored by the computer system, even after the recipients had deleted or destroyed the messages.32

In another case, the members of the Colorado Springs, Colorado town council noticed that their mayor, Robert Isaac, seemed very well informed of their thoughts on local issues.33 They soon discovered that the mayor had been reading printouts of the council members' electronic mail conversations for over a year.34 According to the mayor, the messages had been printed in case they were covered by state public records law and in order to save space on the system.35 The mayor originally asked to see the printouts to ensure that the city council was not meeting secretly by computer.36

In an interesting case from the private sector, electronic mail administrator Alana Shoars was terminated from her position at Epson America after she discovered that her supervisor was reading reams of electronic mail printouts.37 Ms. Shoars' supervisor had been systematically printing thousands of electronic mail messages going to and from sources outside the company, including those with personnel and pricing information.38 Ms. Shoars has sued her former employer on behalf of herself and several other employees alleging violation of, among other things, California wiretap law.39


32. Ziegler, supra note 29, at C16, col. 4.


34. Id.

35. Id.

36. Id.


38. DeBenedictis, supra note 33.

39. Ziegler, supra note 29, at C16. See also infra note 51 and accompanying text. This theory was used in a case recently filed in a Northern California superior court. Jennifer Pittman, Employee Rights Tested in Suit over Electronic Privacy
In another abuse of an electronic mail system in the private sector, Apple Computer, Inc. was shocked to find that its employees were printing messages from the company electronic bulletin board which criticized management and sending them to the local newspaper. These messages made public complaints about company layoffs, executive perquisites, and the company's strategic direction.

C. Legal Background

1. Statutory Options

State and federal statutes provide the most easily applicable areas of protection to both companies and employees with respect to their electronic mail systems. One of the most significant recent developments was the passage of the Electronic Communications Privacy Act of 1986. This federal law makes it a crime to intentionally intercept any wire, oral or electronic communication. The penalty for violation includes up to five years imprisonment and fines up to $500, as well as a civil fine of no less than $1,000. The Act was intended to update existing law to address concerns arising from emerging technology, which should include

---

Invasion, S.F. DAILY J., Nov. 12, 1991 at 4; Brandon Bailey, E-mail Snoops Incense
41. Id.
42. 18 U.S.C. §§ 2510-2511 (1988) [hereinafter referred to in the text as the "Act"].
43. "[A]ny person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished." Id. §§ 2511(1)(a)-(d).
44. Id. § 2511(4)(a).
45. Id. § 2511(4)(b).
46. Id. § 2707 (civil cause of action created when any provider of electronic communication knowingly or intentionally allows unlawful access to stored communication; remedies include declaratory judgment, attorney fees, and actual damages not less than $1,000).
47. S. REP. NO. 541, 99th Cong., 2d Sess. 3 (1986) [hereinafter SENATE REPORT], "[T]remendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques." Id. These technological developments allow "overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others." Id.

This new statute "amends existing chapter 119 of title 18 to bring it in line with technological developments and changes in the structure of the telecommuni-
EMPLOYEE RIGHTS TO ELECTRONIC MAIL

Electronic mail. Thus far, all of the appellate cases citing the Act have considered its application to cellular telephones, not to electronic mail. An important qualifier, however, is that the Act applies only to those companies which in some way affect interstate commerce. Thus, it may leave unprotected those employees at smaller corporations which conduct business solely within one state.

Since the electronic transmissions must travel through the computer cable, they may be protected by wiretapping statutes. All but six jurisdictions have enacted a statute making it illegal to wiretap conversations. A significant hurdle is that most of these laws are limited to the unlawful tapping or eavesdropping of oral communications, which would obviate their application to electronic mail if the statutes were read narrowly. Furthermore, the primary remedy is penal, which would disallow a private cause of action and thereby prevent the victim from obtaining compensatory damages. However, some jurisdictions have responded by enacting statutes which are substantially similar to the federal law and may therefore allow broader application of wiretapping laws.

48. "As a general rule, a communication is an electronic communication protected by [this law] if it is not carried by sound waves and cannot fairly be characterized as containing the human voice . . . . This term also includes electronic mail, digitized transmissions, and video teleconferences." Id. at 14.

49. See United States v. Suarez, 906 F.2d 977 (4th Cir. 1990), cert. denied, 111 S. Ct. 790 (1990); Shubert v. Metropheone, Inc., 898 F.2d 401 (3d Cir. 1990); Tyler v. Berodt, 877 F.2d 705 (8th Cir. 1989), cert. denied, 110 S. Ct. 723 (1990); United States v. Jios, 875 F.2d 17 (2d Cir. 1989); Camacho v. Autoridad de Telefonos de Puerto Rico, 868 F.2d 482 (1st Cir. 1989); Edwards v. State Farm Ins. Co., 833 F.2d 535 (5th Cir. 1987) ("wiretapping" includes only oral terms).


51. ROBERT E. SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (1988). The states which do not have a wiretapping statute are: Indiana, Mississippi, Missouri, South Carolina, Vermont and Wyoming. Id. at 2.

An example of such a wiretapping statute is in California. The state makes it illegal for any person to intentionally tap or make an unauthorized connection with any telegraph or telephone wire. CAL. PENAL CODE § 631(a) (West 1988). The state also makes it illegal to attempt to read messages passing through a wire, line or cable. Id. A similar provision makes it unlawful for any person to "intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, [to] eavesdrop[] upon or record[] the confidential communication." Id. § 632(a).

52. SMITH, supra note 51, at 38-39.

53. SMITH, supra note 51, at 38-39.

54. SMITH, supra note 51, at 38-39. See also 38 HAW. REV. STAT. § 803-42.
In addition to wiretapping statutes, all but five jurisdictions have enacted statutes which make unlawful computer access a criminal act.\(^5\) Such statutes primarily prohibit the intentional access of computer systems by third parties attempting to obtain confidential stored information.\(^6\) In so doing, they may not be broad enough to include intrusion by company management or other employees, or the disclosure of conversations and material not deemed confidential. All jurisdictions, with the exception of Vermont, have either a wiretapping or computer crime statute.\(^7\)

A critical element of each wiretapping statute is the existence or absence of a reasonable expectation of privacy in the communication. Accordingly, the judicial development of privacy expectations must be analysed.

2. **Constitutional and Statutory Privacy Implications**

Electronic mail technology varies among systems, such that the determination of whether the system creates an expectation of privacy will entail a discussion of the underlying facts. However, such a factual analysis is only relevant if employees have recognized privacy expectations in the workplace. In 1965, the United States Supreme Court determined, in *Griswold v. Connecticut*,\(^8\) that there was a right of privacy protected by the Constitution. This case held that a Connecticut contraceptive statute was unconstitutional as applied to a married couple.\(^9\) One characteristic which distinguishes this precedent from the privacy issues related to electronic mail is that *Griswold* considered the physical intrusion of the government into the home,\(^10\) whereas unauthorized access to an electronic

---

(1989), which is a direct state enactment of the federal Electronic Communications Privacy Act. The fact that such an enactment was necessary supports the concern that smaller companies are not covered by the federal law. See supra text accompanying note 50.

55. The jurisdictions which have not enacted a computer crime statute are: Arkansas, District of Columbia, Maine, Vermont and West Virginia. SMITH, supra note 51, at 2.

56. SMITH, supra note 51, at 8-9.

57. SMITH, supra note 51, at 2.

58. 381 U.S. 479 (1965).

59. Id. at 482-85.

60. Id.
mail system may occur from many locations which do not involve an actual physical intrusion.

In an analogous area of search and seizure, the Court held that an actual physical intrusion was not necessary to violate the Fourth Amendment, \(^61\) thus opening the door to challenge violations of privacy in a non-physically intrusive context. Another aspect of this recently developed right is that it only applied to federal or state government. \(^62\) Accordingly, Fourth Amendment privacy rights will not apply to the variety of situations in which the principal actor is not a governmental body, although it will apply to public employees and possibly to some government contractors whose activities may be viewed as state action.

In addition to the federal right to privacy, twenty-four states have either included privacy in their constitutions or have enacted statutory privacy rights. \(^63\) These privacy rights

---


62. Id.

The area of prisoners' rights to their mail may also provide an interesting analogy, although it is also limited to areas involving state action. Initially, mail censorship was considered part of incarceration, and valid unless it resulted in restricted access to the courts. Prewitt v. Arizona, 315 F. Supp. 793 (D.C. 1969). Gradually, however, the courts began to recognize that prisoner mail censorship interfered with the First Amendment rights of the addressees and began to afford more protection. Proctor v. Martinez, 416 U.S. 396 (1974). Inmates were allowed to retain their First Amendment rights to the extent that those rights were not inconsistent with their status as a prisoner or the legitimate penological objectives of the correctional system. Pell v. Procunier, 417 U.S. 817 (1974).

Prisoners eventually received protection similar to civilians, when the Court held that censorship of correspondence must be reasonably related to a legitimate penological interest. Turner v. Safley, 482 U.S. 78 (1986). In evaluating this test, the Court looked at factors including the valid, rational connection between the regulation and the asserted penological interest; the lack of a viable, less burdensome alternative; the impact on guards and others in the institution; and the availability of alternate methods of expression. Id. at 89-90.

This progression shows that interference with the recipient's right to receive the information must be considered in conjunction with the rights of the sender. It also indicates the willingness of the courts to recognize free speech rights of individuals who do not have complete control of their environment, as is the case in the employment context.

63. The states which do not have such an enactment are: Alabama, Arkansas, Colorado, Connecticut, District of Columbia, Idaho, Indiana, Iowa, Kansas, Maryland, Michigan, Minnesota, Mississippi, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oregon, South Dakota, Texas, Vermont, West Virginia, and Wyoming. Smith, supra note 51, at 2.
vary greatly, ranging from general rights to the recognition of specific civil causes of action for invasion of privacy.\textsuperscript{64}

An example of a general right of action is found in the California Constitution, which declares: "All people are by nature free and independent and have certain inalienable rights. Among these are ... pursuing and obtaining safety, happiness, and privacy."\textsuperscript{65} The scope of this provision has been interpreted at least as broadly as the U.S. Constitution.\textsuperscript{66}

In \textit{White v. Davis},\textsuperscript{67} the California Supreme Court found that the provision creates a "legal and enforceable right of privacy for every Californian."\textsuperscript{68} In dictum, the court found that this constitutional provision encompasses both state and private action in California.\textsuperscript{69}

The courts have also applied this privacy right in the area of employee drug testing by private employers.\textsuperscript{70} With respect to private employees, however, the right is not absolute; rather, it is affected by a variety of factors such as the level of intrusiveness, adequacy of notice, purpose of the intrusion and the relationship of the parties.\textsuperscript{71} If the right is not substantially burdened, the countervailing interest must only be reasonable, not compelling.\textsuperscript{72} None of the drug testing cases found that the testing offended the employees' reasonable expectations of privacy.\textsuperscript{73}

Many other states, however, are not so generous in their recognition of privacy rights. Some states proclaim a general right, but then limit its application to governmental intrusion.\textsuperscript{74} Other states settle for a statutory recognition of tort

\textsuperscript{64} SMITH, supra note 51, at 28-29.
\textsuperscript{65} CAL. CONST. art. 1, § 1 (repealed and amended 1974).
\textsuperscript{66} SMITH, supra note 51, at 28-29.
\textsuperscript{67} 533 P.2d 222 (Cal. Sup. Ct. 1975) (holding that police surveillance of college classrooms violates the newly-enacted right of privacy).
\textsuperscript{68} Id. at 233.
\textsuperscript{69} Id.

\textsuperscript{71} Wilkinson v. Times Mirror Corp., 264 Cal. Rptr. 194 ( Ct. App. 1989).
\textsuperscript{72} Id.

\textsuperscript{74} "Every natural person has the right to be let alone and free from gov-
causes of action, without declaring a broad right. In addition to rights to privacy, many states have enacted provisions protecting citizens from unreasonable searches and seizures absent a showing of a compelling state interest. As state enactments, they are more likely than federal provisions to apply to private employers.

3. Common Law Tort: Intrusion Into Seclusion

The common law tort of invasion of privacy was first presented in a law review article by Samuel Warren and Louis Brandeis in 1890, in response to what they saw as the pervasive intrusion of the media into the personal lives of the residents of Boston. Although one of the first cases considering the concept of personal privacy rejected the notion, it was recognized by a state supreme court in 1905. The concept was first considered by the United States Supreme Court in Olmstead v. United States, where the idea was rejected over the strong dissent of Justice Brandeis, the author of the earlier article.

By 1960, over 300 cases had considered the right of privacy. Dean Prosser summarized the right in a four-part scheme; this scheme included (1) intrusion into a person's seclusion or solitude, (2) public disclosure of private facts, (3) publicity which places a person in a false light in the public eye, and (4) misappropriation of a person's name or like-


75. See OKLA. STAT. tit. 21, § 839.1 (recognizing the "misappropriation" right of action).

76. SMITH, supra note 51, at 28-29.


81. 277 U.S. 438 (1927).

82. Id. at 478 (Brandeis, J., dissenting).


84. Id.
ness.\textsuperscript{85} Shortly thereafter, these classifications were included in the American Law Institute Restatement of Torts.\textsuperscript{86}

Of the enumerated causes of action, the unreasonable intrusion into a person's seclusion presents the clearest path for analysis with respect to electronic mail.\textsuperscript{87} This action requires that the plaintiff prove that his solitude or seclusion was intentionally intruded upon, and that the intrusion would be highly offensive to a reasonable person.\textsuperscript{88} It does not require that the invasion be physical, rather, it may be by wiretapping or viewing another through a window.\textsuperscript{89} However, that which was intruded upon must have been private,\textsuperscript{90} thus leading again to a consideration of the reasonable expectation of privacy in the system.\textsuperscript{91} In an analogous area, reasonable expectations of privacy were found in the contents of personal mail.\textsuperscript{92}

There appears to be a trend with respect to the means employed and purposes of the intrusion in the practical application of the doctrine.\textsuperscript{93} For example, if the character of the means used is highly offensive, such as the use of electronic surveillance techniques, the court is more willing to find the intrusion actionable.\textsuperscript{94} Accordingly, as more confidential information is stored on computer systems, courts may increasingly find that intrusion into clearly confidential areas is actionable.


\textsuperscript{86} RESTATEMENT (SECOND) OF TORTS § 652A (1977) [hereinafter, \textit{RESTATEMENT}].

\textsuperscript{87} This statement presumes that the information obtained from the electronic mail system is not disclosed to the public. Were that the case, other causes of action could be used. In any event, the cause of action for misappropriation of name or likeness is not appropriate, in that the name or picture of the user were not taken.

\textsuperscript{88} RESTATEMENT, \textit{supra} note 86, § 652B.

\textsuperscript{89} RESTATEMENT, \textit{supra} note 86, § 652B cmnt. a.

\textsuperscript{90} PROSSER & KEETON, \textit{supra} note 85, at 855.

\textsuperscript{91} See \textit{supra} notes 61-77 and accompanying text.

\textsuperscript{92} Vernars v. Young, 539 F.2d 966 (2d Cir. 1976). \textit{See also} Cruikshank v. United States, 467 F. Supp. 539 (D. Haw. 1979) (damages awarded to an astronomer when CIA agents opened nineteen sealed envelopes to and from the Soviet Union).

\textsuperscript{93} PROSSER & KEETON, \textit{supra} note 85, at 856.

\textsuperscript{94} PROSSER & KEETON, \textit{supra} note 85, at 856.
As a tort, the action for intrusion into seclusion is subject to the defense of consent.\textsuperscript{95} If the plaintiff consents to an unreasonable intrusion, the cause of action will not accrue, because its nature would no longer be unreasonable.\textsuperscript{96} Thus, the plaintiff may be required to show lack of consent as part of the cause of action.\textsuperscript{97} Defendant's actual good-faith belief that consent has been given is generally not a defense, although it may mitigate punitive damages.\textsuperscript{98} In some instances, the defendant may have a qualified right to intrude in order to protect its own interest.\textsuperscript{99} The subject matter involved in the intrusion also acquires constitutional protection if it is a matter of general public concern.\textsuperscript{100}

In summary, both federal and state wiretapping statutes may cover the area of electronic mail. In addition to these concerns, there are serious constitutional, statutory and common law privacy implications which may interfere with unqualified business access into the mail systems of its employees.\textsuperscript{101}

III. Analysis

In examining potential statutory coverage, the main federal statute in the area, the Electronic Communications Privacy Act,\textsuperscript{102} will be analyzed in conjunction with the California wiretapping statute.\textsuperscript{103} The effect of various privacy considerations in the employment context must then be determined in developing the effect of privacy\textsuperscript{104} and common law tort.\textsuperscript{105}

\begin{itemize}
\item \textsuperscript{95}PROSSER \& KEETON, supra note 85, at 867.
\item \textsuperscript{96}PROSSER \& KEETON, supra note 85, at 867.
\item \textsuperscript{97}PROSSER \& KEETON, supra note 85, at 867.
\item \textsuperscript{98}PROSSER \& KEETON, supra note 85, at 867.
\item \textsuperscript{99}PROSSER \& KEETON, supra note 85, at 868. See also, Schmuckler v. Ohio-Bell Tel. Co., 116 N.E.2d 819 (Ohio C.P., Cuyahoga County, 1953) (telephone company may monitor telephone calls); Thomas v. General Elec. Co., 207 F. Supp. 792 (W.D. Ky. 1962) (efficiency studies of employees permitted); University Heights v. Conley, 20 Ohio Misc. 112 (Sup. Ct. 1969) (city may spy on suspected thief).
\item \textsuperscript{100}Time, Inc. v. Hill, 385 U.S. 374 (1967).
\item \textsuperscript{101}Many jurisdictions have recognized a tort of wrongful discharge when that discharge is in contravention of public policy. Payne v. Rozendaal, 520 A.2d. 586 (Vt. Sup. Ct. 1986); Harles v. First Nat'l Bank, 246 S.E.2d. 270 (W. Va. Sup. Ct. 1978). In the context of electronic mail, such a public policy may be seen in the violation of the employee's privacy, or violation of a state or federal wiretapping statute. See infra notes 108-40 and accompanying text.
\item \textsuperscript{102}See infra notes 107-29 and accompanying text.
\item \textsuperscript{103}See infra notes 130-40 and accompanying text.
\item \textsuperscript{104}See infra notes 141-42 and accompanying text.
\end{itemize}
Finally, a variety of business options are presented, which would allow businesses to take an active role in protecting their interests.106

A. Statutory Analysis

1. Electronic Communications Privacy Act

As discussed above,107 one of the most likely areas for coverage is the Electronic Communications Privacy Act of 1986, which forbids any person from intentionally intercepting any wire, oral or electronic communication.108 Although electronic mail would not be considered a wire or oral communication,109 it would be considered an electronic communication.110

To fall within the parameters of the Act, the interception must be intentional, resulting from the interceptor's conscious objective.111 Thus, a person who intentionally intercepted an electronic mail transmission would be in violation, while one who inadvertently stumbled into the wrong electronic mail box would not.112 Under the Act, the contents may be intercepted by "any electronic, mechanical, or other device."113

There are, however, a variety of exceptions to the operative section of the Act. One exemption which applies to private corporations allows any person to intercept an electronic communication which is readily accessible to the general public.114 Although "readily accessible" is defined elsewhere in

105. See infra section III.B.
106. See infra section III.D.
107. See supra notes 42-57 and accompanying text.
109. SENATE REPORT, supra note 47, at 12.
110. "Communications consisting solely of data, for example, and all communications transmitted only by radio are electronic communications. This term also includes electronic mail, digitized transmissions, and video teleconferences." SENATE REPORT, supra note 47, at 14.
111. SENATE REPORT, supra note 47, at 23.
112. SENATE REPORT, supra note 47, at 23.
113. 18 U.S.C. § 2510(4) (1988). This includes any device which can intercept a wire, oral or electronic communication other than any tracking system used by a commercial electronic mail service provider, or devices similar to a hearing aid. Id. § 2510(5).
114. Id. § 2511(2)(g)(i). It is not unlawful for any person "to intercept or access an electronic communication made through an electronic communication
1992] EMPLOYEE RIGHTS TO ELECTRONIC MAIL 181
terms of radio communication, it does not appear to be limited to that medium. Such an exemption indicates that the type of system used affects the applicability of this statute to the company in that communications on a bulletin-board system with wide user access may be intercepted with impunity.

Another exemption under the Act allows the owners of electronic mail systems, not limited to commercial services, to use a pen register or trap and trace device in order to monitor system use. It also allows commercial service providers to record the fact that a communication was initiated or completed for the company's protection. Another exception which may apply to private businesses states that it is not unlawful for an employee of a commercial electronic mail service to intercept transmissions in order to protect the property interests of the company. Likewise, such electronic mail service providers may access their system in support of a court order or certification by the Attorney General that such an order is not necessary.

---

system that is configured so that such electronic communication is readily accessible to the general public." Id.

115. Id. § 2510(16).

'Readily accessible to the general public' means, with respect to a radio communication, that such communication is not scrambled or encrypted transmitted using modulation techniques carried on a subcarrier or other signal subsidiary to a radio transmission transmitted over a communication system provided by a common carrier [or] transmitted on frequencies allocated . . .

Id.

116. Id. See also id. § 2511(2)(g)(i).

117. See supra notes 21-24 and accompanying text.

118. Pen registers and trap and trace devices track the origination and destination of communications flowing through them, without recording the substantive information within. 18 U.S.C. § 3127 (1988).


120. Id. § 2511(2)(i)(ii). It is not unlawful "for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider." Id.

121. Such a service is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." Id. § 2510(15).

122. Id. § 2511(2)(a)(i). It is not unlawful "for an operator of a switchboard, or an officer . . . of a provider of wire or electronic communication service . . . to intercept, disclose, or use that communication in the normal course of his employment . . . or to the protection of the rights or property of the provider of that service." Id.

123. Id. § 2511(2)(a)(ii). It is not unlawful for "providers of wire or electronic
visions apply to corporations who maintain electronic mail services for internal use only. Use of the term "service" seems to indicate an external organization providing electronic mail, especially since the term "user" is defined as a "person or entity... who uses an electronic mail service." This implies that a company which maintains an internal system would not comply with the definition of an "electronic mail service" within the Act.

The Act also exempts employees of the Federal Communications Commission working within the scope of their employment, as well as others acting under color of law or who are parties to the communication. There are also provisions exempting employees of the United States Government conducting surveillance in furtherance of national security or other foreign intelligence activities, as long as it is conducted according to federal law.

Thus, although the statute does provide for limited exceptions, few are likely to shield the corporation from the potential penalties for violation of the Act, which penalties are extensive and severe. Businesses may also be subject to concurrent regulation by state wiretapping statutes, which may limit their access to the electronic mail system.

2. State Wiretapping Statutes

State and federal wiretap laws may provide an area of protection for electronic mail systems because the policies...
involved are similar and because electronic mail messages travel through phone lines. The general purpose of wiretap statutes is to protect the confidentiality and privacy of telecommunications.\textsuperscript{130} Thus, the policy of wiretap laws is similar to that of the Electronic Communications Privacy Act, which seeks to prevent unauthorized interception of personal or proprietary communications of others.\textsuperscript{131} Since the messages are transmitted by wire, the potential coverage by wiretap laws becomes more clear.\textsuperscript{132}

In California, for example, wiretap law makes it illegal for any person to make an unauthorized connection with any telegraph or telephone wire, line or cable, or to read a message while it is in transit over such a wire.\textsuperscript{133} The law does not apply, however, where one of the parties to the conversation consents to or directs the eavesdropping.\textsuperscript{134} The statute provides for a maximum penalty of $2,500 and one year in prison for the first offense.\textsuperscript{135} The exceptions protect public utilities and correctional facilities.\textsuperscript{136}

Although the cases citing the statute all involve the wiretapping of telephone lines, it may be held applicable to electronic mail and computer communications which are transmitted through the same telephone wires that were the original subject of the statute. Since electronic messages are not oral but are transmitted manually via the computer keyboard, they are very similar to telegraphic communications, which are specifically mentioned in the statute. A modern court may find the law applicable to such emerging technologies as electronic mail, which are analogous to those named in the statute. Thus, employees' messages may be protected by statutes not originally designed to apply to computerized communication.

A similar California law prohibits the eavesdropping or recording of confidential communications, making it illegal to intentionally amplify or record confidential discussions without

\textsuperscript{130} People v. Trieber, 171 P.2d 1 (Cal. 1946).
\textsuperscript{131} See supra note 47.
\textsuperscript{132} See supra notes 51-54 and accompanying text.
\textsuperscript{134} People v. Canard, 65 Cal. Rptr. 15 (Ct. App. 1967), cert. denied, 393 U.S. 912 (1968).
\textsuperscript{136} Id. § 631(b).
the consent of all parties.\textsuperscript{137} This law is not restricted to wire-based communication, and may even be more applicable to electronic mail than wiretap statutes. The law does not, however, include communications made in a public gathering or in a proceeding open to the public, or in any other circumstance where the parties may reasonably expect to be overheard,\textsuperscript{138} and may therefore provide little protection to bulletin-board systems which allow for general access. Like the wiretap statute, public utilities and correctional facilities are exempted.\textsuperscript{139}

Both of these statutes allow for a civil cause of action, which provides recovery of $3,000 or three times plaintiff's actual damages.\textsuperscript{140} This section provides employees with the statutory authorization to bring suit and a financial incentive to do so. The statutes may therefore be particularly attractive to employees who feel that their workplace privacy has been violated.

B. Expectations of Privacy

Critical to an analysis of the employees' right to privacy is the determination of their expectation of privacy in the messages within the system.\textsuperscript{141} Because most systems generally limit access to those who provide personal passwords or numbers, many employees will have a subjective expectation of privacy in their use of the system, notwithstanding the fact that the computer is owned by the company. Because a subjective expectation of privacy on the part of the employees is likely, a determination of its reasonableness is necessary to evaluate the measures that a corporation may use to protect itself.

In determining whether this expectation is reasonable, this author believes a court should consider a variety of factors in reviewing the specific employment environment. The first con-

\begin{itemize}
    \item 137. Id. § 632(a).
    \item 138. Id. § 632(c).
    \item 139. Id. § 632(c).
    \item 140. Id. § 637.2 (West 1988).
    \item 141. In O'Connor v. Ortega, 480 U.S. 709 (1987), the court recognized that a public employer must remove the expectations of privacy before searching an employee's desk, and if it failed to do so, the employer needed a reasonable suspicion that he would find something in the desk before he could invade the employee's privacy with the search. Id.
\end{itemize}
Consideration should be the level of notice the employee received that a search was to take place and that access to the system was possible by company management. This level of notice is completely within the control of the employer, although it may decide not to provide notice in order to obtain a more revealing search. The amount of notice that is required might depend in turn on the level of probable cause that has led the employer to believe that objectionable material is contained within the system. Where the search is specific and the finding of probable cause is corroborated, a court is more likely to find the search reasonable, especially if the potential business loss is substantial.

A second factor which should be considered is the type of system involved. Systems which allow employees access only upon the provision of an employer-provided password may create less of an expectation than systems which allow the employee to create personalized passwords and change them at any time. The court will also look at the general structure of the system itself. For example, a bulletin-board type system which allows all users to view all messages creates extremely little expectation that each of the messages will be kept confidential; whereas a system which allows users to send their messages only to selected recipients, or which allows users to designate which messages are confidential, creates a much greater expectation of privacy.

The general work environment should also affect the reasonableness of an employee's privacy expectation. Employees who work in high-technology companies will have less of an expectation of privacy in their electronic messages, because they are exposed to an environment where programs are designed to limit computer access and potential for access is discussed. On the other hand, employees working in a general business environment may be unaware of the potential for system abuse, so their expectation of privacy may be viewed as more reasonable. Likewise, the employee's personal level of technical expertise should be considered. Technologically sophisticated employees will know the faults of the system, and how the faults may be exploited, and will therefore have a lower subjective expectation of privacy.

Finally, the court should consider the wording of corporate policies which may be applicable to the electronic mail sys-
tem, if any such policies are in place. These policies may either require notice prior to employer access, or create an expectation that no employer access will occur. If such a policy exists, it will determine the reasonableness of the privacy expectation at the outset of the inquiry.

C. Intrusion Into Seclusion

Closely related to a finding of the reasonableness of the employee’s expectation of privacy is the determination as to whether the intrusion was unreasonable for purposes of the tort cause of action. In this context, “unreasonable” is defined as a circumstance which would be highly offensive to a reasonable person. In considering this element, this author believes that a court is likely to look directly at the expectation of privacy or confidentiality of the employee, as determined above. Another consideration should be the method of intrusion. Employers who give notice of a search and then use the central system to access messages will be less invasive than those who do not provide notice or who use an employee’s personal terminal to access the system. Likewise, a court is unlikely to look favorably upon employers who tap into the wires or modems of employees using the system in order to view the messages.

The court should also evaluate the employment context in general. The factors here are the type of system used, the fact that the employer is the owner of the system, the level of access which the employer has retained through internal policies, and the type of information typically transmitted through the system. These considerations are very close to those used in determining the reasonable expectation of privacy, so it is likely that a court which finds such an expectation exists will also find that intrusions would be highly offensive to a reasonable person.


143. “The form of invasion of privacy covered by this Section ... consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.” Restatement, supra note 86, § 652B cmt. a.
D. *Business Protections*

1. *Corporate Policy*

As discussed above, company policies will have a controlling effect in determining the reasonableness of the employees' expectation of privacy. It is, therefore, in an employer's best interest to develop and implement a corporate policy which clearly defines the permissive uses of the system, the appropriate search procedure, and how information obtained from searches may be used.

A main focus of the corporate policy should be to provide clear and accurate notice of the permissive use of the system, thereby defining the expectation of privacy which will be allowed. To ensure that each employee receives the notice, the company policy should be provided when the employee's system is loaded, and the policy should be explained along with other aspects of the system during the training session. The employer may also want to provide periodic follow-up notices to employees, in order to assure that each employee is well informed. This may occur either through a dialogue box which flashes onto the screen at intervals, or preferably by use of a message to which the employees must respond before they are allowed access onto the system. The follow-up may be provided on a monthly or even weekly basis.

The policy should clearly explain that, notwithstanding the company's interest in protecting the system, it should be remembered that the system may be accessed by those outside the company. The company should also reserve a property right in the system, so that it may obtain statistical information on the system or access the system to protect company interests. Employees should also be informed that they have no right to the contents of their electronic mail systems once their employment has been terminated. This will allow the employer to clear and delete unused sections, thus enabling the system to work faster because more memory is available and also protecting it from outside intrusion.

The policy should likewise outline the permissive or suggested uses of the system. For example, the company may want to limit the system to business use and disallow transmission of personal information. In any event, the system should only be used for non-confidential personal information because of the
potential for access. The system may similarly be used for non-confidential business memoranda. However, the company should strongly discourage use of the system to discuss any sensitive information, such as pricing statistics, trade secrets, or major business decisions.

The company should also outline the methods by which the system will be searched. For example, the company should provide reasonable actual notice of the search of a specific mailbox. This notice may inform the employee of a fixed time for the search, or merely state that searches will take place in the future, thus informing the employee that the contents of his or her system are under suspicion. Similarly, the company should be required to provide reasonable notice of a blanket search of all systems, since they may not have probable cause to search any given location. This notice should define the scope and breadth of the search to inform employees of exactly what type of information interests company management. Only a limited number of designated company officers should be authorized to conduct the search, thus ensuring that the search will follow company guidelines.

Corporate policy should also consider how the information obtained from the search may be used. The company may want the messages to be used in any manner consistent with the company's interests, or it may want their use to be subject to additional limitations. Likewise, the information should only be used consistently with the announced scope and breadth of the initial search. The corporation may also allow the information to be published for the public or other employees only upon a showing of a legitimate need to know the information.

By creating a clearly defined corporate policy regarding the proper use and access to the electronic mail system, companies will greatly improve their position in any potential litigation.

2. Physical Controls

Another important element in safeguarding the system is for businesses to institute proper physical controls over the computer system itself in order to protect it from unauthorized access.144 The company may want to require an addi-

144. For a synopsis of the various methods of computer access control, see
tional password to access the electronic mail system in addition to the password combinations used to log onto the computer system. Unfortunately, passwords may not deter all determined intruders.145

A more secure method of physical control is to develop a system of changeable security codes.146 Under this type of system, users are provided with a series of codes which they are required to enter before obtaining access.147 In some systems, users are allowed to use the code only once, and are then required to move to the next in the series.148 The problem with these types of access controls is their difficult administration. The business should also take care that the codes are protected once created, such that they may not be misappropriated or misused.

A final type of system asks each user to create and memorize a secret number, and the computer then asks for random digits of that number.149 However, this type of system may allow easier access to others because of the tendency of users to create numbers which they will easily remember, such as their birthday or phone number. Thus, the system must be kept simple in order to allow ease of use in addition to maintaining control.

An integral part of securing the system is to ensure the physical security of the terminals and lines in the system. Care should be taken to keep the central processing unit in a locked, alarmed location. Likewise, all computer lines and switching boxes should be kept locked and secure, and should

JAMES MARTIN, SECURITY, ACCURACY AND PRIVACY IN COMPUTER SYSTEMS (1973). See also Joseph M. Howin, Jr., Protecting Work Product, CAL. LAWYER, Feb. 1989, at 57-60; Miriam Liskin, Protecting the Corporate Database, PERSONAL COMPUTING, Aug. 1989, at 51 (discussing the importance of computer security, especially to LAN users).

For an excellent discussion of encryption devices, see JAMES HANNAN, A PRACTICAL GUIDE TO DATA COMMUNICATIONS MANAGEMENT, 105-08 (1982). See also Stan Miastkowski, Put a Positive Lock on your Data, BYTE, Feb. 1989, at 100 (describing the importance and use of a low-cost encryption device).

145. MARTIN, supra note 144, at 137.
146. MARTIN, supra note 144, at 138. Employees should avoid using English words in their passwords, and should use as many characters as possible, including letters, numbers and symbols. Malcolm Ritter, Making Computer Passwords Guess-Proof, S. F. CHRON., March 18, 1991, at B14.
147. MARTIN, supra note 144, at 138.
148. MARTIN, supra note 144, at 139-40.
149. MARTIN, supra note 144, at 140.
be examined regularly. Companies in which the system is likely to be used to transmit sensitive or confidential data may also consider scramblers and other encrypting devices to provide extra security.

3. Administrative Controls

As a final method of ensuring the security of the system, businesses should institute administrative controls over the computer system which predetermine those responsible for policing the system and the acceptable methods to accomplish this task. The number of administrators with system-wide access should be strictly limited. In larger organizations, executives should divide the responsibility of system-wide access so that it takes two system managers’ passwords to enter. Another aspect of administrative control is the implementation of an electronic mail policy as discussed above.

Thus, by implementing a company-wide policy, caring for the physical security of the system and limiting executive and managerial access, many corporations will be able to avoid unauthorized access, and if it happens, will be better able to apprehend those who have done so.

It appears, in summary, that both the Electronic Communications Privacy Act and state wiretapping statutes may apply to electronic mail systems, depending on the application of statutory exceptions to the employment environment. A court may also consider an extensive series of factors to determine whether the employee has a reasonable expectation of privacy in his or her electronic mail messages, and the outcome of these factors will therefore depend on the specific context. There are also a variety of steps that businesses can take to limit their potential liability. However, the factual determinations required by the levels of legal analysis make it more difficult for businesses to comply with the law and make employees’ rights less clear. It is therefore necessary to consider a variety of business and legal options which may clarify the situation.

150. MARTIN, supra note 144, at 335-41.
151. MARTIN, supra note 144, at 334.
152. MARTIN, supra note 144, at 351-56.
IV. PROPOSALS

There are two primary ways that employees' electronic mail messages may be protected in a manner that will provide adequate protection of employer interests. The first is for businesses to take proactive responsibility for ensuring message confidentiality by providing corporate policies outlining the proper use and potential misuse of the electronic mail systems, by purchasing computers with physical and system controls which ensure confidentiality, and by instituting administrative controls over access to the system, as discussed above. A more effective route, however, is for the legal and legislative systems to provide direct clarification of the area through an interpretation of the Electronic Communications Privacy Act which encompasses electronic mail, the reconsideration of the allocation of the burden of proving that an unauthorized search was made, or the creation of a new statute which directly addresses the issue.

A. Corporate Policy

The goal of a corporate policy is to determine the reasonableness of the employees' expectation of privacy, while allowing the employer to search the system as is necessary to ensure the smooth operation of the business. An example of an appropriate corporate policy would read as follows:

Welcome to the company electronic mail system. This system is designed to facilitate your communication with other employees with respect to your non-confidential business and personal memoranda. Since no computer system is completely secure, and may be accessed by those outside the company, the system is not intended to transmit sensitive or confidential material such as pricing information or trade secrets.

The company reserves the right to search the contents of the system in any manner consistent with state and federal law, in order to protect its business interests. Employees will receive actual notice, twenty-four hours prior to any search, unless the company has cause to believe that such notice will result in the destruction of information or company property.

In the event of contradiction between this policy and any statement made to you by your supervisor or any oth-
er company representative, this policy governs. This policy may be changed only upon the written approval of the company president. Employees will be notified of any policy changes.

This policy clearly defines the intended uses of the system. It also notifies the employees of the possibility that the system may be accessed by persons unaffiliated with the company, and that the company reserves the right to search the system when necessary. It clearly states that the policy may not be changed unilaterally by the statements or actions of supervisors. In other words, employees other than the president cannot modify these terms in any way. The policy therefore protects businesses from potential policy alterations and potential liability for searching the system.

B. Statutory Clarification

Although it may be in the best interests of all businesses to take proactive steps to protect themselves from liability and their employees from unwarranted intrusion, a large number of smaller businesses will not be technologically sophisticated nor well-informed enough to do so. The legal system must therefore endeavor to provide a sufficient response by clarifying the application of the Electronic Communications Privacy Act to include electronic mail systems, by reallocating the burden of proof in a manner which fairly protects the interests of those involved, or by developing a new statute to cover electronic mail systems.

1. Electronic Communications Privacy Act Analysis

Perhaps the easiest and most straightforward way to ensure statutory coverage of the area of electronic mail is through a judicial interpretation of the Electronic Communications Privacy Act which considers the needs of both employers and employees.\(^{153}\) This may be accomplished by allowing the operative section of the Act to apply, thereby protecting the electronic mail systems from intentional interception,\(^{154}\) while allowing employers access through one of the exceptions.

\(^{153}\) See supra notes 107-28 and accompanying text.
\(^{154}\) See supra notes 110-12 and accompanying text.
The Act allows access to the systems in order to protect the company's interests. This exception may provide the clearest protection of business interests. Before this exclusion applies, however, the court would need to determine that the company, who is the owner of the system and provides it to the employees, fits the definition of a "electronic communication service, whose facilities are used in the transmission of a wire communication." Employee interests could be protected by a strict interpretation of business interests, such that searches are disallowed in cases where the corporate interests are small.

The major problem with using a judicial interpretation of the Act to cover the entire area of electronic mail system protection is that it does not clarify when searches may be made and what notice must be provided to employees prior to a search. A better method of clarifying the coverage of the area would therefore be to either shift the burden of proof or enact a new statute which clearly identifies the rights and responsibilities of all parties involved.

2. Shift Burden of Proof

A somewhat more interventionist approach than reinterpreting the current statute is to shift the burden of proving that the system was not private. An interpretation of the Electronic Communications Privacy Act which encompasses electronic mail, as described above, still places the burden of proving all elements of the claim on the employee. Another option is to look at the underlying social policy of protecting the privacy of the employees in the workplace. This policy would require that the burden be placed on the corporation to show that the specific type of system was not private; in other words, presume that the system is private unless it is shown otherwise.

Although the employer is the owner of the system and may therefore have a proprietary interest in its use, it is also the party with the most control. The corporation determines which system is purchased, and thus may decide how confidential the system is initially. The company can easily provide

156. Id.
notice to employees of impending searches and can outline the scope and breadth of the search in advance.

Because current and incoming employees will need to be trained on the use of the system, the employer has an easily-available opportunity to explain what type of information should be sent on the system and under what circumstances the company reserves the right of access. The company may require the system to flash a warning on the screen if a random search is to be conducted, or use a recurring message to outline the company policy regarding such searches.\(^5\)

In addition to shifting the burden to the party with the most control over the system, such a shift would fulfill the policies of the Electronic Communications Privacy Act by limiting the situations in which the systems are invaded.\(^7\) Thus, perhaps the clearest available option would be to place the burden of disproving privacy on the employer, thus protecting employees' privacy rights while allowing the business to search the system when its interests are compelling.

3. New Statute

In order to increase the clarity of a new scheme covering electronic mail systems, a new statute could be written which incorporates the public policies set forth in the Corporate Policy section above. The goals of such a statute would be to provide clarification of the area, enabling businesses to proactively protect their rights and the rights of their employees. It would seek to protect business property and proprietary interests while at the same time ensuring the confidentiality of employee communications. It would also attempt to provide a method of efficient, easy enforcement.

\(^{157}\) For example, prior to logging onto the system each week, employees could be required to acknowledge a message which states the company policy with regard to random or for-cause searches of the employee electronic mail boxes. This would provide a periodic reminder to employees that they should not expect their messages to be kept confidential. It would also allow employees with confidential messages to clear them from the system prior to a search.

a. Text of Proposed Statute

This comment proposes a statute which would read as follows:

A. Terms and definitions. As used in this chapter:
1. "covered person" means any corporation, business entity or organization, whether or not for profit, or any employee or agent of such an entity, which has a computer system which allows or provides for an electronic mail system;
2. "user" means any person who is authorized by his employer to use or access an electronic mail system;
3. "electronic mail system" means any computer or electronic system which allows communication among terminals within the system or with external systems;
4. "contents," when used with respect to any electronic mail system, includes any information concerning the substance, purport, address, location or meaning of that communication.

B. Provisions: except as provided in this chapter:
1. it shall be unlawful for any covered person to access the electronic mail system of any other user;
2. it shall be unlawful to print, publish, display or use in any manner any information obtained in an authorized search inconsistent with the announced purpose of the search, inconsistent with the legitimate property or proprietary interests of the covered person, or to any person without a legitimate need to know the information;
3. it shall be unlawful to print, publish, display or use in any manner any information obtained from an unauthorized search;
4. each covered person shall, upon providing authorization for a user to access the electronic mail system, provide users with a written description of their rights and the company policies regarding use of the electronic mail system, and shall provide a similar notice to all users on a regular basis not less than once per year.

C. Exceptions: notwithstanding any other provision in this chapter, it shall not be unlawful for a covered person to:
1. make a system-wide search of the electronic mail system after providing a notice to all users at least one working day before the search, describing the reason for the search, its method and those authorized to make the search;
2. make an immediate search of a specific user location upon a determination of good cause to justify the lack of notice in order to protect legitimate business interests;
3. clear the system on a regular basis, only after providing 24-hour notice to all users.

D. Penalty and damages:
1. whoever violates this chapter shall be fined or imprisoned not more than five years, or both;
2. any user 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 covered person which engaged in that violation such relief as may be appropriate, equal to the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case less than $1,000;
3. any user 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 addition to other damages, recover attorney fees. 159

E. Defenses: good faith reliance on:
1. a court warrant or order, a grand jury subpoena, a legislative or other statutory authorization;
2. the request of an investigative law enforcement officer; or
3. a good faith determination that section A permitted this conduct is a complete defense to any criminal or civil action based upon this chapter. 160

159. See id. §§ 2511(4)(a), 2707 (providing substantially similar penalties and damages). See also supra note 128 and accompanying text.
b. *Operation of Proposed Statute*¹⁶¹

The coverage for this statute would be broad, so as to include businesses possibly not covered by the Electronic Communications Privacy Act.¹⁶² It would thus include any corporation, business entity, or organization which has a computer system allowing for communication among terminals within the system or with external systems. This language would cover all electronic mail systems utilized in the business, commercial, educational and other settings.

After showing that the employer was covered, the statute would then require that the employer provide its employees with a notice outlining the company policy regarding system searches and the use of the information obtained, and warning employees that the system may be accessed. With respect to searches, the statute would provide that employers may search where they have good cause to believe that information will be found affecting the pecuniary or proprietary interests of the company. It would also allow the employer to clear the system on a regularly scheduled basis, with prior notice to employees. It would likewise allow employers to search and close terminals of recently terminated employees. Such requirements would protect business interests and allow proper system upkeep, while disallowing random searches or those without probable cause.

Information obtained from the searches would then be used only for the pecuniary interests of the company. It could not be published, or relayed to other employees or the public without a legitimate reason to know the information. Such a legitimate reason may include knowledge necessary for the performance of an employee’s regular job duties. The statute would also allow the information to be used in any relevant proceeding, providing that the procedures provided by the statute were followed.

The new statute would provide for damages similar to the Electronic Communications Privacy Act, allowing a corporate criminal remedy in addition to civil damages presumed to be

---

¹⁶¹ This section could be included as a comment to the statute, as in the Uniform Commercial Code.
¹⁶² See supra notes 52-54, 113-27 and accompanying text.
no less than $1,000. By allowing for minimum penalties even in the civil context, the statute would acknowledge the difficulty in proving special damages in this context. In addition, the prosecuting party may receive attorney fees if the violation is willful, thus providing an incentive to bring suit. To provide these remedies, the statute would provide for prosecutorial enforcement and would authorize a personal civil cause of action for the employees. In the alternative, the statute may allow another organization, such as the Equal Employment Opportunity Commission, to enforce the statute according to its prearranged scheme.

V. CONCLUSION

The emerging technologies create new opportunities and challenges at a rapid pace. The speed of these changes mean that statutes which were designed only years ago may not be applicable to new systems.

There is a great need for businesses to develop electronic mail policies and procedures which clearly protect the computer system and business interests, while at the same time protecting the privacy interests of their employees. Unfortunately, not all businesses which use electronic mail technology are likely to provide such programs on their own.

There are a variety of progressively interventionist statutory options to solve the problem. In addition to analyzing the Electronic Communications Privacy Act in a manner which addresses the business environment, a new statute is suggested which would clarify the regulation of electronic mail systems in the employment context. However, this statute may also fall prey to the winds of time, as new systems and technologies emerge. Thus, perhaps the most long-lasting change would be to reevaluate the burden of proving unwarranted intrusion into the computer systems in an employment context. Such a change could be easily applied to new technologies as they arrive in the employment environment, thus providing a clarification of both employee and business protections.

Michael W. Droke

163. See supra notes 44-46 and accompanying text.