University of Miami Law School
Institutional Repository

University of Miami Business Law Review

4-1-1996

Employment Law Implications in the Control and Monitoring of E-mail Systems

Christopher S. Miller

Brian D. Poe

Follow this and additional works at: http://repository.law.miami.edu/umblr

 Part of the Law Commons

Recommended Citation

Christopher S. Miller and Brian D. Poe, *Employment Law Implications in the Control and Monitoring of E-mail Systems*, 6 U. Miami Bus. L. Rev. 95 (1996)
Available at: http://repository.law.miami.edu/umblr/vol6/iss1/5

This Article is brought to you for free and open access by Institutional Repository. It has been accepted for inclusion in University of Miami Business Law Review by an authorized administrator of Institutional Repository. For more information, please contact library@law.miami.edu.

EMPLOYMENT LAW IMPLICATIONS IN THE CONTROL AND MONITORING OF E-MAIL SYSTEMS

Christopher S. Miller*
Brian D. Poe**

I. INTRODUCTION

Like the computer or fax machine, electronic mail ("e-mail") has become an indispensable tool of the workplace as one of the principal means of business communication.[1] It was recently estimated that more than 60 million workers currently communicate using e-mail in some fashion,[2] and it has been projected that more than 60 billion e-mail messages will be transmitted in the year 2000.[3] Most private employers have recognized the need to ensure the proper usage of e-mail as a business resource, as well as the need to protect confidential information passed through e-mail systems. However, as a whole, e-mail technology, has evolved so rapidly that most employers have struggled to institute policies and procedures regarding the use of e-mail systems and the treatment and handling of messages created by these systems.[4] At the same time, it is estimated that one in five employers electronically monitors or "eavesdrops" on its employees' usage of e-mail[5] in order to address many of the concerns related to abuse of e-mail, including harassing or discriminating statements, defamation, and e-mail used to advance personal, religious, or political agendas unrelated to legitimate business interests.[6] The

---

* Partner, Troutman Sanders, LLP, Atlanta, Georgia. B.S. 1978, J.D. 1981, M.A. 1986, Ph.D., 1991, Syracuse University

** Associate, Troutman Sanders, LLP, Atlanta, Georgia. B.S. 1987, Florida State University; M.B.A. 1988, University of Georgia; J.D. 1993, University of Virginia

1 John K. Keitt, Jr., and Cynthia L. Kahn, *CyberSpace Snooping*, LEGAL TIMES, May 2, 1994, at 24.

2 William D. Ellis, Raymond R. Kepner, Brian F. Chase, & Thomas A. Linthorst, *Corporate Guidelines For Employee Use of E-Mail and Voice Mail*, Morgan Lewis & Bockius LLP, White Paper at 1 (Oct. 1995).

3 Scott Dean, *E-Mail Forces Companies to Grapple With Privacy Issues*, CORP. LEGAL TIMES, Sept. 1993, at 11.

4 Richard Raysman & Peter Brown, *New Federal E-Mail Guidelines*, N.Y.L.J., May 10, 1994, at 3.

5 Rosalia J. Costa-Clarke, *Workplace Technology Creates Pitfalls for Employers; On Information Superhighway, Privacy Expectations Collide*, PA. L. WEEKLY, Dec. 5, 1994, at 6.

6 Costa-Clarke, *supra* note 5, at 6.

need for employers to address their controls over an e-mail system is made more immediate by the increasing use of e-mail to communicate with the Internet[7] and the World-Wide Web.[8]

This article discusses the many reasons why employers — particularly those which electronically monitor employees' usage of e-mail — should consider implementing explicit policies concerning the appropriate and legitimate usage of e-mail in the workplace, as well as the parameters of employer monitoring of e-mail usage. Further, this article addresses the legal framework and constraints that those employers which implement such policies must consider. This includes the Electronic Communications Privacy Act of 1986 (hereinafter "ECPA"),[9] and the proposed Privacy For Consumers and Workers Act (hereinafter "PCWA"). [10] Finally, this article suggests the types of policies which employers should consider in light of this legal environment and the needs of the particular employer.

II. CONTRASTING EXPECTATIONS OF EMPLOYEE AND EMPLOYER

While nearly all e-mail systems in the workplace are paid for and developed by the employer, most e-mail systems now contain features, such as encryption[11] and/or log-in via password,[12] which may give employees an expectation or the appearance of privacy.[13] As a result, employers and employees often hold contrasting notions with respect to issues of e-mail usage, control, and monitoring.[14] The conflict in views is often exacerbated by the typical employee perspective of e-mail as more akin to a private telephone conversation than to intra-office memo writing.[15] Accordingly, the widespread use of intra-company e-mail systems has been accompanied by an

---

7 *See generally* John Perry Barlow, *What are we doing Online?; Debate on the Social Consequences of Online Communications*, HARPERS MAG., Aug. 1995, at 35.

8 *See generally* Wallys W. Conhaim, *The Internet: Accessing the Network*, LINK UP, Jan. 1995, at 5.

9 18 U.S.C. §§ 2510-2521 (1988).

10 H.R. 1900, 103d Cong., 1st Sess. (1993); S. 984, 103d Cong., 1st Sess. (1993).

11 "Encrypt" is defined as the process of "[c]onvert[ing] [data] into code, especially to prevent unauthorized access." CONCISE OXFORD DICTIONARY OF CURRENT ENGLISH 385 (8th ed. 1990).

12 James J. Cappel, *Closing the E-Mail Privacy Gap*, J. SYSTEMS MGMT., Dec. 1993, at 6.

13 *Id.* at 7.

14 *Id.* at 13.

15 *Id.*

increase in problems between employers as providers of the system and the employees as users.[16]

A. "E-mail" Defined

"E-mail" is the common term used for electronic mail, and encompasses a number of differing technologies.[17] Congress described e-mail as a service or system that allows two parties to "transmit a digital message"[18] between two computer terminals through a service provider, where it is maintained in electronic storage until accessed by the recipient.[19] E-mail system messages in the workplace can be answered, annotated, commented on, saved, converted into documents, or printed, all on the computer terminal of the user(s).[20] As a result of these state-of-the-art features, e-mail can be used to enhance a company's effectiveness by promoting efficiency, reducing paper and postage usage, playing "telephone tag," and facilitating the flow of communications between employees at all levels.[21]

For the purpose of ensuring privacy of e-mail communications, most e-mail systems in the workplace now contain password restriction and encryption of message features. For example, most multi-user computer systems require passwords to gain access to the system, and employ encryption to allow users to encode their messages so that only the intended recipient can read them.[22] In addition, most e-mail systems contain "multiple backup" capabilities by which messages stored as a file on disk to another medium are routinely performed to ensure that data will not be lost in case of system failure. Finally, it is also important to note that most e-mail systems actually store in a disk file the message that the sender types, irrespective of whether the receiver is currently logged onto the computer.[23] Employees who are unaware of such "backup" capabilities — as is often the case — will more likely feel free to abuse or misuse e-mail for personal or non-job related

---

16 John H. Shannon & David A. Rosenthal, *Electronic Mail and Privacy; Can the Conflicts Be Resolved?*, BUS. FORUM, Jan. 1993, at 31.

17 *See,* Electronic Communications Privacy Act of 1986, H.R. REP. NO. 647, 99th Cong., 2d Sess. 22 (1986).

18 *Id.* at 63.

19 *Id.*

20 Shannon & Rosenthal, *supra* note 16, at 31.

21 Cappel, *supra* note 12, at 6.

22 *Id.*

23 Shannon & Rosenthal, *supra* note 16, at 6.

purposes. At the same time, an employer who exercises control and possession over both the system and its usage, knowingly or by default takes on the responsibility and liability for system monitoring and the prohibition of illegal e-mail usage. It is this series of considerations which sets the stage for both e-mail abuse and the conflict between employers and employees over any effort to minimize such abuse.

B. Employee Expectations

As a result of the distinctive features of e-mail, as well as the fact that many employers have not developed an explicit company policy concerning e-mail usage and monitoring, employees often view their own e-mail communications in the same light as private communications via personal letter, or telephone.[24] Further, employees believe that their messages will be automatically deleted or, if not, that they have the ability to totally destroy any e-mail messages which they once created.[25] Because of these assumptions, employees frequently use e-mail for personal purposes, and in some cases use e-mail for careless, inappropriate, or offensive communication.[26]

C. Employer Expectations

E-mail systems are owned and furnished by employers, who generally invest in such systems for the sole purpose of facilitating business communications and improving individual and group performance. As a result, employers tend to view e-mail systems as being no different than any other capital equipment or processes in which they have an exclusive

---

[24] E-mail messages tend to be more spontaneous than ordinary letters. Keitt & Kahn, *supra* note 1, at 26. An illustration of a user who may not have thought carefully before he acted is a participant in the Rodney King beating, who, after the incident, broadcasted an e-mail message on the Los Angeles Police Department system stating, "Oops, I haven't beaten anyone so bad in a long time." *Id.*

[25] Keitt & Kahn, *supra* note 1, at 25, 26; *see also*, Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.C. Cir. 1993). In *Armstrong*, the court ruled that computer backup tapes containing e-mail messages created during Reagan and Bush presidencies should not be erased. *Armstrong*, 1 F.3d at 1282-87. This occurred after investigators requisitioned backup tapes from storage and used advanced technology to recover e-mail that then-Reagan White House Staffer Oliver North had attempted to erase. Robert Garcia, *Garbage In Gospel Out: Criminal Discovery, Computer Reliability, And The Constitution*, 38 UCLA L. REV. 1043, 1083.

[26] Keitt & Kahn, *supra* note 1, at 24, 26; one recent study concluded that more than forty percent of all e-mail messages sent by employees concerned nonwork-related topics. Ellis, *et al.*, *supra* note 2, at part III.

proprietary interest, such as company file cabinets or computer and information systems. Clearly, while employers encourage the use of e-mail to enhance workplace communications among employees, employers do not implement e-mail systems for the purpose of providing a network for personal or frivolous communications between employees,[27] or, in the union or union campaign setting, for the purpose of providing a ready and unobtrusive medium by which unions can communicate to employees with respect to contractual, organizational, or campaign issues.[28] Most certainly, employers concerned about compliance with equal employment statutes would not tolerate or condone using e-mail to sexually or racially harass fellow employees.

However, in light of the fact that many employers have yet to establish explicit company policies concerning e-mail usage and monitoring,[29] it is clear that those employers have failed to recognize how the implementation of e-mail systems can ultimately result in a wide range of legal liabilities for the company, concerning both the substance of e-mail communications, as well as the monitoring of such communications.

III. CURRENT LAW APPLIED TO E-MAIL POLICIES AND MONITORING

The employers' view on the nature and proper use of e-mail may be closer to the current state of the law than the employees' view. While statutory protections exist to ensure employee privacy rights (of which employers must be aware), federal law does not establish a general right to e-mail privacy in the workplace.[30] Accordingly, the current law appears to allow employers to perform e-mail monitoring regardless of whether or not they have an announced monitoring policy.[31] Only if the employer has explicitly assured employees that their e-mail will be private does the legal balance tip towards the employees in the event of litigation over monitoring.[32]

---

27 Shannon & Rosenthal, *supra* note 16, at 31.

28 *See, e.g., In re* Application of Air Line Pilots Association, 20 NMB 486, 504 (1993) (distributing union campaign literature via the e-mail system lists).

29 Cappel, *supra* note 12, at 6.

30 Ellis, *et al., supra* note 2, at Part II.

31 Cappel, *supra* note 12, at 9; however, some states, including Arkansas, California, Louisiana, Massachusetts, and Texas, are currently attempting to expand employee privacy rights in this area. Ellis, *et al., supra* note 2, at Part II.

32 Daniel B. Moskowitz, *Electronic-Mail Security Is Hot New Issue*, WASH. POST, Oct. 22, 1990, at F35.

A. *Federal or State Constitutional Constraints - Generally Inapplicable*

The Fourth Amendment to the U.S. Constitution affords protection of individual's privacy rights from government intrusion.[33] This Constitutional protection extends only to public employees, whereas private employers' behavior toward employees remains unrestricted.[34] Almost all states have a constitutional provision that mirrors the restrictions in the Fourth Amendment regarding search and seizure.[35] Presently, California is the only state in which the application of a state constitutional right of privacy has been expanded to include the protection of both public and private employers.[36] In other states, employees have successfully asserted a right of privacy under state constitutional law upon showing that the government was the employer.[37]

Private sector employees' communications in the workplace, such as communications using e-mail, generally are not protected under any constitutional right to privacy. The commercial nature of such e-mail communications would also make unavailable any protection under the First Amendment.[38] Therefore, guidance concerning the limits of individual privacy rights must come from other sources.

B. *Electronic Communications Privacy Act of 1986, And The Limits On Its Exceptions*

The Electronic Communications Privacy Act of 1986 (hereinafter "ECPA")[39] was signed into law by President Ronald Reagan, amending the old federal wiretap law.[40] The ECPA provides protection for electronic communications made by "any transfer of signs, signals, writing, images, sounds, data

---

[33] Julie A. Flanagan, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256, 1264 (1994) (citing U.S. Const. amend. IV (providing that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated")).

[34] *Id.* at 1264-65.

[35] *Id.* at 1265.

[36] *Id.*, *see* Porten v. Univ. of San Francisco, 134 CAL. RPTR. 839, 842 (Court. App. 1976).

[37] Flanagan, *supra* note 33, at 1265.

[38] Keitt & Kahn, *supra* note 1, at 24.

[39] 18 U.S.C. §§ 2510-2521 (1988).

[40] Ruel Torres Hernandez, *ECPA and Online Computer Privacy*, 41 FED. COM. L.J. 17, 29 (1994); *see* 18 U.S.C. §§ 2510-2521 (1988).

or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce."[41] Specifically, the ECPA broadly prohibits the interception of "wire, oral or electronic" communications or transmissions as well as the disclosure and use of such information,[42] except where proper legal authorization exists.[43] All telephonic means of communication that "cannot fairly be characterized as containing the human voice" are protected.[44] Protected electronic communications, as noted by the Senate Report, include non-voice communications such as "electronic mail, digitized transmissions, and video teleconferences."[45]

Despite the provisions of ECPA, to date *private* employers can exercise almost complete freedom in monitoring their employees.[46] The manner or extent of employee surveillance has not been restricted.[47] Moreover, employers are not required to provide any type of notice to employees.[48] This is particularly true in the context of employer control of e-mail communications, where not a single case has been published under ECPA.

Some commentators have suggested that this exists because messages exchanged by private employers within internal e-mail systems that are used solely for interoffice communication, by their very nature, do not affect "interstate or foreign commerce" as the Committee on Technology and the Law has found that employers may have a legal right to control access and disclosure of e-mail messages because intra-company e-mail systems are not usually open to the public.[49]

The lack of published cases under ECPA involving disputes in the context of employer's monitoring of e-mail suggests that this may be an accurate assertion. The lack of litigation, as well as the absence of clear prohibitions on private e-mail systems, has led at least one commentator to conclude that

---

41 18 U.S.C. § 2510(12) (1988). "Thus, protection for electronic communications is defined in terms of what is transmitted and how it is transmitted." Hernandez, *supra* note 39, at 29. The Act includes the requirement that the means of transmission must affect interstate or foreign commerce. 18 U.S.C. § 2510(12) (1988).

42 Costa-Clarke, *supra* note 5, at 6.

43 18 U.S.C. § 2511; *see also* Hernandez, *supra* note 39, at 29, 30.

44 Hernandez, *supra* note 40, at 29 (citing S. REP. NO. 541, 99th Cong., 2d Sess. 14, (1986) *reprinted in* 1988 U.S.C.C.A.N. 3555, 3568.

45 Hernandez, *supra* note 40, at 29.

46 *Id.*

47 *Id.*

48 *Id.*at 39.

49 *Id.*at 39.

the ECPA's electronic storage provisions exclusively govern employer-owned e-mail systems.[50] Under this view, employers, as "corporate big brothers" have unfettered discretion to read and disclose the contents of an e-mail message.[51] However, considerable speculation on this subject is evidenced by the lack of published cases. Another commentator has warned that in light of Congress' expressed intent to procure parity in guarding personal communications, the ECPA may impose access limitations on private employers who possess their own systems.[52]

In sum, it remains unclear how the rapid increase in e-mail across state or national boundaries — even within a single employer — and between employers, their customers, and vendors could impact the above-noted views. Accordingly, employers who monitor e-mail communications should consider whether such monitoring fits within the context of at least one of the two ECPA exceptions which, if ECPA indeed applies, must be invoked to avoid liability for certain employer monitoring of e-mail communications. As discussed below, these exceptions have limits, and their availability cannot be guaranteed.

---

[50] Julia Turner Baumhart, *The Employer's Right To Read E-Mail: Protecting Property or Personal Prying?*, 8 LAB. LAW. 923, 926 (1992) (citing Hernandez, *supra* note 40, at 39).

[51] *Id.* at 926 (citing Hernandez *supra* note 40, at 39-40).

[52] Baumhart, *supra* note 50, at 926. Baumhart asserts that Congress's express intention that pre-ECPA prohibitions apply to employers' interceptions of employee telephone conversations, and the subsequent upholding of such intent in federal courts, indicates that Congress saw no need to specify that ECPA coverage likewise extends to employers. Baumhart, *supra* note 50, at 926. In addition, Baumhart points out that certain Senate testimony acknowledged that the proposed legislation was designed to include *all* electronic communications, including those generated through internal employer-owned E-Mail systems. Baumhart, *supra* note 50 at 927 (citing Electronics Communications Privacy, 1985: Hearing on S 1667 Before the Sub. comm. on Patents, Copyrights and Trademarks of the Senate Comm. on the Judiciary, 99th Cong., 1st Sess. 99-100 (statement of Philip Walker, Vice-Chair, Electronic Mail Ass'n)("electronic mail users obviously deserve privacy protection regardless of what type of entity runs their system...")).

However, the same commentator also acknowledges that elements of ECPA legislative history provide some support for the position that Congress did not intend to inhibit employers from reviewing employee-generated e-mail files. Baumhart, *supra* note 50, at 926. For example, while the Senate Report acknowledged the existence of internal corporate E-Mail systems, it did not address the anticipated effect of the proposed legislation on these systems. Baumhart, *supra* note 50, at 926 (citing S. REP. NO. 541, 99th Cong., 2d Sess., 8, *reprinted in* 1986 USCCAN 3555, 3562). Moreover, much of the testimony taken during the Senate hearing reflected a more significant concern for employer interests, rather than for individual employee privacy. Baumhart, *supra* note 50 at 926 (citing Electronics Communications Privacy, 1985: Hearing on S. 1667 Before the Sub. comm. on Patents, Copyrights, and Trademarks of the Senate Comm. on the Judiciary, 99th Cong., 1st Sess. 40, 42 (statement of Senator Patrick J. Leahy, co-sponsor, S 1667), 105 (statement of P. Michael Nugent, Board Member, ADAPSO).

1. *"Ordinary Course of Business" Exception*

"Interception" under the ECPA does not occur if employer monitoring of wire, oral or electronic communications of an employee is "within the ordinary course of business."[53] Courts are split on their interpretation of employer monitoring which falls within the "ordinary course of business."[54] For example, the Eleventh Circuit has held that an employer's listening-in on an employee's personal call is never "in the ordinary course of business . . . except to the extent necessary to guard against unauthorized use of the telephone, or to determine whether a call is personal or not."[55] The Eighth Circuit, has held that an employer is in violation of the ECPA only when the employer excessively monitors personal aspects of an employee's life.[56] For example, in *Deal v. Spears* the Eighth Circuit affirmed the district court's finding that an employer's electronic monitoring violated the ECPA.[57] In *Deal*, store owners believed that their employee was involved in a store

---

[53] "Intercept" is defined under ECPA as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1988). Within the definition of "intercept," the terms "electronic, mechanical, or other device" are defined as:

> any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than
>
> —(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (I) *furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business*;

18 U.S.C. § 2510(5)(a) (1988) (emphasis added).

[54] *See, e.g.*, Griggs-Ryan v. Smith, 904 F.2d 112, 119 (1st Cir. 1990) (holding landlord did not violate Title III because tenant consented to interception of incoming telephone calls); Epps v. St. Mary's Hosp. of Athens Inc., 802 F.2d 412, 416-17 (11th Cir. 1986) (monitoring phone call between employees by another employee acting beyond her authority deemed to be in the ordinary course of business); Briggs v. American Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980) (decided under pre-ECPA Title III, court held that when an employer is concerned about the disclosure of confidential information, "it is within the ordinary course of business to listen in on an extension phone for at least so long as the call involves the type of information he fears is being disclosed").

[55] Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983). The Court noted that once the manager determines that the call is personal, he or she must cease listening to the call in order to remain within the exception, even though the topic of conversation may in some way concern the employer. *Id.*, at 584.

[56] Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992).

[57] *Id.* at 1155.

burglary.[58] The owners secretly recorded and listened to twenty-two hours of telephone calls that contained highly personal information, including details of an extramarital affair.[59] Although the court found that some monitoring would have been justified,[60] it held that the extent to which the owners intercepted personal phone calls was "well beyond the boundaries of the ordinary course of business."[61]

Clearly, the "ordinary course of business" exception is more likely to be available to employers who effectively communicate written information control and monitoring policies to their employees.[62] Additionally, the ECPA's expressed purpose of evenhanded protection of privacy may encourage courts to be more supportive of an employer's monitoring of the transmission of the message itself, rather than the content of the message.[63] However, it has been demonstrated that where an employer does set forth a monitoring policy, the employer must stay within the parameters of such a policy in order to successfully avail itself of the exception.[64] In *Watkins*, a pre-ECPA Title III case, the defendant had a policy of monitoring employee's sales calls, and employees were advised of this policy.[65] The employer further advised employees that their personal calls would not be monitored except to the extent necessary to determine whether their calls were of a personal or business nature.[66] The plaintiff, an employee, sued when he discovered that his employer monitored a call in which he discussed a job interview with a prospective employer.[67] The court found that this interception was "not in the ordinary course of business" because the employee was an employee-at-will and the employer had no legal interest in his future employment plans.[68] The

---

58 *Id.*

59 *Id.* at 1155-56.

60 *Id.* at 1158.

61 *Id.*

62 Costa-Clarke, *supra* note 5, at 25 (citing Simmons v. Southwestern Bell Telephone, Co., 452 F. Supp. 392, 394-395 (W.D. Okla. 1978) (holding that defendant employer's monitoring was in "ordinary course of business" where the defendant had a policy against the use of phones for personal calls and the plaintiff had been warned about making personal calls on these lines).

63 Baumhart, *supra* note 50, at 933.

64 *See, e.g.*, Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983).

65 *Id.* at 579.

66 *Id.*

67 *Id.*

68 *Id.* at 582.

court stressed that "in the ordinary course of business" cannot be extended to mean "anything that interests a company."[69]

2. *"Consent" Exception*

Interception is not a violation under EPCA if a party to the communication has given prior consent to the interception at issue.[70] However, an employee's awareness or knowledge that they are being monitored does not necessarily constitute consent.[71] The *Watkins* holding emphasizes this point.[72] Clearly, employers who set forth policies and act within the parameters of such policies maximize their potential for success by invoking a "consent" defense.

3. *Employer Monitoring of E-Mail In Light Of ECPA*

Although most employer monitoring of e-mail systems would probably fall within the "ordinary course of business" exception to the ECPA, there has yet to be a case decided where an employee sued an employer under the ECPA for unlawfully accessing that employee's e-mail or voice mail.[73] However, several California lower court cases concerning employer accessing of e-mail messages are pending on appeal.[74] These cases are based on state privacy law and offer little guidance or variation.[75] Additionally, the telephone

---

[69] *Id.*

[70] 18 U.S.C. § 2511(2)(d) (1988).

[71] Costa-Clarke, *supra* note 5, at 25 (citing Jandak v. Village of Brookville, 520 F. Supp. 815 (N.D. Ill. 1981)) (holding that while the defendant's employee should have known that the line he used was monitored, he had not implicitly consented to this monitoring; the court reasoned that consent should not be given expansive definition in context of statute designed to protect privacy).

[72] *See supra* notes 68-71 and accompanying text.

[73] *See* Thomas R. Greenberg, *E-Mail and Voice Mail: Employee Privacy And The Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 238 n.102 (1994).

[74] *Id.* at 239.

[75] *See* Cameron v. Mentor Graphics, No. 716361 (Cal. Sup. Court., Santa Clara County, filed Nov. 7, 1991) (claiming wrongful termination as a result of employer's reading of an employee's e-mail message, where the employer apparently searched the e-mail message for the principal purpose of finding incriminating information to support its just-cause termination action against the employee; Bourke v. Nissan Motor Co., No. YC003979 (Cal. Sup. Court., Los Angeles County, filed 1989); Flanagan v. Epson America, No. BC007036 (Cal. Sup. Court., Los Angeles County, filed 1989). One case brought under California Penal Code § 631, was dismissed when the judge found that the provision covered telephone interception and wiretapping, but not electronic communications such as e-mail. *See* Shoars v. Epson Am., No. SCW112749 (Cal. Sup. Court., Los Angeles County, filed 1989).

communication cases do not provide a perfect analogy. As one commentator has noted, equating e-mail with a mailed letter — with its historical enjoyment of significant privacy protection — might alter the outcome.[76] In light of both the "ordinary course of business" and "consent" exceptions, it is evident that employer monitoring of e-mail systems is far more likely to be permissible if such monitoring is consistent with announced employer policies.

C. *Pending Privacy For Consumers Act*

Privacy concerns generated from employer monitoring led to the introduction of the proposed Privacy for Consumers and Workers Act (hereinafter "PWCA"). The PCWA, introduced before Congress in 1993, and not reported out of Committee, was designed to establish "privacy protections for employees and customers with respect to electronic monitoring in the workplace by employers."[77] The PCWA, which has yet to be reintroduced before the current session of Congress, would require employers: to inform prospective employees of monitoring policies, through prior written notice to employees of the collection and use of personal data, and detailing the manner and frequency of these practices.

The PCWA would permit monitoring of individuals without notice where the employer has "reasonable suspicion" of employee conduct which (1) violates civil or criminal laws, (2) constitutes "willful gross misconduct," or (3) adversely affects the employer.[78] Further, employers who conduct monitoring based on "reasonable suspicion" would be required to complete a statement "setting forth the basis for the reasonable suspicion."[79]

Despite the fact that the PCWA is viewed as pro-employee legislation, it contains provisions limiting the scope of employer acts subject to PCWA's purview. Specifically, the PCWA expressly permits all employee monitoring performed in compliance with its guidelines.[80] Accordingly, an employer's concern with employee privacy claims may be minimized through its voluntary compliance with the PCWA's provisions.[81]

---

76 Cappel, *supra* note 12, at 9.

77 Costa-Clarke, *supra* note 5, at 25 (citing 1993 H.R. 1900; S. 984 (bill digest)).

78 *Id.*

79 *Id.*

80 *Id.*

81 *Id.*

D. Potential Cause of Action Under State Wiretapping Statutes

The following states provide a private statutory right of action for illegal wiretapping, which substantially parallel Title III and ECPA: California, Delaware, District of Columbia, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Nebraska, New Hampshire, New Jersey, New Mexico, Ohio, Oregon, Pennsylvania, Rhode Island, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.[82] Generally, these statutes allow for actual or statutory damages of up to $100 per day of violation, or $1000, whichever is greater, in addition to reasonable attorney's fees and costs.[83] To date, only California (see above) has considered an e-mail monitoring case under such a state statute.

E. Potential Common Law Causes of Action

Some legal authorities have pointed out that an employer could still be sued for intercepting employees' e-mail messages under the common law tort of "invasion of privacy."[84] Under this theory, the employee would be required to prove that he or she had a "reasonable expectation of privacy" in his/her e-mail messages and that the employer violated this expectation.[85] The employer, on the other hand, would likely defend this action by showing that the monitoring was justified by a "legitimate business interest."[86] To date, we are unaware of any court which has considered and addressed a tort claim of this type involving e-mail privacy.[87]

At the same time, employers are increasingly being sued for defamation[88] and intentional infliction of emotional distress[89] based on intra-company

---

[82] Greenberg, *supra* note 73, at 222 n.16. For a list of the relevant statutes see Greenberg, *supra* note 73, at 222 n.16.

[83] *Id.*

[84] Cappel, *supra* note 12, at 8.

[85] Cappel, *supra* note 12, at 8-9.

[86] Cappel, *supra* note 12, at 9.

[87] *Id.*

[88] *See*, e.g., Kurtz v. Williams, 371 S.E.2d 878 (Ga. Court. App. 1988).

[89] *See, e.g.*, Levie v. AT&T Communications, Inc., 52 Fair Empl. Prac. Cas. (BNA) 664 (N.D. Ga. 1990) *aff'd* 929 F.2d 706 (11th Cir. 1991).

communications regarding employer performance appraisals or critiques.[90] Where e-mail is used to offer assessments on employee performance, and the sender is a manager or agent of the employer, another front can be opened in the ongoing battle over an employer's qualified privilege to communicate performance evaluations. When the qualified privilege is lost, or when e-mail is inadvertently read by someone not subject to the privilege, the potential for defamation liability is considerable.

The stakes have risen recently as a result of a New York Supreme Court case — *Stratton Oakmont, Inc. v. Prodigy Services Co.* — where the on-line computer service owned and operated by Prodigy is being sued for defamation.[91] The investment firm of Stratton Oakmont contends that Prodigy is liable for a message posted by a subscriber to the service which accused the firm of fraud.[92] In an early decision in the case, the judge ruled that in operating and marketing the service,[93] Prodigy was the publisher of the alleged defamatory statement.[94] Holding Prodigy responsible for a user's statement has serious implications for an employer's e-mail system, where the extent to which the e-mail system is owned, operated and controlled by the employer is much more evident.

F. Equal Employment Statutes

The mountain of federal and state equal employment and anti-discrimination laws create another significant concern in the use of e-mail. The use of company memos has long enabled employers and former employees to succeed in race, sex, and age discrimination litigation. E-mail can be another source of "direct evidence" of intentional discrimination or a hostile or harassing work environment,[95] and when the senders are managers,

---

[90] *See, e.g.*, Kurtz v. Williams, 371 S.E.2d 878 (Ga. Court. App. 1988); Levie v. AT&T Communications, Inc., 52 Fair Empl. Prac. Cas. (BNA) 664 (N.D. Ga. 1990) *aff'd.* 929 F.2d 685 (11th Cir. 1991).

[91] 23 Media L. Rep. 1794 (N.Y. Sup., May 24, 1995)(No. 31063/94).

[92] *Id.*

[93] *Id.*

[94] *Id.* at B2. Interestingly, the judge subsequently refused to vacate his decision despite apparent settlement of the dispute, citing the need for "precedent in the area of cyberspace law." THE NATIONAL LAW JOURNAL, Dec. 28, 1995, at B2.

[95] For example, in a recent decision that polarized the campus at the California Institute of Technology, a promising doctoral candidate was expelled from the prestigious university for allegedly sexually harassing another student — largely via e-mail. Amy Harmon, *Expulsion from Cal-Tech Raises Issue of E-Mail Harassment*, ATLANTA CONST. J., Nov. 23, 1995, at A11.

the potential liability can, once again, be extensive.[96]

For example, in *Straus v. Microsoft Corp.*, the Southern District of New York relied on evidence of inappropriate e-mail messages by a supervisor, in its denial of Microsoft's motion for summary judgment against a plaintiff alleging Title VII gender discrimination.[97] The Court found that a reasonable jury could conclude that Microsoft's stated reason for failure to promote, namely that Plaintiff was not qualified,[98] was pretextual, where similarly situated individuals were promoted[99] *and* where the decision-maker's conduct included: (1) his transmission of one e-mail message to his company's entire staff about "Mouse Balls," which contained sexual innuendo about male genitalia; (2) his transmission of an e-mail message directly to Plaintiff entitled "Alice in UNIX Land", which mixed computer language with sexual innuendo; and (3) his transmission of two other sexually explicit e-mail messages to another employee of the company who then sent the material to the rest of the staff.[100] The Court also used evidence from e-mail communications between the decision-maker and his superior to show that the Company was willing to hire a similarly-situated person despite his lack of experience.[101] The same Court revisiting this case following the United States Supreme Court's 1993 *St. Mary's Honor Center v. Hicks*[102] decision, which purportedly increased a plaintiff's burden of proof in Title VII cases,[103] found

---

[96] For example, in a case filed earlier this year, four female employees sued their Fortune 500 employer for pornographic e-mail messages sent between employees at the Company's information and technology division. Although they denied the charges, this company quickly settled the lawsuit for $2.2 million plus the plaintiffs' attorneys' fees and court costs. Ellis, *et al.*, *supra* note 2, at part III (citing Annie M. Soden, *Protect Your Corporation from E-Mail Litigation*, CORP. LEGAL TIMES, May 1995, at 19).

[97] *See* Strauss v. Microsoft Corp., 814 F. Supp. 1186 (S.D.N.Y. 1993).

[98] *Id.*, at 1193.

[99] *Id.*

[100] *Id.* at 1194. The Court also heavily weighed several oral comments of the supervisor including: (1) his comments to Plaintiff that he was "president of the amateur gynecology club," (2) his reference to a woman employee as a "Spandex queen," (3) his reference to a black woman as "Sweet Georgia Brown," and (4) his offer to pay 500 dollars to call the woman "Sweet Georgia Brown." *Id.* at 1194.

[101] *Id.* at 1193-94. The pertinent e-mail stated that the applicant who was eventually hired would "have one heck of a learning curve to come up on since he has not even written for publication, much less acquired materials or managed the editorial process . . . IF you decide he is your candidate, then he needs . . . a real, real strong right-hand person . . . involved in TRAINING him on the issues and problems." *Id.* at 1194.

[102] 113 S.Ct. 2742, 2745 (1993).

[103] *Id.* at 2745.

that such evidence was also sufficient to support a reasonable jury's finding of intentional discrimination.[104]

In *Miller v. U.S.F. & G.*, the District Court upheld the summary judgment motion of a defendant who terminated the plaintiff, in part, for her knowledge and acquiescence in the extensive usage of a numerical e-mail list of approximately 75 profane words and phrases by certain employees who express dissatisfaction with the company's new salary guidelines.[105] However, the Court rejected the plaintiff's comparison of herself and other male employees who allegedly knew about the numerical code and used profanity around the office, but were not discharged, because plaintiff, who had been the Human Resources Manager, was held to a higher standard of conduct than the other employees.[106]

In *Donley v. Ameritech Services*, the Eastern District of Michigan granted summary judgment for a defendant sued by a Caucasian plaintiff who was discharged because his supervisor found that an e-mail message which he had sent to a co-worker about an African-American client was offensive and disrespectful of the client.[107] The plaintiff brought a reverse discrimination claim under Michigan's Elliott-Larsen Civil Rights Act[108] (hereinafter "Act"), arguing that *if* a non-white male had sent the same e-mail message such person would not have been discharged.[109] The Court found this argument to be insufficient to meet the "comparable employee" requirement under the Act.[110]

Finally, in a case which never reached trial, a woman in Seattle sued her former employer for age discrimination after she was fired. Although her complaint initially appeared unlikely to succeed as a result of the employer's "picture perfect" termination letter, Plaintiff was able to negotiate after the Plaintiff's attorney hired a computer consultant who used a sophisticated software to "un-erase" a supposedly deleted e-mail message from the company's president to the head of the personnel department. In colorful

---

104 Strauss v. Microsoft Corp., 856 F. Supp. 821, 825 (S.D.N.Y. 1994).

105 *Miller v. U.S.F.&G.*, No. HAR 93-1968, 1994 U.S. Dist. LEXIS 10541, at *4 (D. Md. May 13, 1994).

106 *Id.* at *17.

107 No. 92-72238, 1992 U.S. Dist. LEXIS 21281, at *1 (E.D. Mich. 1992). The Plaintiff acknowledged that in e-mail messages he and two other Caucasian male employees "referred to an African American client John Webb as "John the Turd" and that he thought it would be funny to replace all the "th"'s with "t"'s in his messages." *Id.*, at *4.

108 MICH. COMP. LAWS ANN. § 37.2101 (1985).

109 *Donley*, 1992 U.S. Dist. LEXIS 21281 at *7.

110 *Id.* at *9.

language, the president's e-mail had instructed to supervisor to fire the plaintiff. Faced with this evidence, the company's attorney, who had previously viewed the case as nothing more than a nuisance, suddenly agreed to settle the case for $250,000.[111]

IV. ADOPTION OF E-MAIL POLICIES TO SATISFY GOALS OF ORGANIZATION

As a result of the uncertain legal environment, as well as several other factors, employers should establish explicit policies with respect to issues of e-mail usage, control, and monitoring to ensure protection from potential causes of action, and to foster organizational goals generally.

A. Foster Organizational Goals and Expectations With Regards To E-Mail

Explicit company e-mail policies would foster the achievement of the goals of employers with regards to e-mail usage and control, as well as ensure that both employee and employer expectations are met, whether the policies themselves are restrictive (pro-employer monitoring) or non-restrictive (pro-employee privacy).[112]

B. Accomplish Full Compliance with ECPA

Although it appears that employer monitoring of e-mail is permissible in all cases under ECPA,[113] the lack of precedent makes this issue uncertain. Employers may, however, fully shield themselves from ECPA liability under the "consent" exception by simply establishing clear policies with respect to monitoring of e-mail communications, and acting within the parameters of such policies.[114]

---

[111] Ellis, *et. al, supra* note 2, at part III (*citing* Ellen Wright, *Executive Secrets Incriminating Data*, HEMISPHERES, June 1993, at 32).

[112] In cases where the employer wishes to place emphasis on employee privacy, an explicit policy would likely reduce instances of "snooping" by management, and give the company grounds legally to distance itself from, and to impose disciplinary penalties against, any management employee who commits misconduct in this context.

[113] *See, supra* notes 39-54 and accompanying text.

[114] Costa-Clarke, *supra* note 5, at 25.

C. *Close Gap Between Employee's Expectations And Legal Realities*

Explicit company e-mail policies also would close the significant gap between employees' e-mail privacy perceptions and legal realities.[115] As noted, there is no clear precedent or federal statute which establishes that employers are generally free to monitor employee e-mail communications at their discretion.[116] Accordingly, this area is ripe for lawsuits whenever conflicts arise, and at this time employers do not have tangible legal precedent to discourage employees from pursuing such lawsuits.

Even assuming that employers prevail in most of these cases, fighting legal battles is costly, diverts employers' attention away from the real management of the business, and may lead to workplace conflict that has a demoralizing effect on employees.[117] In several instances where company management has reviewed employees' e-mail messages without the employees' knowledge and consent, a legal action against the employer has resulted.[118] All of these lawsuits may have been avoided or discouraged had the defendant company established and communicated clear policies on e-mail usage and privacy. Moreover, given the rapid growth of electronic mail, it is likely that more lawsuits will be filed over the issue of e-mail privacy, particularly if employees or management remain misinformed or ignorant of their rights or limitations.

D. *Protect Employer from Potential Harassment Claims Arising From E-Mail Abuses*

Certain characteristics of e-mail such as the ease and informality of use, the absence of face-to-face communication, and the notion of limited publication, provide potential for actual or perceived sexual harassment.[119] For example, there have been unpublished cases where female employees have been the object of sexually harassing e-mail letters from a fellow male

---

115 Cappel, *supra* note 12, at 9.

116 *See, supra* notes 51-53 and accompanying text.

117 Cappel, *supra* note 12, at 10.

118 Cappel, *supra* note 12, at 7. The two most prominent cases involve Epson America and Nissan Motor Corp. *See* Cappel, *supra* note 12, at 7; see Shoars v. Epson Am., No. SCW112749 (Cal. Sup. Court., Los Angeles County, filed 1989); Bourke v. Nissan Motor Corp., No. YC 003979 (Cal. Sup. Court., Los Angeles County, filed 1989).

119 Shannon & Rosenthal, *supra* note 16, at 31.

employee. The employee retained anonymity by using the computer identification number of another worker.[120] The feature of informality also may lead to e-mail communications being construed as harassing when such was not the intention of the author.[121]

Clear company policies and disclaimers, as well as the implementation of technologically advanced e-mail log-in systems, can limit an employer's potential liability in this sensitive area.[122] For instance, the employer may include a provision which bars the use of e-mail to send foul, improper, or offensive language which may include actionable statements such as racial or sexual slurs. Further, the employer may include a provision which informs employees that abuse of the company's written e-mail policies may result in discipline against employees up to and including termination.[123] In addition, the employer might include a provision encouraging users to treat e-mail messages in the same careful manner which they would letters or interoffice memos and to realize that their e-mail communications may be seen by third parties or management.[124] Of course, all of these policies would typically fit comfortably within an employer's existing general prohibitions against workplace discrimination and harassment.

E. Protect Employer From Liability Arising From Involuntary Disclosure of Confidential Information

Explicit company e-mail policies would also reduce exposure to liability arising from the involuntary disclosure and often unrecognized disclosure of confidential information. The e-mail explosion and retention of massive quantities of information on computers has recently raised these issues of company liability.[125]

The adoption of good information control policies and procedures, including security systems, such as extensive user passwords and encryption devices, could address these problems.[126] The employer may further include a provision which prohibits employees from using unauthorized codes or

---

120 *Id.*

121 *Id.*

122 *Id.* at 33.

123 Costa-Clarke, *supra* note 5, at 25.

124 Keitt & Kahn, *supra* note 1, at 26.

125 *Id.* at 24.

126 *Id.* at 26.

passwords to gain access to other files.[127] In addition, the employer might consider adopting a document retention policy which discards mail files permanently on a systematic basis.[128] In choosing this option, the employer should decide which (if not all) e-mail materials will be erased permanently from the network and after what period of time (*e.g.* 30, 60, or 90 days). Company managers should then warn employees that important electronic mail messages should be printed or transcribed before the applicable deadline.[129] Finally, the employer may include a provision establishing strict scrutiny procedures for confidentiality of information and accountability for intentional or negligent release of information.[130] To this end, employees should be reminded periodically not to leave e-mail messages on screen when leaving a computer, and to periodically change their passwords to avoid unauthorized access by hackers.[131]

F. Potential Compliance With Privacy Legislation

Adopting an information control and monitoring policy and communicating it to employees will also give employers a head start in complying with proposed legislation such as the Privacy for Consumers and Workers Act ("PCWA").[132]

G. Improved Employer-Employee Relations

The early development of well-articulated company policies can provide an excellent basis for improved employer-employee relations, employee morale, and an enhanced perception of the company by its employees.[133] These policies should also minimize those situations where managers face the dilemma of determining whether e-mail monitoring or "snooping" is professionally required, or ethically inappropriate. To foster such improved employer-employee relations, the employer might consider policies limiting its use of the information obtained from the e-mail messages to the stated

---

127 *Id.*

128 *Id.*

129 Ellis, *et. al*, *supra* note 2, at Part III.

130 Cappel, *supra* note 12, at 10.

131 Ellis, *et. al*, *supra* note 2 at Part V.

132 Costa-Clarke, *supra* note 5, at 25.

133 Alice LaPlante, *Is Big Brother Watching*, INFOWORLD, Oct. 22, 1990, at 65-66.

purpose of any search or surveillance.[134] At the same time, employer credibility is strengthened by notifying employees in advance of any investigation, that the electronic mail system and the e-mail messages circulated constitute employer property and are subject to employer monitoring without notice. Finally, by initially communicating a clear statement of the proper and improper use of e-mail, an employer can avoid allowing employee expectations of e-mail usage to develop into a perceived benefit or entitlement thereby minimizing a negative impact on employee relations when such a "benefit" is eliminated.

H. Union Concerns

Most employers implementing a restrictive e-mail policy should consider a specific provision which bars the use of e-mail to solicit outside business opportunities or for personal, political, or religious concerns.[135] However, as will be discussed below, employers with unionized workforces, or those employers concerned about a union organizing their employees, would be best served by implementing and enforcing a relatively broad prohibition against the use of e-mail for non-business reasons, without necessarily adding any specific prohibitions.[136]

V. SURVEY OF E-MAIL POLICIES IN EFFECT

Specific e-mail policies which have been implemented to-date have distinguishing characteristics. These differences appear to be a result of the specific concerns that the policies are intended to address, the existence of any practices, policies, or procedures which already address the concerns, and the nature of the workforce, *i.e.*, union or non-union. In all cases, however, it appears that employers implementing e-mail policies seek to establish clear written policies and procedures which tell the employees what they can

---

134 Cappel, *supra* note 12, at 10.

135 Costa-Clarke, *supra* note 5, at 25.

136 Belcher Towing Co. v. NLRB, 614 F.2d 88, 90 (5th Cir. 1980) (holding a rule that prohibits solicitation, on company premises, by non-employees is ordinarily presumed valid and will only be overturned by a showing that either the rule discriminates against unions by allowing other solicitation or that no reasonable alternative access to employees exists) *citing* NLRB v. Babcock & Wilcox Co., 351 U.S. 105 (1956).

expect, what is expected of them, and what impact the policy will have on them.[137]

A. *Restrictive Policies*

Many companies, such as Federal Express, Eastman-Kodak,[138] DuPont, Pacific Bell, Nordstrom,[139] Bank of Boston, Hughes Aircraft, and United Parcel Service,[140] have employed restrictive policies which specify that e-mail systems are company property, reserve the right for the company to examine e-mail without notice, and designate e-mail systems as purely for "business use."[141] From the outset, these policies, if properly announced, eliminate any reasonable expectation of privacy and alert employees to the potential risks of using e-mail for non-business purposes.

Restrictive policies may become more popular with employers in union or union campaign settings, since they may allow employers to act against employees who use e-mail systems to organize union campaigns or to post organizational notices. However, in light of a recent National Labor Relations Board ("NLRB") decision, discussed below, it is important that employers not specifically bar such activity, but instead broadly bar all non-work-related activity and enforce such a prohibition in a consistent manner.

---

[137] Shannon & Rosenthal, *supra* note 16, at 33.

[138] Kodak's e-mail policy requires its employees to sign a statement at the time they apply for a new computer account, confirming that they have read and understand Kodak's policy about e-mail monitoring. Kodak's Director of Records Management and Information Security Services indicates that while the company has an e-mail monitoring policy, in practice, a Kodak manager would only look at the personal files or messages of an employee under "special circumstances," such as if an employee is leaving Kodak's employ, if necessary to resolve a technical problem, or if the employee is a known abuser of the system. Cappel, *supra* note 12, at 6-7.

[139] Nordstrom, a Seattle-based retailer, distributes its e-mail privacy policy to its new hires and quarterly to all employees using the e-mail system. In pertinent part, the policy discourages an expectation of employee privacy in e-mail messages as follows:

> Electronic mail is a company resource and is provided as a business-communications tool. Employees with legitimate business purposes may have the need to view your electronic-mail messages. It is also possible that others may view your messages inadvertently, since there is no guarantee of privacy for electronic-mail messages. Please use your good judgment as you use the electronic-mail system.

Cappel, *supra* note 12, at 6-7.

[140] At United Parcel Service, workers are informed when they log onto the network that the company reserves the right to monitor e-mail messages. The company uses this message to discourage employee use of the e-mail for personal reasons and to guard against potential complaints from employees who claim to be unaware of the policy. Cappel, *supra* note 12, at 7.

[141] Cappel, *supra* note 12, at 6-7.

In *E.I. DuPont De Nemours & Co.*,[142] the NLRB found that an employer policy prohibiting employees from using electronic mail systems for distributing union literature and notices violated Section 8(a)(1) of the National Labor Relations Act.[143] The Board found that this prohibition was clearly discriminatory after observing that the employer had permitted the routine use of the electronic mail by a recreational committee of employees, as well as other employees, to distribute a wide variety of material that had "little if any relevance to the company's business."[144] In general, employers who work with unionized labor forces should be sure to write and enforce their "business use only" rules without exception.[145] Those non-union employers who may live without fear of union campaigns have greater flexibility in establishing exceptions, such as using e-mail for legitimate charitable purposes.

B. Non-Restrictive Policies

As mentioned, the goals of the company in developing specific e-mail policies should affect the nature of the actual policies adopted. Some firms, such as General Motors, McDonnell-Douglas, Hallmark Cards, Warner Brothers, Media General, and CitiBank reportedly have e-mail policies which place greater emphasis on employee privacy rights.[146] These employers also may be primarily concerned with the chilling impact that a restrictive policy may have on the morale of their employees. For example, one employer — Media General of Richmond, Virginia — reportedly chose its e-mail communications system, PC-MAIL, with user privacy as a top priority.[147] Media General's PC-MAIL system automatically encrypts files and messages to prevent even network administrators from reading them.[148] The administrators can only change passwords, but do not know the existing

---

142 311 NLRB 893 (1993).

143 *Id.* at 919.

144 *Id.*

145 For example, in *St. Anthony's Hospital*, the NLRB held that although employees had no statutory right to use of an employer's bulletin board, once an employer permits nonwork-related material to be posted, it may not discriminate against what type is posted. 292 NLRB 1304, 1307 (1989); ***but see*** Guardian Industries Corp. v. NLRB, 49 F.3d 317 (7th Cir. 1995). (holding employer was entitled to bar union notices while allowing "for sale" announcements on bulletin board).

146 Cappel, *supra* note 12, at 7.

147 *Id.*

148 *Id.*

passwords.[149] Such a policy choice, while perhaps best for the particular business needs and culture of an employer, should be made with a full understanding of the potential for abuse by an employee and the imposition of liability on the employer.

CONCLUSION

In light of the current absence of legislation or court decisions delineating employee privacy rights in the context of intra-company e-mail communications, it appears that employers presently have the legal right to monitor and read employees' e-mail communications without being *required* to announce a policy. However, to minimize misunderstanding and potential legal action, employers should develop and articulate a policy with regards to intra-company e-mail communications and employer monitoring. Whether restrictive or non-restrictive, a clearly stated policy should ensure that both employer and employee expectations are met, while supporting the operating and human resources strategies of the organization.

---

[149] *Id.* at 6, (citing Alice LaPlante, Is Big Brother Watching?, INFOWORLD, Oct. 22, 1990, at 58).